This document is scheduled to be published in the
Federal Register on 04/18/2023 and available online at
federalregister.gov/d/2023-07229, and on **govinfo.gov**

DEPAR

Office of the Secretary

45 CFR Parts 170, 171

RIN: 0955-AA03

Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing

AGENCY: Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS).

ACTION: Proposed rule.

SUMMARY: This proposed rule would implement the Electronic Health Record (EHR) Reporting Program provision of the 21st Century Cures Act by establishing new Conditions and Maintenance of Certification requirements for health information technology (health IT) developers under the ONC Health IT Certification Program (Program). This proposed rule would also make several updates to certification criteria and implementation specifications recognized by the Program, including a revised certification criterion for decision support and revised certification criteria for patient demographics and observations and electronic case reporting. This proposed rule would establish a new baseline version of the United States Core Data for Interoperability (USCDI). Additionally, this proposed rule would provide enhancements to support information sharing under the information blocking regulations. The implementation of these provisions would advance interoperability, improve transparency, and support the access, exchange, and use of electronic health information. The proposed rule would also update the Program in additional ways to advance interoperability, enhance health IT certification, and reduce burden and costs.

DATES: To be assured consideration, written or electronic comments must be received at one of the addresses provided below, no later than 5 p.m. on [**INSERT DATE 60 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER**].

ADDRESSES: You may submit comments, identified by RIN 0955-AA03, by any of the following methods (please do not submit duplicate comments). Because of staff and resource limitations, we cannot accept comments by facsimile (FAX) transmission.

- *Federal eRulemaking Portal:* Follow the instructions for submitting comments. Attachments should be in Microsoft Word, Microsoft Excel, or Adobe PDF; however, we prefer Microsoft Word. http://www.regulations.gov.
- *Regular, Express, or Overnight Mail:* Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Attention: Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing Proposed Rule, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street, S.W., Washington, D.C. 20201. Please submit one original and two copies.
- *Hand Delivery or Courier:* Office of the National Coordinator for Health Information Technology, Attention: Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing Proposed Rule, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street, S.W., Washington, D.C. 20201. Please submit one original and two copies. (Because access to the interior of the Mary E. Switzer Building is not readily available to persons without federal government identification, commenters are encouraged to leave their comments in the mail drop slots located in the main lobby of the building.)

Enhancing the Public Comment Experience: To facilitate public comment on this proposed rule, a copy will be made available in Microsoft Word format on ONC's website (http://www.healthit.gov). We believe this version will make it easier for commenters to access and copy portions of the proposed rule for use in their individual comments. Additionally, a separate document ("public comment template") will also be made available on ONC's website (http://www.healthit.gov) for the public to use in providing comments on the proposed rule. This

document is meant to provide the public with a simple and organized way to submit comments on proposals and respond to specific questions posed in the preamble of the proposed rule. While use of this document is entirely voluntary, we encourage commenters to consider using the document in lieu of unstructured comments, or to use it as an addendum to narrative cover pages. We believe that use of the document may facilitate our review and understanding of the comments received. The public comment template will be available shortly after the proposed rule publishes in the **Federal Register**. This short delay will permit the appropriate citation in the public comment template to pages of the published version of the proposed rule.

Inspection of Public Comments: All comments received before the close of the comment period will be available for public inspection, including any personally identifiable or confidential business information that is included in a comment. Please do not include anything in your comment submission that you do not wish to share with the general public. Such information includes, but is not limited to, the following: a person's social security number; date of birth; driver's license number; state identification number or foreign country equivalent; passport number; financial account number; credit or debit card number; any personal health information; or any business information that could be considered proprietary. We will post all comments that are received before the close of the comment period at http://www.regulations.gov.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov or the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street, S.W., Washington, D.C. 20201 (call ahead to the contact listed below to arrange for inspection).

FOR FURTHER INFORMATION CONTACT: Michael Lipinski, Office of Policy, Office of the National Coordinator for Health Information Technology, 202-690-7151.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Executive Summary
A. Purpose of Regulatory Action
B. Summary of Major Provisions
1. ONC Health IT Certification Program Updates
a. "The ONC Certification Criteria for Health IT" and Discontinuing Year Themed "Editions"
b. New and Revised Standards and Certification Criteria
i. The United States Core Data for Interoperability Standard Version 3 (USCDI v3)
ii. C-CDA Companion Guide Updates
iii. "Minimum Standards" Code Sets Updates
iv. Electronic Case Reporting
v. Decision Support Interventions and Predictive Models
vi. Synchronized Clocks Standard
vii. Standardized API for Patient and Population Services
viii. Patient Demographics and Observations Certification Criterion in § 170.315(a)(5)
ix. Updates to Transitions of Care Certification Criterion in § 170.315(b)(1)
x. Patient Requested Restrictions Certification Criterion
xi. Requirement for Health IT Developers to Update their Previously Certified Health IT
2. Assurances Condition and Maintenance of Certification Requirements
3. Real World Testing – Inherited Certified Status
4. Insights Condition and Maintenance of Certification
5. Information Blocking Enhancements
C. Costs and Benefits
II. Background
A. Statutory Basis
1. Standards, Implementation Specifications, and Certification Criteria
2. Health IT Certification Program(s)
B. Regulatory History
III. ONC Health IT Certification Program Updates
A. "The ONC Certification Criteria for Health IT" and Discontinuing Year Themed "Editions"
B. Standards and Implementation Specifications
1. National Technology Transfer and Advancement Act
2. Compliance with Adopted Standards and Implementation Specifications
3. "Reasonably Available" to Interested Parties
C. New and Revised Standards and Certification Criteria
1. The United States Core Data for Interoperability Standard (USCDI) v3
a. Background
b. Certification Criteria that Reference USCDI
c. USCDI Standard – Data Classes and Elements Added since USCDI v1
2. C-CDA Companion Guide Updates
3. "Minimum Standards" Code Sets Updates
4. Electronic Case Reporting
a. Background
b. Standards Landscape for Case Reporting
c. Proposed Updates to Case Reporting in § 170.315(f)(5)
d. Proposed Adoption of Standards for Electronic Case Reporting
e. Proposal for Reporting
5. Decision Support Interventions and Predictive Models
a. Background
b. Summary of Proposals
c. Proposed Requirements for Decision Support Interventions (DSI) Certification Criterion
d. Proposed Updates to Real World Testing Condition for CDS Criterion
6. Synchronized Clocks Standard

a. Background
b. Justification
7. Standardized API for Patient and Population Services
a. Native Applications and Refresh Tokens
b. FHIR United States Core Implementation Guide Version 5.0.1
c. FHIR Endpoint for Service Base URLs
d. Access Token Revocation
e. SMART App Launch 2.0
8. Patient Demographics and Observations Certification Criterion in § 170.315(a)(5)
9. Updates to Transitions of Care Certification Criterion in § 170.315(b)(1)
10. Patient Requested Restrictions Certification Criterion
a. Patient Right to Request a Restriction New Criterion – Primary Proposal
b. Alignment with Adopted Standards – Alternate Proposals and Request for Information
c. Alignment with Applicable Law – Request for Information
11. Requirement for Health IT Developers to Update their Previously Certified Health IT
D. Assurances Condition and Maintenance of Certification Requirements
1. Condition of Certification
2. Maintenance of Certification Requirements
E. Real World Testing – Inherited Certified Status
F. Insights Condition and Maintenance of Certification
1. Background and Purpose
2. Insights Condition – Proposed Measures
3. Insights Condition and Maintenance of Certification Requirements
4. Insights Condition and Maintenance of Certification's Process for Reporting
G. Requests for Information
1. Laboratory Data Interoperability Request for Information
a. Background
b. Request for Information
2. Request for Information on Pharmacy Interoperability Functionality within the ONC Health IT Certification Program including Real-Time Prescription Benefit Capabilities
a. Background
b. Request for Information
c. Real-Time Prescription Benefit Certification Criterion
d. Health IT Ecosystem for Pharmacy Interoperability
3. FHIR Standard
a. FHIR Subscriptions Request for Information
b. Clinical Decision Support Hooks Request for Information
c. FHIR Standard for Scheduling Request for Information
d. SMART Health Links Request for Information
IV. Information Blocking Enhancements
A. Defined Terms
1. Offer Health Information Technology or Offer Health IT
a. Exclusion of Certain Funding Subsidy Arrangements from *Offer* Definition
b. Implementation and Use Activities That Are Not an Offering
c. Consulting and Legal Services Exclusion from *Offer* Definition
2. Health IT Developer of Certified Health IT: Self-developer Health Care Providers
3. Information Blocking Definition
B. Exceptions
1. Infeasibility
a. Infeasibility Exception – Uncontrollable Events Condition
b. Third Party Seeking Modification Use
c. Manner Exception Exhausted

2. Manner Exception – TEFCA Reasonable and Necessary Activities
a. Background
b. TEFCA Condition for the "Manner" Exception
C. Information Blocking Requests for Information
1. Additional Exclusions from Offer Health IT – Request for Information
2. Possible Additional TEFCA Reasonable and Necessary Activities – Request for Information
3. Health IT Capabilities for Data Segmentation and User/Patient Access – Request for Information
V. Incorporation by Reference
VI. Response to Comments
VII. Collection of Information Requirements
A. Independent Entity
B. Health IT Developers
C. ONC-ACBs
VIII. Regulatory Impact Statement
A. Statement of Need
B. Alternatives Considered
C. Overall Impact
1. Executive Orders 12866 and 13563 – Regulatory Planning and Review Analysis
a. Costs and Benefits
b. Accounting Statement and Table
D. Regulatory Flexibility Act
E. Executive Order 13132 – Federalism
F. Unfunded Mandates Reform Act of 1995

Regulation Text

I. Executive Summary

A. Purpose of Regulatory Action

The Secretary of Health and Human Services has delegated responsibilities to ONC for the implementation of certain provisions in Title IV of the 21st Century Cures Act (Pub. L. 114-255, Dec. 13, 2016) (Cures Act) including: the Electronic Health Record (EHR) Reporting Program condition and maintenance of certification requirements under the ONC Health IT Certification Program (Program) and identifying reasonable and necessary activities that do not constitute information blocking.[1] ONC is responsible for implementation of certain provisions of the Health Information Technology for Economic and Clinical Health Act (Pub. L. 111-5, Feb. 17. 2009) (HITECH Act) of 2009 including, among other things: requirements that the National

[1] Reasonable and necessary activities that do not constitute information blocking, also known as information blocking exceptions, are identified in 45 CFR part 171 subparts B and C. ONC's official website, HealthIT.gov, offers a variety of resources on the topic of Information Blocking, including fact sheets, recorded webinars, and frequently asked questions. To learn more, please visit: https://www.healthit.gov/topic/information-blocking/.

Coordinator perform duties consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information and that promotes a more effective marketplace, greater competition, and increased consumer choice, among other goals; and requirements to keep or recognize a program or programs for the voluntary certification of health information technology. This proposed rule would fulfill statutory requirements; provide transparency; advance equity, innovation, and interoperability; and support the access, exchange, and use of electronic health information (EHI). Transparency regarding healthcare information and activities— as well as the interoperability and electronic exchange of health information—are all in the best interest of the patient and are central to the efforts of the Department of Health and Human Services to enhance and protect the health and well-being of all Americans.

In addition to fulfilling the HITECH Act's and Cures Act's requirements described above and advancing interoperability, the proposed rule would contribute to fulfilling Executive Orders (E.O.) 13994, 13985, 14036, 14058, and 14091. The President issued E.O. 13994 on January 21, 2021, to ensure a data-driven response to COVID-19 and future high-consequence public health threats. The Cures Act and the information blocking provisions in the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (85 FR 25642) (ONC Cures Act Final Rule) have enabled critical steps to making data available across the healthcare system. The proposed update in this proposed rule to adopt the United States Core Data for Interoperability Standard Version 3 (USCDI v3) would promote the establishment and use of interoperable data sets of EHI for interoperable health data exchange. As discussed in section III.C.1, USCDI v3 would facilitate the gathering, sharing, and publication of data for use in public health and emergency response (e.g., the COVID-19 pandemic) by capturing and promoting the sharing of key data elements related to public health. The proposed updates to Application Programming Interfaces (APIs) Conditions and Maintenance of Certification requirements, as discussed in section III.C.7, would continue ONC's efforts to develop and

standardize APIs and would help individuals and other authorized health care providers, including those engaged in public health, to securely access EHI through the broader adoption of standardized APIs.[2, 3] Additionally, the proposed rule would adopt consensus-based, industry-developed health IT standards for certified Health IT Modules to support electronic case reporting. As discussed in section III.C.4, this would, among other benefits, facilitate faster and more efficient disease tracking and case management. It also would provide more timely and complete data than manual or non-standardized reporting. In addition to proposing new standards to support public health initiatives, we also request comment and seek input from the public in section III.G regarding health IT standards that could be adopted within the Program to strengthen and advance laboratory interoperability.

We are committed to advancing health equity, and this proposed rule is consistent with E.O. 13985 of January 20, 2021, Advancing Racial Equity and Support for Underserved Communities Through the Federal Government[4] and E.O. 14091 of February 16, 2023, Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government.[5] Section 1 of E.O. 13985 states that "the Federal Government should pursue a comprehensive approach to advancing equity for all, including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality." Section 1 of E.O. 13985 also states that because "advancing equity requires a

---

[2] ONC. (2022, October 18). *API Resource Guide*. ONC Health IT Certification Program API Resource Guide. Retrieved March 16, 2023, from https://onc-healthit.github.io/api-resource-guide/.

[3] Section 4002 of the 21st Century Cures Act (Cures Act) establishes a condition of certification that requires health IT developers to publish application programming interfaces (APIs) that allow "health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law." The Cures Act's API Condition of Certification requirement also states that a developer must, through an API, "provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws." The API Conditions and Maintenance of Certification requirements and certification criteria are identified in 45 CFR part 170.

[4] United States, Executive Office of the President [Joseph Biden]. Executive Order 13985: Advancing Racial Equity and Support for Underserved Communities Through the Federal Government. Jan 20, 2021. 86 FR 7009-7013, https://www.federalregister.gov/documents/2021/01/25/2021-01753/advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government.

[5] United States, Executive Office of the President [Joseph Biden]. Executive Order 14091: Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government. Feb 16, 2023. 88 FR 10825-10833, https://www.federalregister.gov/documents/2023/02/22/2023-03779/further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal.

systematic approach to embedding fairness in decision-making processes, executive departments and agencies must recognize and work to redress inequities in any policies and programs that serve as barriers to equal opportunity." As noted above, we propose to adopt USCDI v3. If finalized, the adoption of USCDI v3 would update the USCDI standard to include data elements such as sexual orientation and social determinants of health, as discussed in sections III.C.1 and III.C.8 of this proposed rule. Expanding the data elements included in USCDI would increase the amount and type of data available to be used and exchanged through certified health IT. These proposed updates could help capture more accurate and complete patient characteristics that are reflective of patient diversity and could potentially help data users address disparities in health outcomes for all patients, including those who may be marginalized and underrepresented. The use of USCDI v3 would also support data users' abilities to identify, assess, and analyze gaps in care, which could in turn be used to inform and address the quality of healthcare through interventions and strategies. This could lead to better patient care, experiences, and health outcomes.

As discussed in section III.C.1.c, the proposal to adopt USCDI v3 also supports the concept of "health equity by design," where health equity considerations are identified and incorporated from the beginning and throughout the technology design, build, and implementation process, and health equity strategies, tactics, and patterns are guiding principles for developers, enforced by technical architecture, and built into the technology at every layer. If the proposal to adopt USCDI v3 is finalized, certified health IT products and capabilities should be designed with a foundational approach to promote equity. As a result, by their very design, certified health IT and the workflows around them should support equity and efforts to reduce disparities.

E.O. 14091 of Feb. 16, 2023, builds upon previous equity-related E.O.s, including E.O. 13985. Section 1 of E.O. 14091 requires the Federal Government to "promote equity in science and root out bias in the design and use of new technologies, such as artificial intelligence."

Section 8 of E.O. 14091 requires agencies to "prevent and address discrimination and advance equity for all" and to "consider opportunities to prevent and remedy discrimination, including by protecting the public from algorithmic discrimination."

This proposed rule would revise the existing clinical decision support (CDS) certification criterion by proposing a "Decision Support Interventions" (DSIs) certification criterion to keep pace with advances in software that developers of certified health IT enable or interface with to aid decision-making in healthcare. As discussed in section III.C.5, this criterion would also advance health equity by design by making it known to users of certified Health IT Modules certified to the criterion whether demographic, social determinants of health assessment data are used in DSIs. Finally, these proposals would: (1) establish a definition for algorithm-based, "predictive" DSIs; (2) require certified Health IT Modules certified to the criterion that enable or interface with predictive DSIs to enable users to review information about additional source attributes relevant to health equity, among other purposes, (3) require developers of certified Health IT Modules certified to the criterion to employ or engage in intervention risk management practices for all predictive DSIs that the developers' certified Health IT Modules enable or interface; and (4) make summary information regarding these practices available publicly.

Together, these proposed requirements should improve transparency, promote trustworthiness, and incentivize the development and wider use of fair, appropriate, valid, effective, and safe predictive DSIs to aid decision-making. The resulting information transparency would enable users, including health care providers, to scrutinize these technologies and would increase public trust and confidence in these technologies. The resulting information transparency could expand the use of these technologies in safer, more appropriate, and more equitable ways. This transparency would also inform wider discussions across industry and academia regarding how to evaluate and communicate performance related to predictive decision support interventions.

President Biden's E.O. 14036, Promoting Competition in the American Economy, issued on July 9, 2021, established a whole-of-government effort to promote competition in the American economy and reaffirmed the policy stated in E.O. 13725 of April 15, 2016 (Steps to Increase Competition and Better Inform Consumers and Workers to Support Continued Growth of the American Economy).[6] This proposed rule would foster competition by advancing foundational standards for certified API technology, which enable—through applications (apps) and without special effort—improved legally permissible sharing of EHI among clinicians, patients, researchers, and others. As described in section III.C.7, competition would be advanced through these improved API standards that can help individuals connect to their information and can help authorized health care providers involved in the patient's care to securely access information. For example, these standards are designed to foster an ecosystem of new applications that can connect through the API technology to provide patients with improved electronic access to EHI and more choices in their health care providers. This is similar to how APIs have impacted other sectors of the economy, such as travel, banking, and commerce.

Further, as described in section IV, this proposed rule would provide enhancements to support information sharing under the information blocking regulations and promote innovation and competition, as well as address market consolidation. As we have noted, addressing information blocking is critical for promoting innovation and competition in health IT and for the delivery of healthcare services to individuals. In both the ONC Cures Act Proposed (84 FR 7508) and Final (85 FR 25790 through 25791) Rules, we discussed how the information blocking provisions provide a comprehensive response to the issues identified by empirical and economic research that suggested that information blocking may weaken competition, encourage consolidation, and create barriers to entry for developers of new and innovative applications and

[6] United States, Executive Office of the President [Joseph Biden]. Executive Order 14036: Promoting Competition in the American Economy. Jul 9, 2021. 86 FR 36987-36999, https://www.federalregister.gov/documents/2021/07/14/2021-15069/promoting-competition-in-the-american-economy.

technologies that enable more effective uses of EHI to improve population health and the patient experience.[7] We explained that the information blocking provision of the Public Health Service Act (PHSA) itself expressly addresses practices that impede innovation and advancements in EHI access, exchange, and use, including care delivery enabled by health IT (section 3022(a)(2)(C)(ii) of the PHSA). Actors subject to the information blocking provisions may, among other practices, attempt to exploit their control over interoperability elements to create barriers to entry for competing technologies and services that offer greater value for health IT customers and users, provide new or improved capabilities, and enable more robust access, exchange, and use of electronic health information (EHI) (85 FR 25820).[8] Information blocking may also harm competition not just in health IT markets, but also in markets for healthcare services (85 FR 25820). In the ONC Cures Act Final Rule, we described practices that dominant market providers may leverage and use to control access and use of their technology, resulting in technical dependence and possibly leading to barriers to entry by would-be competitors, as well as making some market providers vulnerable to acquisition or inducement into arrangements that enhance the market power of incumbent providers to the detriment of consumers and purchasers of healthcare services (85 FR 25820). The implementation of the new information blocking provisions proposed in section IV of this proposed rule would promote innovation, encourage market competition, and address consolidation in the interest of the patient to advance interoperability, improve transparency, and support the access, exchange, and use of electronic health information.

---

[7] *See*, e.g., Martin Gaynor, Farzad Mostashari, and Paul B. Ginsberg, Making Health Care Markets Work: Competition Policy for Health Care, 16-17 (Apr. 2017), available at http://heinz.cmu.edu/news/news-detail/index.aspx?nid=3930; Diego A. Martinez et al., A Strategic Gaming Model For Health Information Exchange Markets, Health Care Mgmt. Science (Sept. 2016). ("[S]ome healthcare provider entities may be interfering with HIE across disparate and unaffiliated providers to gain market advantage.") Niam Yaraghi, A Sustainable Business Model for Health Information Exchange Platforms: The Solution to Interoperability in Healthcare IT (2015), available at http://www.brookings.edu/research/papers/2015/01/30-sustainable-business-model-health-information-exchange-yaraghi;; Thomas C. Tsai Ashish K. Jha, Hospital Consolidation, Competition, and Quality: Is Bigger Necessarily Better? 312 J. AM. MED. ASSOC. 29, 29 (2014).

[8] See also Martin Gaynor, Farzad Mostashari, and Paul B. Ginsberg, Making Health Care Markets Work: Competition Policy for Health Care, 16-17 (Apr. 2017), available at http://heinz.cmu.edu/news/news-detail/index.aspx?nid=3930.

Lastly, in support of E.O. 14058, Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government, issued on December 16, 2021, we are committed to advancing the equitable and effective delivery of services with a focus on the experience of individuals, health IT developers, and health care providers.[9] As required by section 4002 of the Cures Act and included in the ONC Cures Act Final Rule (85 FR 25717), we established certain Conditions and Maintenance of Certification requirements, which express initial and ongoing requirements for health IT developers and their certified Health IT Module(s) under the Program. This proposed rule would implement the EHR Reporting Program Condition and Maintenance of Certification requirement outlined in the Cures Act by establishing a new Insights Condition and Maintenance of Certification ("Insights Condition") within Program. As discussed in section III.F, the implementation of the Insights Condition would provide transparent reporting to address information gaps in the health IT marketplace and provide insights on the use of specific certified health IT functionalities. The implementation of this new Condition and Maintenance of Certification requirement would allow ONC to gain understanding of the use of health IT and would provide ONC with information about consumers' experience with certified health IT.

We also strive to improve federal agency coordination. ONC works with the Centers for Medicare & Medicaid Services (CMS) to ensure that our own certification timelines complement timelines for CMS programs that reference ONC regulations, such as the Medicare Promoting Interoperability Program and the Promoting Interoperability performance category of the Merit-based Incentive Payment System (MIPS). In the interest of clarity and cohesion among HHS components, we have proposed to align some of our compliance dates to the calendar year for consistency with calendar-year based performance periods in CMS programs when participants

[9] United States, Executive Office of the President [Joseph Biden]. Executive Order 14058: Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government. Dec 13, 2021. 86 FR 71357-71366, https://www.federalregister.gov/documents/2021/12/16/2021-27380/transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government.

may be required to use updated certified health IT. We believe this approach reduces confusion for participants in these programs and better serves the public interest.

B. Summary of Major Provisions

1. ONC Health IT Certification Program Updates

a. "The ONC Certification Criteria for Health IT" and Discontinuing Year Themed "Editions"

Section 3001(c)(5) of the PHSA provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health IT. ONC first introduced the concept of an "edition" of ONC health IT certification criteria in 2012. In 2012, we stated that we would refer to the certification criteria adopted in §§ 170.302, 170.304, and 170.306 collectively as the "2011 Edition EHR certification criteria" and that the certification criteria adopted in § 170.314 would be referred to as the "2014 Edition EHR certification criteria" (77 FR 13836). In 2015, we issued a final rule, "2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications," (2015 Edition Final Rule) and adopted the "2015 Edition Health IT Certification Criteria" (80 FR 62602). We codified the 2015 Edition certification criteria in § 170.315 to set them apart from other editions of certification criteria (80 FR 62608). In 2020, we published the ONC Cures Act Final Rule (85 FR 25642) and adopted updates to the 2015 Edition. These updates included new certification criteria, standards, and requirements, as well as incremental revisions to existing 2015 Edition certification criteria to better enable interoperability and the access, exchange, and use of electronic health information (85 FR 25664-65). Because we did not adopt a wholesale new edition of certification criteria in a different CFR section, we retained the overall 2015 Edition title for the changes included in the ONC Cures Act Final Rule and made specific timebound compliance changes within certification criteria.

Subsequent to publication of the ONC Cures Act Final Rule through public meetings and correspondence, we heard that the continued use and reference to the 2015 Edition inaccurately implied an age and outdatedness to the certification criteria we had adopted. More importantly, we heard significant positive feedback that the incremental approach to updates is generally beneficial as a long-term approach. Specifically, we heard that a consistent, transparent, incremental update cycle that includes the following features would be preferred by some: 1) regular updates to recognize standards advancement and an allowance for voluntary standards advancement between updates, 2) incremental updates rather than wholesale certified Health IT Module certification criteria overhauls, 3) a predictable timeline for updates based on standards development cycles with reasonable development timelines, and 4) a reasonable development timeline for any new criterion based on the specific development needs.

For these reasons, we no longer believe that it is helpful or necessary to maintain an "edition" naming convention or to adopt entirely new editions of certification criteria to encapsulate updates over time. Instead, we believe there should be a single set of certification criteria, which will be updated in an incremental fashion in closer alignment to standards development cycles and regular health IT development timelines. Therefore, in section III.A, we propose to rename all criteria within the Program simply as "ONC Certification Criteria for Health IT." We believe maintaining a single set of "ONC Certification Criteria for Health IT" would create more stability for the Program and for federal partners who reference the Program, as well as make it easier for developers of certified health IT to maintain their product certificates over time. This proposal to remove "editions" from the Program would also help users of certified health IT identify which certification criteria are necessary for their participation in other HHS programs, such as Medicare Promoting Interoperability Program and the Promoting Interoperability performance category of the MIPS. For example, users would only need to know that their Health IT Module is certified by ONC in accordance with the ONC Certification Criteria for Health IT for successful participation in MIPS, as compared to the

current state where they must also know if the Health IT Module complies with the 2014 Edition Certification Criteria, the 2015 Edition Certification Criteria, or the 2015 Edition Cures Update Certification Criteria.

In addition, we believe that this approach will have the benefit of reducing administrative burden for health IT developers with Health IT Modules certified through the Program. Previously, duplicative references to certification criteria across different year themed editions created administrative burden on developers as they had the effect of requiring health IT developers to seek an updated certificate attributed to the "new" duplicated certification criterion even in circumstances when the certification criterion remained substantively unchanged. Under this proposal, unchanged certification criteria would no longer be duplicated as separate criteria under multiple editions.

b. New and Revised Standards and Certification Criteria

i. The United States Core Data for Interoperability Standard Version 3 (USCDI v3)

In the ONC Cures Act Final Rule, ONC adopted the United States Core Data for Interoperability (USCDI) as a standard to replace the Common Clinical Data Set (CCDS) in several ONC certification criteria (85 FR 25670). We adopted USCDI Version 1 (USCDI v1) as a standard in § 170.213 and incorporated it by reference in § 170.299. The new USCDI v1 standard established a set of data classes and constituent data elements required to support interoperability nationwide. USCDI v1 is a required part of certain certification criteria updates that were made to the existing 2015 Edition Health IT Certification Criteria in the ONC's Cures Act Final Rule. These changes constitute the "2015 Edition Cures Update."

ONC also indicated in the ONC Cures Act Final Rule that we intended to establish and follow a predictable, transparent, and collaborative process to expand future versions of the USCDI, including providing the public with the opportunity to comment on the USCDI's expansion (85 FR 25670). ONC established a process, including creating the ONC New Data

Element and Class (ONDEC) submission system,[10] which provides the public with the opportunity to submit new data elements to be considered for inclusion in future versions of USCDI. Following this established process, ONC published USCDI Version 2 (USCDI v2) in July 2021[11] and finalized and released USCDI Version 3 (USCDI v3) in July 2022.[12] Both USCDI v2 and USCDI v3 contain new data elements and data classes beyond what was included in USCDI v1. USCDI v3 contains all data elements and classes added in USCDI v2.

Because USCDI is the standard for data required to be accessible through certified health IT for numerous certification criteria, expanding the data elements and data classes included in USCDI increases the amount of data available to be used and exchanged for patient care. To advance interoperability, in section III.C.1, ONC proposes to add the newly released USCDI v3 in § 170.213(b). We propose that USCDI v1 would remain in regulation and now be codified in § 170.213(a) and we propose to add USCDI v3 to § 170.213 (to be codified as § 170.213(b)). We also propose to incorporate by reference USCDI v3 in § 170.299 as of the effective date of the final rule. In addition, we propose that the USCDI v1 (July 2020 Errata) in the USCDI standard in § 170.213(a) will expire on January 1, 2025. Under this proposal, both versions would be referenced as applicable in the USCDI standard in § 170.213 for the time period up to and including December 31, 2024.

ii. C-CDA Companion Guide Updates

In section III.C.2, we propose to adopt the HL7® CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes STU Companion Guide, Release 3 – US Realm (C-CDA Companion Guide R3) in § 170.205(a)(6). The C-CDA Companion Guide R3 provides supplemental guidance and additional technical clarification for specifying data in the C-CDA Release 2.1, including data specified in USCDI v2. However, it is our understanding that HL7 is

---

[10] ONC. (2020, July 27). USCDI ONDEC. Retrieved March 16, 2023, from https://www.healthit.gov/isa/ONDEC).
[11] ONC. (2021, July 2). *United States Core Data for Interoperability (USCDI)*. Interoperability Standards Advisory (ISA). Retrieved March 16, 2023, from https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi#uscdi-v2.
[12] United States Core Data for Interoperability (USCDI)," Interoperability Standards Advisory (ISA) (ONC, July 5, 2022), https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi#uscdi-v3.

working on updating the C-CDA Companion Guide for USCDI v3. If the updated C-CDA Companion Guide Release 4 (R4) is published before the date of publication of the final rule, it is our intention to consider adopting the updated Companion Guide that provides guidance and clarifications for specifying data in USCDI v3.

iii. "Minimum Standards" Code Sets Updates

In the 2015 Edition Final Rule, we established a policy of adopting newer versions of "minimum standards" code sets that update frequently (80 FR 62612). Adopting newer versions of these code sets enables improved interoperability and implementation of health IT with minimal additional burden (77 FR 54170). If adopted, newer versions of these minimum standards code sets would serve as the baseline for certification, and developers of certified health IT would be able to use newer versions of these adopted standards on a voluntary basis. Because these code sets are updated frequently, we will consider whether it may be more appropriate to adopt a version of a minimum standards code set issued after publication of this proposed rule but before publication of a final rule. In section III.C.3, we propose to adopt newer versions of the following minimum standards code sets:

- § 170.207(a) – Problems
- § 170.207(c) – Laboratory tests
- § 170.207(d) – Medications
- § 170.207(e) – Immunizations
- § 170.207(f) – Race and ethnicity
- § 170.207(m) – Numerical references
- § 170.207(n) – Sex
- § 170.207(o) – Sexual orientation and gender information
- § 170.207(p) – Social, psychological, and behavioral data
- § 170.207(r) – Provider type
- § 170.207(s) – Patient insurance

In addition to updating the minimum standards code sets listed above, we propose to update some of the certification criteria that reference those minimum standards. These criteria include § 170.315(a)(5)(i)(A)(*1*) and (*2*), (a)(5)(i)(C) through (E), (a)(12), (b)(1)(iii)(B)(*2*), (b)(1)(iii)(G)(*3*), (b)(6)(ii)(B)(*2*), (c)(4)(iii)(C), (c)(4)(iii)(E), (c)(4)(iii)(G) through (I), (f)(1)(i)(B) and (C), (f)(3)(ii), and (f)(4)(ii).

We also propose to change the heading of § 170.207(o) from "sexual orientation and gender identity" to "sexual orientation and gender information" to acknowledge that § 170.207(o) may include standard code sets to support other gender related data items.

iv. Electronic Case Reporting

In section III.C.4 of this proposed rule, we propose to revise the "transmission to public health agencies – electronic case reporting" criterion in § 170.315(f)(5) to adopt consensus-based, industry-developed electronic standards and implementation guides (IGs) to replace all functional, descriptive requirements in the present criterion in § 170.315(f)(5). These standards are proposed to support the following requirements for Health IT Modules certified to § 170.315(f)(5): (i) create a case report for electronic transmission; (ii) consume and process a case report response; and (iii) consume and process electronic case reporting trigger codes and parameters. We note that these electronic standards are standards-based representations of the functional requirements described in the existing criterion in § 170.315(f)(5) as described in section III.C.4 of this preamble.

v. Decision Support Interventions and Predictive Models

In section III.C.5 of this proposed rule, we propose the certification criterion, "decision support interventions (DSI)" in § 170.315(b)(11). The DSI criterion is a revised certification criterion as it serves as both an iterative and replacement criterion for the "clinical decision support (CDS)" criterion in § 170.315(a)(9). This criterion would reflect an array of contemporary functionalities, data elements, and software applications, including the use of

predictive models or algorithms, that certified Health IT Module(s) enable or interface with to aid decision-making in healthcare.

We propose to adopt a new definition for "predictive decision support intervention," in § 170.102, and we propose that developers of certified health IT with Health IT Module(s) certified to the criterion we propose in § 170.315(b)(11) that enable or interface with predictive DSIs would be subject to requirements to provide transparency of predictive DSIs. Specifically, we propose that Health IT Modules that enable or interface with predictive DSIs enable a user to review predictive DSI "source attribute" information through the Health IT Module. We also propose that developers of certified health IT with Health IT Modules that enable or interface with predictive DSIs employ or engage in "intervention risk management" practices. We also propose that summary information regarding these intervention risk management practices be made available via a publicly accessible hyperlink. Together, our proposals for predictive DSI-specific source attributes and intervention risk management practices information are intended to provide appropriate information to help guide medical decisions at the time and place of care, consistent with 42 U.S.C. § 300jj–11(b)(4).

We propose that Health IT Modules certified to § 170.315(b)(11) enable users to provide feedback regarding DSI information displayed through the Health IT Module, and that such Health IT Modules make available such feedback data for export in a computable format.

We propose that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) comply with these new requirements by December 31, 2024. For the intervening time between finalization of this proposed rule and December 31, 2024, we propose to add § 170.315(a)(9) to the list of applicable certification criteria for the real-world testing Condition and Maintenance of Certification requirement in § 170.405(a), thus requiring developers of certified health IT with Health IT Module(s) certified to § 170.315(a)(9) or § 170.315(b)(11) to participate in real world testing plan and results submission.

Finally, we propose to update the Base EHR definition in § 170.102 to include an option of either the existing "clinical decision support (CDS)" version of the criterion in § 170.315(a)(9) or the revised "decision support interventions" criterion in § 170.315(b)(11) for the period up to and including December 31, 2024, and to include only "decision support interventions" in § 170.315(b)(11) on and after January 1, 2025. We discuss in section III.C.5.d of this preamble proposals that would constitute changes to the CDS criterion, as the new DSI criterion. We describe how much of the structure and requirements are duplicated across these criteria and reflect the capabilities included in the CDS criterion with which Program participants have years of familiarity and can find, for comparison purposes, in § 170.315(a)(9).

vi. Synchronized Clocks Standard

We propose in section III.C.6 to remove the current named specification for clock synchronization, which is Network Time Protocol (NTP v4 of RFC 5905), in § 170.210(g), based on public feedback and reflective of contemporary norms within the industry. Additionally, we propose to keep the requirement for any network time protocol (NTP) standard to be present, though any NTP standard could be used.

vii. Standardized API for Patient and Population Services

We propose in section III.C.7 to revise the "standardized API for patient and population services" certification criterion in § 170.315(g)(10) in several ways. We propose to require a certified Health IT Module's authorization server to issue a refresh token according to the implementation specification adopted in § 170.215(c). The token should be valid for a period of no less than three months and will apply to all applications using the "confidential app" profile for both first time and subsequent connections.

We also propose to adopt the FHIR US Core Implementation Guide STU version 5.0.1 in § 170.215(b)(1)(ii). Based on the annual US Core release cycle, we believe US Core IG v6.0.0 will be published before ONC issues a final rule.[13] Therefore, it is our intent to consider adopting

[13] http://hl7.org/fhir/us/core/history.html.

the updated US Core IG v6.0.0 that supports the data elements and data classes in USCDI v3 since we propose to adopt USCDI v3 in this rule. Health IT systems that adopt this version of the US Core IG can provide the latest consensus-based capabilities for providing access to USCDI data classes and elements using a FHIR API.

Additionally, we propose to amend the API Condition and Maintenance of Certification requirements by adding the requirement that Certified API Developers with patient-facing apps must publish their service base URLs for all customers, regardless of whether the certified Health IT Modules are centrally managed by the Certified API Developer or locally deployed by an API Information Source, according to a specified format.

We also propose to revise the requirement in § 170.315(g)(10)(vi) to specify that Health IT Modules presented for certification that allow short-lived access tokens to expire, in lieu of immediate access token revocation, must have such access tokens expire within one hour of the request. This revised requirement would align with industry standard practice for short-lived access tokens, would provide clarity and consistent expectations that developers revoke access or expire access privileges within one hour of a request, and would offer patients an assurance that an application's access to their data would be revoked or expired within one hour of a request.

We propose to adopt the Substitutable Medical Applications, Reusable Technologies (SMART) Application Launch Framework Implementation Guide Release 2.0.0 (SMART v2 Guide) in § 170.215(c)(2), which would replace SMART v1 Guide as the standard in § 170.215(a)(3) (proposed in this rule as § 170.215(c)(1)). The SMART v2 Guide iterates on the features of the SMART v1 Guide by including new features and technical revisions based on industry consensus, including features that reflect security best practices. We propose that the availability of the SMART v1 Guide to be adopted as a standard in the Program would expire on January 1, 2025. After this time, the SMART v2 Guide would be the only version of the IG available for use in the Program.

viii. Patient Demographics and Observations Certification Criterion in § 170.315(a)(5)

In section III.C.1 of this proposed rule, we introduce proposals to change certain data elements in USCDI, namely Sex (Assigned at Birth), Sexual Orientation, and Gender Identity, that are also data elements in § 170.315(a)(5). We propose these changes to reflect public feedback that the standards and terms used to represent these data elements needed to be updated. Therefore, to ensure consistency, in section III.C.8 of this preamble, we propose to change the name of the certification criterion in § 170.315(a)(5) from "demographics" to "patient demographics and observations." Additionally, in order to ensure consistent capture of these data elements across health IT, we propose in section III.C.8 to carry these changes into their respective data elements in § 170.315(a)(5).

We propose to replace the specific codes sets referenced in § 170.315(a)(5)(i)(D) and (E), Sexual Orientation and Gender Identity, respectively, with the Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT ®) code set, as referenced in the standard proposed in § 170.207(o)(3). We propose that the adoption of the code sets referenced in § 170.207(n)(1) would expire on January 1, 2026, and we also propose that health IT developers can continue to use the specific codes in the current terminology standard until December 31, 2025, in order to provide adequate time for health IT systems to transition to the updated terminology standards.

As also discussed in section III.C.1 of this proposed rule, we have taken note of efforts to develop clinically relevant ways of identifying a patient's sex based on observations, to be used by a patient's clinician when considering or evaluating diagnostic or therapeutic services in areas such as radiology, laboratory, and genetic testing. The concept "Sex For Clinical Use" (SFCU) is seen as a valuable tool in addressing these concerns and therefore important for clinical capture. We also propose to add SFCU as a new data element in § 170.315(a)(5)(i)(F). Additionally, we propose to add new data elements "Name to Use" in § 170.315(a)(5)(i)(G) and "Pronouns" in §

170.315(a)(5)(i)(H), to facilitate data capture that supports providers' ability to provide culturally competent care for their patients.

ix. Updates to Transitions of Care Certification Criterion in § 170.315(b)(1)

We propose in section III.C.9 to update the "transitions of care" certification criterion (§ 170.315(b)(1)) to align it with changes proposed in § 170.213, including the proposed adoption of USCDI v3 in § 170.213(b)). This change would ensure that Health IT Modules certified to § 170.315(b)(1) are capable of accessing, exchanging, and using USCDI data elements referenced in § 170.213.

x. Patient Requested Restrictions Certification Criterion

We believe that individuals should be provided a reasonable opportunity and technical capability to make informed decisions about the collection, use, and disclosure of their electronic health information. The Health Insurance Portability and Accountability Act (HIPAA)[14] Privacy Rule[15] provides individuals with several legal, enforceable rights intended to empower them to be more active participants in managing their health information. We make several proposals in support of the HIPAA Privacy Rule's individuals' "right to request a restriction" on certain uses and disclosures of their PHI (*see also* 45 CFR 154.522(a)). We propose to adopt a new certification criterion, revise a certification criterion, and propose modifications for Health IT Modules certified to specific criteria under the Privacy and Security certification Framework.

We propose a new certification criterion in § 170.315(d)(14), an addition to ONC's Privacy and Security Certification Framework under the Program in § 170.550(h), and a revision to an existing criterion in § 170.315(e)(1) to support additional tools for implementing patient requested information privacy restrictions.

---

[14] Pub. L. 104-191,110 Stat. 1936 (August 21, 1996), codified at 42 U.S.C. 1320d-1320d8.
[15] 45 CFR part 160 and subparts A and E of part 164.

xi. Requirement for Health IT Developers to Update their Previously Certified Health IT

We propose to make explicit in the introductory text in § 170.315 that health IT developers voluntarily participating in the Program must update their certified Health IT Modules and provide that updated certified health IT to customers in accordance with the timelines defined for a specific criterion or standard included in § 170.315. More specifically, we propose in section III.C.11 that health IT developers with health IT certified to any of the certification criteria in § 170.315 would need to update their previously certified Health IT Modules to be compliant with any revised certification criterion adopted in § 170.315, including any new standards adopted in 45 CFR part 170 subpart B and capabilities included in the revised certification criterion. We further propose that health IT developers would also need to provide the updated heath IT to customers of the previously certified health IT according to the timelines established for that criterion and any applicable standards.

2. Assurances Condition and Maintenance of Certification Requirements

We propose in section III.D to establish additional Assurances Condition and Maintenance of Certification requirements. We propose as a Condition of Certification that a health IT developer must provide an assurance that it will not interfere with a customer's timely access to interoperable health IT certified under the Program. To support this assurance, we propose two accompanying Maintenance of Certification requirements. We propose that a health IT developer must update a Health IT Module, once certified to a certification criterion adopted in § 170.315, to all applicable revised certification criteria, including the most recently adopted capabilities and standards included in the revised certification criterion. We also propose that a health IT developer must provide all Health IT Modules certified to a revised certification criterion to its customers of such certified health IT. Additionally, we propose separate "timely access" or "timeliness" requirements for each of the two proposed Maintenance of Certification requirements above dictating by when a Health IT Module must be updated to revised

certification criteria and by when a Health IT Module certified to a revised certification criterion must be provided to the health IT developer's customers.

3. Real World Testing – Inherited Certified Status

Section 4002(a) of the Cures Act added a new Condition and Maintenance of Certification requirement that health IT developers must successfully test the real-world use of health IT for interoperability in the type(s) of setting(s) in which such technology would be marketed. Many health IT developers update their certified Health IT Module(s) on a regular basis leveraging the flexibility provided through ONC's Inherited Certified Status (ICS).[16] Because of the way that ONC issues certification identifiers, this updating can cause an existing certified Health IT Module to be recognized as new within the Program. Regular updating, especially on a frequent basis (such as quarterly or semi-annually) creates an anomaly that could result in existing certified Health IT Modules being inadvertently excluded from the real world testing reporting requirements.

In order to ensure that all developers continue to test the real world use of their technology as required, we propose in section III.E to eliminate this anomaly by requiring health IT developers to include in their real world testing results report the newer version of those certified Health IT Module(s) that are updated using Inherited Certified Status after August 31 of the year in which the plan is submitted. This will ensure that health IT developers fully test all applicable certified Health IT Module(s) as part of their real world testing requirements.

4. Insights Condition and Maintenance of Certification

The Cures Act specified requirements in section 4002(c) to establish an Electronic Health Record (EHR) Reporting Program to provide transparent reporting on certified health IT in the categories of interoperability, usability and user-centered design, security, conformance to

[16] ONC, Applicability Of Inherited Certified Status And Gap Certification (2016). https://www.healthit.gov/sites/default/files/policy/public_applicability_of_gap_certification_and_inherited_certified_status.pdf.

certification testing, and other categories, as appropriate to measure the performance of EHR technology. The Cures Act also specified that a health IT developer be required, as a Condition and Maintenance of Certification requirement under the ONC Health IT Certification Program, to submit responses to reporting criteria in accordance with the Electronic Health Record Reporting Program established with respect to all certified technology offered by such developer. For clarity purposes, we intend to refer to the Condition and Maintenance of Certification associated with the "EHR Reporting Program" as the "Insights" Condition and Maintenance of Certification (also referred to as the "Insights Condition") throughout this proposed rule. We believe this descriptive name captures the essence of this requirement and will help avoid confusion that might occur through use of the term "EHR Reporting Program."

We propose in section III.F to adopt nine reporting measures for developers of certified health IT that focus initially on the interoperability category, emphasizing four areas of interoperability: individuals' access to electronic health information, public health information exchange, clinical care information exchange, and standards adoption and conformance. Through this first set of proposed measures, ONC intends to provide insights on the interoperability category specified in the Cures Act. We intend to explore the other Cures Act categories (security, usability and user-centered design, conformance to certification testing, and other categories to measure the performance of EHR technology) in future years.

We also propose in section III.F to implement the Insights Condition and Maintenance of Certification requirements in § 170.407 in two phases, where some of the measures will be required to be reported earlier than others. For each proposed measure, we have included information on the rationale for proposing the measure, the proposed numerators and denominators, and other key topics. Overall, the intent of the Insights Condition is to provide transparent reporting, address information gaps in the health IT marketplace, and provide insights on the use of health IT.

5. Information Blocking Enhancements

We propose in section IV.A to define what it means to "offer health information technology" or "offer health IT" for purposes of the information blocking regulations in 45 CFR part 171. This definition of what it means to *offer health IT* would, as proposed, narrow the applicability of the health IT developer of certified health IT definition. While the definition of *offer health IT* proposed at 45 CFR 171.102 would generally continue to include holding out for sale, selling, or otherwise supplying certified health IT to others on commercial or other terms, it would carve out by explicit exclusion the provision of funding for obtaining or maintaining certified health IT. The proposed definition would also explicitly codify that we do not interpret health care providers or other health IT users to offer health IT when they engage in certain activities customary and common amongst both health care providers that purchase certified health IT from a commercial developer or reseller and health care providers that self-develop certified health IT. Activities we propose to codify as explicitly excluded from the definition of what it means to *offer health IT* include implementing APIs or portals for clinician or patient access as well as the issuance of login credentials allowing licensed healthcare professionals who are in independent practice to use a hospital or other healthcare facility's EHR to furnish and document care to patients in the hospital or other healthcare facility. We also include a proposal to potentially exclude from what it means to *offer health IT* the inclusion of health IT in a package of items, supplies, facilities, and services that a management consultant handles for a clinician practice or other health care provider in a comprehensive ("turn key") package of services for administrative or operational management of the clinician practice or other health care provider (see section IV.A.1.c, below). Finally, we seek comment on the proposed definition of *offer health IT* and whether we should consider additional exclusions.

We also propose in section IV.A to modify the *health IT developer of certified health IT* definition so that it is clear that health care providers who self-develop certified health IT would continue to be excluded from this definition if they supply their self-developed certified health IT to others under arrangements excluded from the definition of what it means to *offer health IT*.

This would treat self-developer health care providers who supply use of their self-developed certified health IT to others under arrangements, or in the course of activities, excluded from the proposed *offer health IT* definition in the same way that we treat health care providers who supply commercial developers' certified health IT under arrangements, or in the course of activities, excluded from the *offer health IT* definition.

We propose in section IV.A to revise the text of § 171.103, the information blocking definition, to remove paragraph (b) (*see* § 171.103(b)). Paragraph (b) established the period of time during which electronic health information (EHI) for purposes of the information blocking definition (§ 171.103) was limited to a subset of electronic health information (EHI) that was identified by the data elements represented in the USCDI standard adopted in 171.213. The end date of that period of time, October 5, 2022, has passed. On and after October 6, 2022, the scope of EHI for purposes of the information blocking definition (§ 171.103) is EHI as defined in § 171.102 and thus paragraph (b) of § 171.103 is no longer needed.

We note that we do not propose to change the scope of EHI for purposes of the information blocking definition, only to update the CFR text to remove the paragraph specific to the period of time now passed. Similarly, because we included the same time period in reference to the scope of electronic health information in two paragraphs of the Content and Manner exception (§ 171.301(a)(1) and (2)), we propose to revise § 171.301 to remove from the regulatory text the existing § 171.301(a)(1) and (2) as no longer necessary.

We propose in section IV.B to revise the Infeasibility Exception codified in 45 CFR 171.204(a) by adding two new conditions and by revising one existing condition to further clarify when an actor's practice of not fulfilling a request for access, exchange, or use of EHI meets the condition. First, we propose to revise the "uncontrollable events" condition in § 171.204(a)(1) to further clarify when an actor's practice meets the uncontrollable events condition. Second, we propose to add two new conditions to be codified as subparagraphs (a)(3)

and (a)(4), and to therefore renumber the "infeasible under the circumstances" condition currently codified in § 171.204(a)(3) as (a)(5).

The first new infeasibility condition would apply to an actor's practice of denying a third party's request to enable use of EHI in order to modify EHI, including but not limited to creation and deletion functionality, provided the request is not from a health care provider requesting such use from an actor that is its business associate. The second new infeasibility condition would apply where an actor has exhausted the manner exception in § 171.301, including offering all alternative manners in accordance with § 171.301(b), and the actor does not currently provide a substantial number of individuals or entities similarly situated to the requestor with the same requested access, exchange, or use of the requested EHI.

We also seek comment on ways health IT can support EHI segmentation for access, exchange, and use of EHI; and particularly how the Program, through the certification of health IT to certain functionalities and/or standards, can support EHI segmentation for access, exchange, and use, including to assist health care providers with sharing EHI consistent with patient preferences and all laws applicable to the creation, use, and sharing of EHI.

Additionally, in section IV.B, we propose to add a Trusted Exchange Framework and Common Agreement (TEFCA) condition to the proposed revised and renamed Manner Exception, proposed to be codified in 45 CFR 171.301. This proposal aligns with a foundational policy construct underpinning the Manner Exception in that it facilitates an actor reaching agreeable terms with a requestor to fulfill an EHI request and acknowledges that certain agreements have been reached between these parties for the access, exchange, and use of EHI.

C. Costs and Benefits

E.O. 12866 on Regulatory Planning and Review and E.O.13563 on Improving Regulation and Regulatory Review direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects,

distributive impacts, and equity). Section 3(f) of Executive Order 12866 defines a "significant regulatory action" as an action that is likely to result in a rule that may: (1) have an annual effect on the economy of $100 million or more in any 1 year, or adversely and materially affecting a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local or Tribal governments or communities; (2) create a serious inconsistency or otherwise interfere with an action taken or planned by another agency; (3) materially alter the budgetary impacts of entitlement grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in the Executive Order. A regulatory impact analysis (RIA) must be prepared for major rules with significant effects as per section 3(f)(1)) ($100 million or more in any one year). OMB has determined that this proposed rule is a significant rule as the potential costs associated with this proposed rule could be greater than $100 million per year. Accordingly, we have prepared an RIA that to the best of our ability presents the costs and benefits of this proposed rule. We have estimated the potential monetary costs and benefits of this proposed rule for the health IT community, including costs and benefits as they relate to health IT developers, health care providers, patients, and the Federal Government (*i.e.,* ONC), and have broken those costs and benefits out by section. In accordance with E.O. 12866, we have included the RIA summary table as Table 35.

We note that we have rounded all estimates to the nearest dollar and that all estimates are expressed in 2021 dollars as it is the most recent data available to address all cost and benefit estimates consistently. The wages used to derive the cost estimates are from the May 2021 National Occupational Employment and Wage Estimates reported by the U.S. Bureau of Labor Statistics.[17] We also note that estimates presented in the following "Employee Assumptions and Hourly Wage," "Quantifying the Estimated Number of Health IT Developers and Products," and

[17] May 2021 National Occupational Employment and Wage Estimates, United States. U.S. Bureau of Labor Statistics. https://www.bls.gov/oes/current/oes_nat.htm.

"Number of End Users that Might Be Impacted by ONC's Proposed Regulations" sections are used throughout this RIA.

We estimate that the total annual cost for this proposed rule for the first year after it is finalized (including one-time costs), based on the cost estimates outlined above and throughout this RIA, would result in $742 million. The total undiscounted perpetual cost over a 10-year period for this proposed rule (starting in year three), based on the cost estimates outlined above, would result in $712 million. We estimate the total costs to health IT developers to be $742 million and estimate the government (ONC) costs to be between $62,000 to $124,000.

We estimate the total annual benefit for this proposed rule, based on the benefit estimates outlined above, would be on average $1.0 billion. We estimate the total undiscounted perpetual annual net benefit for this proposed rule (starting in year three), based on the estimates outlined above, would be $326 million.

II. Background

A. Statutory Basis

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), was enacted on February 17, 2009. The HITECH Act amended the Public Health Service Act (PHSA) and created "Title XXX—Health Information Technology and Quality" (Title XXX) to improve healthcare quality, safety, and efficiency through the promotion of health IT and electronic health information (EHI) exchange.

The 21st Century Cures Act, Pub. L. 114-255 (Cures Act), was enacted on December 13, 2016, to accelerate the discovery, development, and delivery of 21st century cures, and for other purposes. The Cures Act, through Title IV – Delivery, amended the HITECH Act by modifying or adding certain provisions to the PHSA relating to health IT.

Section 119 of Title I, Division CC of the Consolidated Appropriations Act, 2021, Pub. L. 116-260 (CAA), enacted on December 27, 2020, requires PDP sponsors of prescription drug

plans to implement one or more real-time benefit tools (RTBTs) that meet the requirements described in the statute, after the Secretary has adopted a standard for RTBTs and at a time determined appropriate by the Secretary. For purposes of the requirement to implement a real-time benefit tool in section 1860D-4(o)(1) of the Social Security Act, described above, the CAA provides that one of the requirements for an RTBT is that it is capable of integrating with electronic prescribing and EHR systems of prescribing healthcare professionals for the transmission of formulary and benefit information in real time to such professionals. The statute requires incorporation of RTBTs within both the Medicare Part D prescription drug program and the ONC Health IT Certification Program (Program). Specifically, the law amends the definition of a "qualified electronic health record" (qualified EHR) in section 3000(13) of the PHSA to require that a qualified EHR must include (or be capable of including) an RTBT.

1. Standards, Implementation Specifications, and Certification Criteria

The HITECH Act established two Federal advisory committees, the Health IT Policy Committee (HITPC) and the Health IT Standards Committee (HITSC). Each was responsible for advising the National Coordinator for Health Information Technology (National Coordinator) on different aspects of standards, implementation specifications, and certification criteria.

Section 4003(e) of the Cures Act amended sections 3002 and 3003 of the PHSA by replacing, in an amended section 3002, the HITPC and HITSC with one committee named the Health Information Technology Advisory Committee (Health IT Advisory Committee or HITAC). Section 3002(a) of the PHSA, as added by the Cures Act, establishes that the HITAC recommends to the National Coordinator policies and standards, implementation specifications, and certification criteria, relating to the implementation of a health information technology infrastructure, nationally and locally, that advances the electronic access, exchange, and use of health information. Further described in section 3002(b)(1) of the PHSA, this includes recommending to the National Coordinator a policy framework to advance interoperable health information technology infrastructure, updating recommendations to the policy framework, and

making new recommendations, as appropriate. Section 3002(b)(2)(A) of the PHSA specifies that in general, the HITAC shall recommend to the National Coordinator for purposes of adoption under section 3004, standards, implementation specifications, and certification criteria and an order of priority for the development, harmonization, and recognition of such standards, specifications, and certification criteria. Like the process previously required of the former HITPC and HITSC, section 3002(b)(5) of the PHSA requires the HITAC to develop a schedule, updated annually, for the assessment of policy recommendations, which the Secretary publishes in the **Federal Register**.

Section 3004 of the PHSA establishes a process for the adoption of health IT standards, implementation specifications, and certification criteria and authorizes the Secretary to adopt such standards, implementation specifications, and certification criteria. As specified in section 3004(a)(1), the Secretary is required, in consultation with representatives of other relevant federal agencies, to jointly review standards, implementation specifications, and certification criteria endorsed by the National Coordinator under section 3001(c) and subsequently determine whether to propose the adoption of such standards, implementation specifications, or certification criteria. Section 3004(a)(3) requires the Secretary to publish all such determinations in the **Federal Register**.

Section 3004(b)(3) of the PHSA, titled, Subsequent Standards Activity, provides that the Secretary shall adopt additional standards, implementation specifications, and certification criteria as necessary and consistent with the schedule published by the HITAC. We consider this provision in the broader context of the HITECH Act and Cures Act to grant the Secretary the authority and discretion to adopt standards, implementation specifications, and certification criteria that have been recommended by the HITAC and endorsed by the National Coordinator, as well as other appropriate and necessary health IT standards, implementation specifications, and certification criteria.

2. Health IT Certification Program(s)

Section 3001(c)(5) of the PHSA provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health IT. Section 3001(c)(5)(A) specifies that the National Coordinator, in consultation with the Director of the National Institute of Standards and Technology (NIST), shall keep or recognize a program or programs for the voluntary certification of health IT that is in compliance with applicable certification criteria adopted under section 3004 of the PHSA. The certification program(s) must also include, as appropriate, testing of the technology in accordance with section 13201(b) of the HITECH Act. Section 13201(b) of the HITECH Act requires that, with respect to the development of standards and implementation specifications, the Director of NIST shall support the establishment of a conformance testing infrastructure, including the development of technical test beds. Section 13201(b) also indicates that the development of this conformance testing infrastructure may include a program to accredit independent, non-federal laboratories to perform testing.

Section 4003(b) of the Cures Act added section 3001(c)(9)(B)(i) to the PHSA, which requires the National Coordinator "to convene appropriate public and private stakeholders" with the goal of developing or supporting a Trusted Exchange Framework and a Common Agreement (collectively, TEFCA) for the purpose of ensuring full network-to-network exchange of health information. Section 3001(c)(9)(B) outlines provisions related to the establishment of a Trusted Exchange Framework for trust policies and practices and a Common Agreement for exchange between health information networks (HINs)—including provisions for the National Coordinator, in collaboration with the NIST, to provide technical assistance on implementation and pilot testing of TEFCA. Section 3001(c)(9)(C) requires the National Coordinator to publish TEFCA on its website and in the **Federal Register.**

Section 4002(a) of the Cures Act amended section 3001(c)(5) of the PHSA by adding section 3001(c)(5)(D), which requires the Secretary, through notice and comment rulemaking, to require conditions of certification and maintenance of certification for the Program. Specifically,

the health IT developers or entities with technology certified under the Program must, in order to maintain such certification status, adhere to certain conditions and maintenance of certification requirements concerning information blocking; assurances regarding appropriate exchange, access, and use of electronic health information; communications regarding health IT; application programing interfaces (APIs); real world testing; attestations regarding certain conditions and maintenance of certification requirements; and submission of reporting criteria under the EHR Reporting Program in accordance with section 3009A(b) of the PHSA.

B. Regulatory History

The Secretary issued an interim final rule with request for comments on January 13, 2010, "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology" (75 FR 2014), which adopted an initial set of standards, implementation specifications, and certification criteria. On March 10, 2010, the Secretary issued a proposed rule, "Proposed Establishment of Certification Programs for Health Information Technology" (75 FR 11328), that proposed both temporary and permanent certification programs for the purposes of testing and certifying health IT. A final rule establishing the temporary certification program was published on June 24, 2010, "Establishment of the Temporary Certification Program for Health Information Technology" (75 FR 36158), and a final rule establishing the permanent certification program was published on January 7, 2011, "Establishment of the Permanent Certification Program for Health Information Technology" (76 FR 1262).

We have engaged in multiple rulemakings to update standards, implementation specifications, certification criteria, and the certification program, a history of which can be found in the October 16, 2015, final rule "2015 Edition Health Information (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications" (80 FR 62602) (2015 Edition Final Rule). The history can be found at 80 FR 62606. A correction notice was published for the 2015 Edition

Final Rule on December 11, 2015 (80 FR 76868), to correct preamble and regulatory text errors and clarify requirements of the Common Clinical Data Set (CCDS), the 2015 Edition privacy and security certification framework, and the mandatory disclosures for health IT developers.

The 2015 Edition Final Rule established a new edition of certification criteria ("2015 Edition health IT certification criteria" or "2015 Edition") and a new 2015 Edition Base EHR definition. The 2015 Edition established the minimum capabilities and specified the related minimum standards and implementation specifications that certified electronic health record technology (CEHRT) would need to include to support the achievement of "meaningful use" by eligible clinicians, eligible hospitals, and critical access hospitals under the Medicare and Medicaid EHR Incentive Programs (EHR Incentive Programs) (now referred to as the Promoting Interoperability (PI) Programs) when the 2015 Edition is required for use under these and other programs referencing the CEHRT definition. The final rule also adopted a proposal to change the Program's name to the "ONC Health IT Certification Program" from the ONC HIT Certification Program, modified the Program to make it more accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond the ambulatory and inpatient settings, and adopted new and revised Principles of Proper Conduct (PoPC) for ONC-Authorized Certification Bodies (ONC-ACBs).

After issuing a proposed rule on March 2, 2016, "ONC Health IT Certification Program: Enhanced Oversight and Accountability" (81 FR 11056), we published a final rule by the same title (81 FR 72404) (EOA Final Rule) on October 19, 2016. The EOA Final Rule finalized modifications and new requirements under the Program, including provisions related to our role in the Program. The final rule created a regulatory framework for our direct review of health IT certified under the Program, including, when necessary, requiring the correction of non-conformities found in health IT certified under the Program and suspending and terminating certifications issued to Complete EHRs and Health IT Modules. The final rule also set forth processes for us to authorize and oversee accredited testing laboratories under the Program. In

addition, it included provisions for expanded public availability of certified health IT surveillance results.

On March 4, 2019, the Secretary published a proposed rule titled, "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program" (84 FR 7424) (ONC Cures Act Proposed Rule). The proposed rule proposed to implement certain provisions of the Cures Act that would advance interoperability and support the access, exchange, and use of electronic health information. We also requested comment in the ONC Cures Act Proposed Rule (84 FR 7467) as to whether certain health IT developers should be required to participate in TEFCA as a means of providing assurances to their customers and ONC that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI, with the goal of developing or supporting TEFCA for the purpose of ensuring full network-to-network exchange of health information.

On May 1, 2020, a final rule was published titled, "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program" (85 FR 25642) (ONC Cures Act Final Rule). This final rule implemented certain provisions of the Cures Act, including Conditions and Maintenance of Certification requirements for health information technology (health IT) developers, the voluntary certification of health IT for use by pediatric health providers, and reasonable and necessary activities that do not constitute information blocking. The final rule also implemented certain parts of the Cures Act to support patients' access to their EHI, and the implementation of information blocking policies that support patient electronic access. Additionally, the final rule modified the 2015 Edition health IT certification criteria and Program in other ways to advance interoperability, enhance health IT certification, and reduce burden and costs, as well as improving patient and health care provider access to EHI and promoting competition. On November 4, 2020, the Secretary published an interim final rule with comment period titled, "Information Blocking and the ONC Health IT Certification

Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency" (85 FR 70064) (Cures Act Interim Final Rule). The interim final rule extended certain compliance dates and timeframes adopted in the ONC Cures Act Final Rule to offer the healthcare system additional flexibilities in furnishing services to combat the COVID-19 pandemic, including extending the applicability date for information blocking provisions to April 5, 2021.

On January 19, 2022, we published a notice titled, "Notice of Publication of the Trusted Exchange Framework and Common Agreement" (87 FR 2800) ("TEFCA"). The notice fulfilled an obligation under section 3001(c)(9)(C) of the PHSA, which requires the National Coordinator for Health Information Technology to publish on the Office of the National Coordinator for Health Information Technology's public internet website, and in the **Federal Register**, the trusted exchange framework and common agreement developed under the PHSA.

III. ONC Health IT Certification Program Updates

A. "The ONC Certification Criteria for Health IT" and Discontinuing Year Themed "Editions"

ONC first introduced the concept of an "edition" of ONC health IT certification criteria in 2012. In March 2012, in the 2014 Edition Proposed Rule,[18] to make a clear distinction between the certification criteria finalized in the 2010 ONC "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology" interim final rule (75 FR 20132047) and adopted in §§ 170.302, 170.304, and 170.306 (to support "Stage 1 meaningful use criteria") and the certification criteria proposed for adoption in § 170.314 (to support "Stage 2 meaningful use criteria") (77 FR 13832), we discussed that we would use an "edition" naming approach for the sets of certification criteria subsequently adopted by the Secretary (77 FR 13836). We stated that we would refer to the

[18] Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology (77 FR 13832).

certification criteria adopted in §§ 170.302, 170.304, and 170.306 collectively as the "2011 Edition EHR certification criteria" and that the certification criteria adopted in § 170.314 would be referred to as the "2014 Edition EHR certification criteria" (77 FR 13836). We finalized this approach and adopted a "2014 Edition" in a September 2012 final rule (77 FR 54163) (the 2014 Edition Final Rule). Overall, we created the concept of certification criteria "editions" with the expectation that it would make it easier for developers of certified health IT and health care providers to quickly determine the certification criteria to which their health IT would need to be certified to remain in compliance with CMS program requirements regarding the use of certified EHR technology (CEHRT) (77 FR 54167).

We coined the "2011 Edition" and "2014 Edition" because the edition's name was designed to coincide with the first year in which compliance with that edition of certification criteria was required for use under the Medicare and Medicaid EHR Incentive Programs (79 FR 54431). We thought this approach would simplify communications related to the certification criteria editions and enable clear compliance statements like "an EP needs to be using 2014 Edition CEHRT when they demonstrate meaningful use … in CY 2014" (79 FR 54431). This approach resulted for many people in a direct, and limited in scope, link between certification criteria editions and "meaningful use" even though these certification criteria were already being referenced by other HHS programs (e.g., the CMS and HHS Office of the Inspector General (OIG) final rules to modify the Physician Self-Referral Law exception and Anti-kickback Statute safe harbor for certain EHR donations (78 FR 78751) and (78 FR 79202), respectively).[19]

In September 2014, we issued a final rule to update the 2014 Edition with "2014 Edition Release 2" certification criteria and to remove the 2011 Edition from the Code of Federal Regulations (CFR) starting in 2015 (79 FR 54430). At that time, EHR technology certified to the

[19] The CMS final rule is titled "Medicare Program; Physicians' Referrals to Health Care Entities with Which They Have Financial Relationships: Exception for Certain Electronic Health Records Arrangements" (78 FR 78751). The OIG final rule is titled "Medicare and State Health Care Programs: Fraud and Abuse; Electronic Health Records Safe Harbor Under the Anti-Kickback Statute" (78 FR 79201).

2011 Edition had become outmoded, no longer met the CEHRT definition, and no longer supported an acceptable level of interoperability (79 FR 54447). Further, as referenced by OIG and CMS in the rulemakings completed by those agencies around donations of EHR items and services, we had planned to retire old or no longer applicable certification criteria editions ((78 FR 79205) and (78 FR 78754), respectively). During this same time period, we jointly issued with CMS a final rule (79 FR 52910) that allowed for continued use of 2011 Edition CEHRT in combination with 2014 Edition CEHRT within 2014, which allowed for certain providers to meet meaningful use requirements with EHRs certified to the 2011 or the 2014 Edition criteria, or a combination of both editions, for an EHR Reporting Period in 2014.[20] The rule also extended Stage 2 through 2016, meaning that providers who first attested to meaningful use in 2011 or 2012 would remain in Stage 2 for an additional year (79 FR 52926). These actions further demonstrated that linking a certification criteria edition's year to any other program's compliance date had drawbacks and could ultimately confuse the original intent of the edition's year selection. This experience also highlighted unintended negative impacts stemming from this approach of packaging all ONC certification criteria into discrete editions, even where those editions might have overlapping criteria. Specifically, the editions approach had two major negative impacts relating to how updates were implemented: 1) it required **all** developers and providers to update their systems by a specific date, and 2) it required all developers and providers to update their systems to all edition criteria even where criteria may overlap or only have minor revisions between editions.

Accordingly, we set out to establish a simpler approach that could be used for future certification criteria editions. First, we intentionally adopted an overlapping transition period from any one edition to a subsequent edition (e.g., the 2014 Edition to the subsequent edition).

---

[20] The CMS final rule is titled "Medicare and Medicaid Programs; Modifications to the Medicare and Medicaid Electronic Health Record (EHR) Incentive Program for 2014 and Other Changes to the EHR Incentive Program; and Health Information Technology: Revisions to the Certified EHR Technology Definition and EHR Certification Changes Related to Standards" (79 FR 52909).

Second, we modified our approach to name the edition for *the year in which the final rule was published,* and subsequent rulemakings that include additional criteria or alternatives to previously adopted certification criteria would be added to the most current edition of certification criteria (79 FR 54431). To further clarify, we stated that a rulemaking that does not adopt an edition of certification criteria would be referred to as "[current edition year] Release #X" (79 FR 54431). We intended this approach to provide the public with predictable naming expectations for future editions and to support ONC's broader interests to have the Program be generally accessible to other programs designed to use certified health IT, either within or outside government. Developers of certified health IT and health care providers that sought to leverage the Program would then be able to choose which edition of certification criteria (or subset of criteria within an edition) was most relevant and appropriate for their program needs for the time their program requirements would be applicable (79 FR 54431).

Following this approach, in 2015, ONC issued a final rule, "2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications," (2015 Edition Final Rule) and adopted the "2015 Edition Health IT Certification Criteria" (80 FR 62602). We codified the 2015 Edition certification criteria in § 170.315 to set them apart from other editions of certification criteria (80 FR 62608). Importantly, the program compliance requirements for certain health care providers to use 2015 Edition certified health IT was ultimately set by CMS to start in 2019 (83 FR 41144).[21]

Four years later, as part of implementation of the 21st Century Cures Act, we issued the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule (84 FR 7424) to update to the 2015 Edition, mindful that

[21] The CMS final rule is titled "Medicare Program; Hospital Inpatient Prospective Payment Systems for Acute Care Hospitals and the Long-Term Care Hospital Prospective Payment System and Policy Changes and Fiscal Year 2019 Rates; Quality Reporting Requirements for Specific Providers; Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs (Promoting Interoperability Programs) Requirements for Eligible Hospitals, Critical Access Hospitals, and Eligible Professionals; Medicare Cost Reporting Requirements; and Physician Certification and Recertification of Claims" (83 FR 41144).

2015 Edition certified health IT was just being implemented. In 2020, we published the ONC Cures Act Final Rule (85 FR 25642) and adopted updates to the 2015 Edition. These updates included new certification criteria, standards, and requirements, as well as incremental revisions to existing 2015 Edition certification criteria to better enable interoperability and the access, exchange, and use of EHI (85 FR 25664-65). Because we did not adopt a new edition of certification criteria in a different CFR section, we retained the overall 2015 Edition title for the changes included in the ONC Cures Act Final Rule and made specific timebound compliance changes within certification criteria.

In the final rule, we stated that we considered a variety of factors when we determined to update the 2015 Edition rather than adopt a new "edition." First, we reviewed the scope of each proposed update and the cumulative scope of the proposals overall for health IT developers and sought to identify whether it would be more appropriate to require health IT developers participating in the Program to implement updates to Health IT Modules certified to the 2015 Edition or to test and certify health IT products to an entirely new edition of certification criteria. Second, we considered the impact that either approach would have on health care providers, including how such updated Health IT Modules or products certified to a new edition would be implemented by providers participating in CMS programs. We also noted that historically, with a new edition of certification criteria, health IT developers have packaged Health IT Modules certified to new, revised, and unchanged criteria into a wholly new certified product. We observed that historical data indicated that these complete updates to the edition were particularly challenging for both health IT developers seeking certification and for health care providers as they establish deadlines for a significant number of health IT developers to support and implement new products for a significant number of health care providers simultaneously. As a result, the burden of updating the technology is compounded for both health IT developers and health care providers (85 FR 25665).

Our intent with this approach was to maintain a single set of certification criteria that have been updated to include the most recent versions of adopted standards, and to establish an incremental approach to health IT updates over time. In the ONC Cures Act Final Rule, we stated our belief that this approach should also include development timelines based on the updates required for each criterion and a transition period allowing for multiple standards to be used for a reasonable period of time. We noted our belief that, as a whole, this approach can help to reduce the burden on health IT developers and health care providers and could allow health IT developers to implement updates in the manner most appropriate for their product and their customers (85 FR 25665). Commenters noted this approach would provide stability and that an incremental approach best serves the health care provider and health IT developer community (85 FR 25664).

However, in response to public comment related to how we communicate and avoid public confusion (85 FR 25666), we distinguished the "original" 2015 Edition certification criteria from the new and revised 2015 Edition certification criteria by referring to the updates we adopted as the 2015 Edition "Cures Update" certification criteria. Subsequent to publication of the final rule, through public meetings and correspondence, we have been informed that the continued use and reference to the 2015 Edition inaccurately implied an age and outdatedness to the certification criteria we had adopted. More importantly, we have received significant positive feedback expressing that the incremental approach to updates is generally beneficial as a long-term approach. Specifically, feedback conveyed that a consistent, transparent, incremental update cycle that includes the following features would be preferred by some: 1) regular updates to recognize standards advancement and an allowance for voluntary standards advancement between updates, 2) incremental updates rather than "wholesale" product overhauls, 3) a predictable timeline for updates based on standards development cycles with reasonable development timelines, and 4) a reasonable development timeline for any new criterion based on the specific development needs.

For these reasons, we no longer believe that it is helpful or necessary to maintain an "edition" naming convention and to adopt entirely new editions of certification criteria to encapsulate updates over time. Instead, we believe that there should be a single set of certification criteria, which would be updated in an incremental fashion in closer alignment to standards development cycles and regular health IT development timelines. We therefore propose to rename all certification criteria within the Program simply as "ONC Certification Criteria for Health IT." We believe maintaining a single set of "ONC Certification Criteria for Health IT" would create more stability for users of health IT and Program partners, such as CMS, as well as make it easier for developers of certified health IT to maintain their product certificates over time. In addition, we believe that this approach will have the benefit of reducing administrative burden for health IT developers participating in the Program. Previously, duplicative references to separate certification criteria under multiple year-themed editions created administrative burden on developers, as they had the effect of requiring health IT developers to seek an updated certificate attributed to the "new" duplicated certification criterion even in circumstances when the certification criterion remained substantively unchanged. Under this proposal, unchanged certification criteria would no longer be duplicated as separate criteria under multiple editions. Accordingly, we propose to rename § 170.315 as the "ONC Certification Criteria for Health IT" and replace all references throughout 45 CFR part 170 to the "2015 Edition" with this new description (this would impact the wording, though not the substance or effect, of §§ 170.102, 170.405, 170.406, 170.523, 170.524, and 170.550, as shown in proposed revised regulation text, below). We welcome public comment on this proposal.

In the 2014 Edition Final Rule we defined the terms "new," "revised," and "unchanged" to both describe the differences between the 2014 Edition certification criteria and the 2011 Edition certification criteria, as well as establish what certification criteria in the 2014 Edition

were eligible for gap certification[22] (see 77 FR 54171, 54202, and 54248). Beginning with the 2015 Edition, "Complete EHR" certifications were no longer issued (see also 79 FR 54443 through 54445) and, as part of our effort to make the Program more open and accessible to other healthcare and practice settings, we also defined these terms for the purpose of a gap certification analysis as follows:

- "New" certification criteria are those that as a whole only include capabilities never referenced in previously adopted certification criteria editions and to which a Health IT Module presented for certification to the 2015 Edition could have never previously been certified.
- "Revised" certification criteria are those that include the capabilities referenced in a previously adopted edition of certification criteria as well as changed or additional new capabilities; and to which a Health IT Module presented for certification to the 2015 Edition could not have been previously certified to all of the included capabilities.
- "Unchanged" certification criteria are those that include the same capabilities as compared to prior certification criteria of adopted editions; and to which a Health IT Module presented for certification to the 2015 Edition could have been previously certified to all of the included capabilities (80 FR 62608).

We propose that these same concepts as applied to the certification criteria would continue to be used by the Program in the absence of a year named "edition." However, for clarity, we now propose to define "revised certification criterion (or criteria)" in § 170.102 to mean a certification criterion that meets at least one of the following: (1) has added or changed the functions or capabilities described in the existing criterion in 45 CFR 170 part C; (2) has an

---

[22] *Gap certification* means the certification of a previously certified Health IT Module(s) to:
(1) All applicable new and/or revised certification criteria adopted by the Secretary at subpart C of this part based on test results issued by a NVLAP-accredited testing laboratory under the ONC Health IT Certification Program or an ONC-ATL; and
(2) All other applicable certification criteria adopted by the Secretary at subpart C of this part based on the test results used to previously certify the Complete EHR or Health IT Module(s) under the ONC Health IT Certification Program (§ 170.502).

added or changed standard or implementation specification referenced in the existing criterion in 45 CFR part 170 subpart B; or (3) is specified through notice and comment rulemaking as an iterative or replacement version of an existing criterion in 45 CFR part 170 subpart C.

By way of example, proposed provisions (1) and (2) were met in § 170.315(b)(3) in the ONC Cures Act Final Rule (85 FR 25683) because we modified this criterion to include new functions or capabilities in § 170.315(b)(3)(ii)(A)(*7*) through (*9*) that did not exist in § 170.315(b)(3). Also, in § 170.315(b)(3), in the ONC Cures Act Final Rule we added cross-references to the NCPDP SCRIPT standard version 2017071 in § 170.315(b)(3)(ii)(A) and (b)(3)(ii)(B), which did not exist in § 170.315(b)(3). An example of proposed provision (3) can be found in the ONC Cures Act Final Rule in § 170.315(b)(6) "Data export" being replaced by § 170.315(b)(10) "Electronic Health Information export" (85 FR 25699). If finalized as proposed there would not be an "edition" to differentiate between such revisions to existing criteria; instead, such criteria would be considered "revised" until a subsequent rulemaking where no further revision to the criterion renders them "unchanged."

We would continue to use these terms when: communicating proposals for future criteria, such as revising a criterion that will maintain its place in the CFR or establishing a new criterion that is an iterative or replacement criterion in the Program; establishing scenarios for when gap certification is an option for developers of certified health IT; and when setting expiration dates or applicable timelines related to standards and certification criteria. Through the development of educational resources, such as fact sheets[23] and resource guides,[24] these designations will help users and the public understand to which versions of standards and certification criteria a Health IT Module may be certified when multiple versions of standards or certification criteria are available under the Program. In this proposed rule, we propose applicability or implementation timelines for both our certification criteria and the standards adopted in 45 CFR part 170 by

[23] See 2015 Edition Cures Update Fact Sheet: https://www.healthit.gov/sites/default/files/page/2022-03/Cures-Update-Fact-Sheet.pdf.
[24] See API Resource Guide: https://onc-healthit.github.io/api-resource-guide/.

establishing the dates by which an existing version of a criterion is no longer applicable and by establishing a date by when a new or revised certification criterion or standard version is adopted. For example, if finalized as proposed, a user and the public would know that a Health IT Module certified to "revised" § 170.315(b)(1) would support USCDI v3 (§ 170.213(b)) after January 1, 2025, because we state that USCDI v1 expires on January 1, 2025, in § 170.213(a).

We propose the following revised standards and implementation specifications: § 170.205(a); §§ 170.207(a), (c), (d), (e), (f), (m), (n), (o), (p), (r), and (s); § 170.210(g); § 170.213; § 170.215(b), and § 170.215(c). We propose new standards and implementation specifications in § 170.205(t) and § 170.205(o). Table 1 below includes the proposed new and revised certification criteria described in this rule.

Table 1: List of Proposed Health IT Certification Criteria

New Certification Criterion	
§ 170.315(d)(14)	Privacy and security – Patient Requested Restrictions
Revised Certification Criteria	
§ 170.315(a)(5)	Clinical – Patient demographics and observations (currently Demographics)
§ 170.315(a)(9)	Clinical – Clinical decision support (CDS) (to be recategorized as "Care Coordination § 170.315(b)(11)")
§ 170.315(b)(1)	Care Coordination – Transitions of care
§ 170.315(b)(2)	Care Coordination – Clinical information reconciliation and incorporation
§ 170.315(e)(1)	Patient Engagement – View, download, and transmit to 3rd party
§ 170.315(f)(5)	Public Health – Transmission to public health agencies – electronic case reporting
§ 170.315(g)(10)	Design and Performance – Standardized API for patient and population services
Revised Certification Criteria (standards updates)	
§ 170.315(a)(12)	Clinical – Family health history
§ 170.315(b)(6)	Care Coordination – Data export
§ 170.315(b)(9)	Care Coordination – Care plan
§ 170.315(c)(4)	Clinical Quality Measures – Clinical quality measures – filter.
§ 170.315(f)(1)	Public Health – Transmission to immunization registries.

§ 170.315(f)(3)	Public Health – Transmission to public health agencies – reportable laboratory tests and values/results
§ 170.315(f)(4)	Public Health – Transmission to cancer registries
§ 170.315(g)(3)	Design and Performance – Safety-enhanced design
§ 170.315(g)(6)	Design and Performance – Consolidated CDA creation performance
§ 170.315(g)(9)	Design and Performance – Application access – all data request

When we published the 2015 Edition Final Rule, ONC released educational resources to inform the public. Educational and communication resources included charts on the 2015 Edition certification criteria, reader-friendly fact sheets on specific topics like addressing health disparities and patient engagement, the Companion Certification Guides, and a new "2015 Edition Standards Hub" to help interested parties quickly crosswalk and identify standards referenced by 2015 Edition certification criteria. While our proposal may have the near-term effect of requiring ONC to revise existing communications materials, as well as conforming regulatory updates and updates to materials by other agencies such as CMS that reference the 2015 Edition, we believe the overall benefit of having a single ONC branded set of certification criteria outweighs the burdens that result administratively, as well as for developers of certified health IT and their customers, from rolling out a new "edition." Moreover, starting with the ONC Cures Act Final Rule, we developed a new approach for conformance requirement changes within certification criteria that, when applied in conjunction with this proposed approach, can also reduce administrative and regulatory burden and help to ensure the updates to criteria are clearly defined to support both a transition period and a predictable development timeline aligned to the scope of the specific update. In the ONC Cures Act Final Rule, we did not create a new CFR section as we had done previously but instead updated the existing CFR section, § 170.315. The new approach was designed to make it clear for health IT developers, as well as ONC-Authorized Testing Labs (ONC-ATLs) and ONC-ACBs, how long certain capabilities and standards remain available for the purposes of certification. We also implemented new

Maintenance of Certification requirements as a result of the Cures Act to give health IT developers specific deadlines relative to complying with updated technical requirements, while still allowing developers to continue supporting technology certified to the prior version of certification criteria or standards for use by their customers.

Building upon this approach, in this proposed rule, we also propose modifications to our approach for setting applicability or implementation timelines for both our certification criteria and the standards adopted in 45 CFR part 170. This approach includes establishing the dates by which an existing version of a certification criterion is no longer applicable because a new or revised version of that criterion is adopted. In addition, we have proposed to establish applicable timelines, including expiration dates, for the adoption of standards when a new or revised version of the standard is adopted for the same purpose. This proposed approach would support the ongoing establishment of clear timelines associated with the specific criterion or standard in alignment with the development and update cycle for that specific criterion or standard – again supporting an incremental and flexible approach.

In addition, we believe this approach would facilitate ease of reference for federal, state, local or tribal programs seeking to align their program requirements to the standards and implementation specifications available in certified health IT. These programs may not require use of the entirety of the Base EHR, or they may not even require the use of certified health IT, but they may still seek to align to a specific certification criterion or a specific standard where applicable to their program goals and consistent with their applicable authorities. Furthermore, as we move away from the use of editions to define updated timelines, we believe it is important to continue to provide clarity on existing Program requirements and to ensure that customers are provided with timely technology updates. We therefore propose to incorporate the applicable timelines and expiration dates for functional and standards updates within each individual criterion or standard. In section III.C.11 of this proposed rule, we propose to make explicit in the introductory text in § 170.315 that health IT developers voluntarily participating in the Program

must update their certified Health IT Modules and provide that updated certified health IT to customers in accordance with the timelines defined for each criterion and standard if they intend to maintain certification of the Health IT Module. (For ease of reference and reading, we use "developer of certified health IT" in this proposed rule to reference developers who voluntarily participate in the Program). We believe this approach will also help to advance interoperability. Under this proposal, a developer of certified health IT would not be required to provide technology updates for certification criteria or standards to a user who declined such updates. However, we note that if such an update is not provided, and the Health IT Module was previously certified to a criterion or criteria that now make it subject to a "revised" criterion or criteria, the Health IT Module would no longer be certified under the Program, in the same manner that previously removed or expired "editions" are no longer certified under the Program.

We direct readers to section III.C.11 of this proposed rule for further discussion of the requirements for health IT developers voluntarily participating in the Program related to health IT certification updates.

In the ONC Cures Act Final Rule, we revised the Principles of Proper Conduct for ONC-ACBs and ONC-ATLs by revising the records retention policies to include the "life of the edition" (85 FR 25710 through 25713). Specifically, we clarified that the records retention provisions in §§ 170.523 and 170.524 included the "life of the edition" as well as three years after the retirement of an edition related to the certification of Complete EHRs and Health IT Modules. We explained that "[b]ecause the 'life of the edition' begins with the codification of an edition of certification criteria in the CFR and ends on the effective date of the final rule that removes the applicable edition from the CFR, the start and end dates for the 'life of the edition' are published in the **Federal Register** in the rulemaking actions that finalize them. The period of three years beyond the 'life of the edition' begins on the effective date of the final rule that removes the applicable edition from the CFR, thus the three-year period after removal from the CFR continues through three full calendar years following that date" (85 FR 25710). Because in

this proposed rule we propose to maintain a single set of "ONC Certification Criteria for Health IT" and not an edition, we propose to revise § 170.523 and § 170.524. We propose that the period of three years begins on the effective date of the final rule that removes the applicable ONC certification criterion or criteria for health IT from the CFR, thus the three-year period after removal from the CFR continues through three full calendar years following that date (in addition to the calendar year in which it was removed). We also retain the "Complete EHR" language in these sections because beginning with the 2015 Edition, Complete EHR certifications could no longer be issued. However, since the 2014 Edition was not removed from the CFR until the ONC Cures Act Final Rule, which became effective on June 30, 2020, records would need to be retained (including Complete EHRs) until June 30, 2023.

B. Standards and Implementation Specifications

1. National Technology Transfer and Advancement Act

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 et. seq.) and the Office of Management and Budget (OMB) Circular A-119[25] require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A-119 provide exceptions to electing only standards developed or adopted by voluntary consensus bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. Agencies have the discretion to decline the use of existing voluntary consensus standards if it is determined that such standards are inconsistent with applicable law or otherwise impractical, and instead use a government-unique standard or other standard. In addition to the consideration of voluntary consensus standards, the OMB Circular A-119 recognizes the contributions of standardization activities that take place outside of the voluntary consensus standards process. Therefore, in instances where use of voluntary consensus standards would be inconsistent with applicable law or otherwise impracticable, other

[25] https://www.whitehouse.gov/wp-content/uploads/2020/07/revised_circular_a-119_as_of_1_22.pdf.

standards should be considered that meet the agency's regulatory, procurement or program needs, deliver favorable technical and economic outcomes, and are widely utilized in the marketplace. In this proposed rule, we use voluntary consensus standards except for:

- The United States Core Data for Interoperability (USCDI), October 2022 Errata, Version 3 (v3) standard. We propose to adopt USCDI v3 (October 2022 Errata) in § 170.213. This standard is a hybrid of government policy (i.e., determining which data to include in the USCDI) and voluntary consensus standards (i.e., the vocabulary and code set standards attributed to USCDI data elements); and
- The standard we propose to adopt in § 170.207(f)(3) for race and ethnicity.

We are not aware of any voluntary consensus standards that could serve as an alternative for the purposes we describe in further detail throughout this proposed rule including establishing a baseline set of data that can be commonly exchanged across care settings for a wide range of uses. We refer readers to section III.C.1 of this preamble for a discussion of the USCDI.

2. Compliance with Adopted Standards and Implementation Specifications

In accordance with Office of the Federal Register regulations related to "incorporation by reference," 1 CFR part 51, which we follow when we adopt proposed standards and/or implementation specifications in any subsequent final rule, the entire standard or implementation specification document is deemed published in the **Federal Register** when incorporated by reference therein with the approval of the Director of the Federal Register. Once published, compliance with the standard and implementation specification includes the entire document unless we specify otherwise. For example, if we adopted the HL7® FHIR US Core Implementation Guide 5.0.1 proposed in this proposed rule (*see* section III.C.7.b), health IT certified to certification criteria referencing this IG would need to demonstrate compliance with all mandatory elements and requirements of the IG. If an element of the IG is optional or permissive in any way, it would remain that way for testing and certification unless we specified

otherwise in regulation. In such cases, the regulatory text would preempt the permissiveness of the IG.

3. "Reasonably Available" to Interested Parties

The Office of the Federal Register has established requirements for materials (e.g., standards and implementation specifications) that agencies propose to incorporate by reference in the Code of Federal Regulations (79 FR 66267; 1 CFR 51.5(a)). To comply with these requirements, in section V ("Incorporation by Reference") of this preamble, we provide summaries of, and uniform resource locators (URLs) to, the standards and implementation specifications we propose to adopt and subsequently incorporate by reference in the Code of Federal Regulations. To note, we also provide relevant information about these standards and implementation specifications throughout the relevant sections of the proposed rule.

C. New and Revised Standards and Certification Criteria

1. The United States Core Data for Interoperability Standard (USCDI) v3

a. Background

The United States Core Data for Interoperability (USCDI) is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange.[26] In the ONC Cures Act Final Rule, ONC established USCDI as a standard to replace the Common Clinical Data Set (CCDS) in several ONC certification criteria (85 FR 25670). ONC adopted USCDI Version 1 (USCDI v1) in § 170.213 and incorporated it by reference in § 170.299.[27] In an interim final rule with comment period published by ONC on November 4, 2020, "Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency," ONC adopted and incorporated by reference the updated standard USCDI v1 (July 2020 Errata) (85 FR 70073).

[26] https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.
[27] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-170#p-170.213.

USCDI v1 established a baseline set of data that can be commonly exchanged across care settings for a wide range of uses and is a required part of certain certification criteria in the 2015 Edition Cures Update. These certification criteria include transitions of care; clinical information reconciliation and incorporation; view, download, and transmit to 3rd party; transmission to public health agencies – electronic case reporting; consolidated CDA creation performance; application access – all data request, and standardized API for patient and population services (adopted in § 170.315(b)(1), (b)(2), (e)(1), (f)(5), (g)(6), (g)(9), and (g)(10) respectively). USCDI is also referenced by HHS programs and the healthcare community to align interoperability requirements and national priorities for health IT and healthcare standards broadly across industry initiatives. Additionally, at a minimum, entities that sign the Common Agreement are required to exchange all available data elements from USCDI v1.[28] USCDI is composed of data classes which aggregate data elements by common themes. Data elements are the granular level at which a piece of data is defined for exchange within the USCDI standard. For example, "Laboratory" is a data class, and within that data class there is "Values/Results" which is a data element. For the overall structure and organization of USCDI, including data classes and data elements in USCDI v1, please see the discussion in the ONC Cures Act Final Rule (85 FR 25669 – 25670) as well as www.healthIT.gov/USCDI.

ONC stated in the ONC Cures Act Final Rule that we intended to utilize a predictable, transparent, and collaborative process to expand USCDI, including providing the public with the opportunity to comment on USCDI's expansion (85 FR 25670). We also noted that health IT developers would be able to use the Standards Version Advancement Process (SVAP) to voluntarily implement and use a newer, National Coordinator-approved version of USCDI in the future without waiting for ONC to propose and adopt via rulemaking an updated version of the USCDI (85 FR 25669). ONC, therefore, established a process for expanding USCDI based on

[28] Trusted Exchange Framework and Common Agreement Qualified Health Information Network (QHIN) Technical Framework (QTF). Version 1.0. January 2022. https://rce.sequoiaproject.org/wp-content/uploads/2022/01/QTF_0122.pdf.

public input and submissions of new data elements and classes.[29] To enable these submissions, ONC created the ONC New Data Element and Class (ONDEC) submission system, which provides the public with the opportunity to submit new data elements for consideration for inclusion in future versions of USCDI.[30] ONC accepts submissions for new USCDI data elements in ONDEC on an ongoing basis, with a September cutoff each year for submissions to be considered for the next version of USCDI. ONC evaluates these submissions and assigns "levels" based on technical maturity, implementation feasibility, overall breadth of impact on potential users, and any known challenges to use of these data. Level 2 elements are those ONC deems the most mature and ready for consideration for future versions, followed by Level 1 elements as less mature, and Comment Level elements as the least mature. After the submission cutoff, ONC selects from Level 2 elements. ONC then publishes a draft of the next version of USCDI and accepts public feedback on the draft.[31] This feedback informs the version of USCDI released in July each year. In this way, the standard can continue to evolve in an incremental and predictable manner, even though ONC might not propose to adopt each new version in the Code of Federal Regulations.

ONC has received several hundred submissions through ONDEC recommending new and updated data classes and data elements during each annual update cycle. In July 2021, ONC published USCDI Version 2 (USCDI v2),[32] and this version was later added to the SVAP Approved Standards for 2022.[33] SVAP allows health IT developers to voluntarily update their products to USCDI v2 without waiting for rulemaking to update the version of USCDI listed in the regulations (85 FR 25669). At the time of release of USCDI v2, ONC also announced additional criteria on which new and existing submissions would be evaluated and selected for

---

[29] https://www.healthit.gov/buzz-blog/interoperability/uscdi-onc-new-data-element-and-class-submission-system-now-available.
[30] https://www.healthit.gov/isa/ONDEC.
[31] https://www.healthit.gov/buzz-blog/interoperability/opportunity-trifecta-isa-svap-and-draft-uscdi-version-3-feedback-period-now-open.
[32] https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi#uscdi-v2.
[33] https://www.healthit.gov/sites/default/files/page/2022-06/SVAP_Approved_Standards_2022.pdf.

USCDI v3 and future versions. These criteria included the ability of the data elements to promote health equity, address the needs of underserved communities, and enable public health data interoperability.[34] In January 2022, ONC released Draft USCDI v3 and provided for a three-month public feedback period.[35] After reviewing and incorporating public feedback, ONC finalized and released USCDI v3 in July 2022.

We propose to update the USCDI standard in § 170.213 by adding the newly released USCDI v3 and by establishing a January 1, 2025, expiration date for USCDI v1 (July 2020 Errata) for purposes of the Program. We propose to add USCDI v3 in § 170.213(b) and incorporate it by reference in § 170.299. Specifically, USCDI v3 in this proposed rule refers to the USCDI v3 (October 2022 Errata). We propose to codify the existing reference to USCDI v1 (July 2020 Errata) in § 170.213(a). We propose that as of January 1, 2025, any Health IT Modules seeking certification for criteria referencing § 170.213 would need to be capable of exchanging the data classes and data elements that comprise USCDI v3.

b. Certification Criteria that Reference USCDI

The USCDI standard is currently cross-referenced, via cross-reference to § 170.213, in certain certification criteria. A Health IT Module could currently be certified to any of these criteria by ensuring that it complies with either the USCDI v1 or USCDI v2 standards, since USCDI v2 is approved for SVAP. Should we adopt our proposal to add the USCDI v3 in § 170.213, Health IT Modules certified to these criteria that cross-reference § 170.213 could also be certified by meeting the USCDI v3 standard. Through December 31, 2024, we propose that a Health IT Module certified to criteria that cross-reference § 170.213 may be certified by complying with (1) USCDI v1; (2) USCDI v2 under SVAP; and (3) USCDI v3. We propose to

[34] https://www.healthit.gov/buzz-blog/interoperability/opportunity-trifecta-isa-svap-and-draft-uscdi-version-3-feedback-period-now-open.
[35] https://www.healthit.gov/sites/default/files/page/2022-01/Standards_Bulletin_2022-1.pdf.

allow only USCDI v3 after this date for the criteria that cross-reference § 170.213. The criteria cross-referencing to USCDI via cross-reference to § 170.213 are as follows:

- "Care coordination – Transitions of care – Create" (§ 170.315(b)(1)(iii)(A)(*1*));
- "Care coordination – Clinical information reconciliation and incorporation – Reconciliation" (§ 170.315(b)(2)(iii)(D)(*1*) through (*3*));
- "Patient engagement – View, download, and transmit to 3rd party – View" (§ 170.315(e)(1)(i)(A)(*1*));
- "Design and performance – Consolidated CDA creation performance" (§ 170.315(g)(6)(i)(A));
- "Design and performance – Application access – all data request – Functional requirements" (§ 170.315(g)(9)(i)(A)(*1*)); and
- "Design and performance – Standardized API for patient and population services – Data response" (§ 170.315(g)(10)(i)(A) and (B)).

We note that § 170.315(f)(5) also currently references § 170.213. However, as discussed later in this preamble, we propose to rely on specific IGs for this criterion, rather than reference § 170.213. As such, we do not propose to require Health IT Modules certified to § 170.315(f)(5)(iii) to certify using either USCDI v1 or USCDI v3 through December 31, 2024, and only USCDI v3 after December 31, 2024.

As noted previously, a developer of certified health IT would not be required to provide technology updates for certified criteria or standards to a user who declined such updates. However, we note that if such an update is not provided, even if the version of the Health IT Module in use still operates, that version would no longer be considered certified. This means that it may no longer meet the requirements of HHS programs requiring the use of certified health IT.

We propose to add introductory text to § 170.213 noting that the Secretary adopts the following standards as the standards available for the purpose of representing electronic health

information, and we also propose to include the date the adoption of the standard in § 170.213(a) expires. Consistent with our proposals in sections III.A and III.C.11, we propose this expiration date to be January 1, 2025. Health IT developers with Health IT Modules certified to certification criteria that reference § 170.213 would have to update such certified health IT to USCDI v3 and provide it to customers by December 31, 2024. Further, we propose that Health IT Modules certified to the above-listed certification criteria would need to update their Health IT Modules to accommodate USCDI v3 data elements using the FHIR US Core Implementation Guide Version 5.0.1 in § 170.215(b)(1)(ii) and the HL7 CDA® R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 3 in § 170.205(a)(6). If the FHIR US Core Implementation Guide and the HL7 CDA® R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide are updated before the date of publication of the final rule, it is our intent to consider adopting the updated versions that support USCDI v3.

We clarify that under this proposal, for the time period up to and including December 31, 2024, USCDI v1 would remain applicable as the minimum version of the USCDI required for certification criteria that reference § 170.213. This means that upon the effective date of a rule finalizing this proposal, for the identified certification criteria that reference § 170.213, the following would apply as available versions of USCDI for certification and compliance:

- USCDI v1 (2020 Errata) for the time period up to and including December 31, 2024 (the adoption of the standard expires on January 1, 2025),
- USCDI v3.

We refer to the term "expires" in standards throughout this proposed rule, and it would mean that the Secretary no longer recognizes the standard in the Code of Federal Regulations and its use for purposes of the Program is no longer available.

USCDI v2 would remain available via SVAP for developers of certified health IT who want to voluntarily update their Health IT Modules, or for developers of certified health IT who

want to certify to applicable criteria in addition to or instead of USCDI v1 up to and including December 31, 2024.

Additionally, because we finalized in the ONC Cures Act Final Rule that the Common Clinical Data Set (CCDS) would no longer be applicable for certified Health IT Modules 24 months after the publication date of the ONC Cures Act Final Rule (85 FR 25671), and then extended that date to December 31, 2022 in the interim final rule titled "Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency" (85 FR 70073), we propose to remove references to CCDS in the following sections of 45 CFR 170.315: § 170.315(b)(1)(iii)(A)(*2*); (e)(1)(i)(A)(*2*); (g)(6)(i)(B); and (g)(9)(i)(A)(*2*). In each of those sections, we have instead proposed to include a reference to USCDI. Because § 170.315(b)(6)(ii)(A), which also references CCDS, is still available for the period before December 31, 2023, we are not removing the reference to CCDS in that section.

c. USCDI Standard – Data Classes and Elements Added since USCDI v1

ONC proposes to update the USCDI standard in § 170.213 by proposing a January 1, 2025 expiration date for USCDI v1 (July 2020 Errata) and by adding the newly released USCDI v3 (October 2022 Errata). ONC proposes to incorporate USCDI v3 by reference in § 170.299. USCDI v3 includes all data elements defined in USCDI v1 and USCDI v2, and includes additional data elements added in USCDI v3.

Adopting USCDI v3 would provide more comprehensive health data for providers and patients accessing and exchanging electronic health information. USCDI v3 includes Sexual Orientation, Gender Identity, Functional Status, Disability Status, Mental/Cognitive Status, and Social Determinants of Health data elements including: SDOH Assessment, SDOH Goals, SDOH Interventions, and SDOH Problems/Health Concerns. Access, exchange, and use of these data elements can support more informed care for patients. These data elements are described in more detail below.

While the SVAP process provides an opportunity for health IT developers to voluntarily update their certified products to newer versions of USCDI, setting a new USCDI v3 floor for all certified health IT that includes Health IT Modules certified to certification criteria that reference § 170.213 would enable a more consistent adoption of an expanded baseline set of data, realizing the benefits described above. We propose to add USCDI v3 to § 170.213 in addition to USCDI v1 (July 2020 Errata). Because USCDI v1 (July 2020 Errata) may be used for the time period up to and including December 31, 2024, we propose to amend § 170.213 to include paragraph (a) that will note that the USCDI v1 (July 2020 Errata) standard will expire on January 1, 2025, and paragraph (b) that will note the addition of USCDI v3.

Below, we describe the data classes and data elements in USCDI v3 that are not included in USCDI v1. We also describe any data classes or data elements that were changed through the USCDI update processes when comparing USCDI v3 to USCDI v1. For the overall structure and organization of the USCDI standard, including USCDI v3, we urge the public to consult www.healthIT.gov/USCDI. All the following data classes and data elements were added to USCDI based on submissions through the ONDEC system and ONC's determination that they represented significant additions to core interoperable health data and met the prioritization criteria previously set forth in this process. We propose each of these data classes or data elements to be included in the USCDI standard in § 170.213 and to be incorporated by reference in § 170.299 as part of our proposal to adopt USCDI v3.

i. Social Determinants of Health (SDOH)

SDOH[36] are the conditions in which people live, learn, work, and play, and these conditions affect a wide range of health and quality-of-life risks and outcomes.[37] In the 2015 Edition, ONC adopted a certification criterion to enable users of Health IT Modules(s) that certified to that criterion with the functionality to electronically capture, modify, and access

[36] See SDOH Toolkit for more information, https://www.healthit.gov/sites/default/files/2023-02/Social%20Determinants%20of%20Health%20Information%20Exchange%20Toolkit%202023_508.pdf.
[37] https://www.healthit.gov/topic/health-it-health-care-settings/social-determinants-health.

SDOH data elements – that is information that identifies common SDOH conditions in a standardized manner – in § 170.315(a)(15) social, psychological, and behavioral data (80 FR 62631). These functionalities were intended to support users with the ability to use technology to comply with applicable existing legal requirements or organizational policies that may require such data collection and broader, existing industry interests and efforts to collect and use this data to inform clinical decision-making and improve patient care by looking at the whole patient, including leveraging other types of care such as home and community-based services.[38] ONC supports the use of technology to improve the standardized capture of a set of health data classes to support the healthcare industry's need to electronically capture the underlying data they need or want to collect for healthcare.

SDOH data are often categorized into domains based on the type of circumstances they are intended to represent, such as food or housing insecurity. However, many of these circumstances overlap, and there are continuing efforts aiming to capture additional areas of focus such as broadband access or environmental risk factors.

USCDI v3 includes four SDOH data elements that represent specific aspects of SDOH data related to the use or purpose of the SDOH data rather than based on the domain. In this way, the data elements can emphasize the use case aspect of the data and expand to additional domains over time. These data elements are new for USCDI v3 as compared to USCDI v1. However, because each of these aspects is closely related to data elements that exist in USCDI data classes, these new data elements were organized into the applicable existing data classes.

Existing USCDI Data Class	New Data Element
Assessment and Plan of Treatment	SDOH Assessment – related to the conditions in which people live, learn, work and play.
Goals	SDOH Goals – related to expected outcomes for interventions addressing the conditions in which people live, learn, work and play.

[38] https://www.federalregister.gov/d/2015-25597/p-406.

Procedures	SDOH Interventions – related to addressing the conditions in which people live, learn, work and play.
Problems	SDOH Problems/Health Concerns – related to the conditions experienced by a person that impact how they live, learn, work and play. (e.g., transportation insecurity, food insecurity).

ii. Care Team Member

In USCDI v1, the Care Team Member data class had one data element to capture all aspects about a care team member. ONC received submissions recommending the addition of more granular data elements that provide greater detail around a patient's health care provider and other members of the care team. USCDI v3 includes five Care Team Member data elements: Name, Identifier, Role, Location, and Telecom.

iii. Clinical Notes

For the data element Discharge Summary Note in the Clinical Notes data class, we specified additional requirements in USCDI v3 including admission and discharge dates and locations, discharge instructions, and reason(s) for hospitalization, which are also required elements in the Transitions of Care certification criterion (§ 170.315(b)(1)).

iv. Clinical Tests

USCDI v3 includes a data class for Clinical Tests, which has two data elements, Clinical Test and Clinical Test Result/Report. This is a new data class as compared to USCDI v1. These elements will enable the capture and exchange of non-imaging and non-laboratory tests. Some examples include electrocardiogram (ECG), visual acuity exam, macular (ophthalmic) exam, or graded exercise testing (GXT). These tests are routinely performed on patients and result in structured or unstructured (narrative) findings that facilitate the diagnosis and management of a patient's condition(s).

v. Diagnostics Imaging

USCDI v3 includes the Diagnostic Imaging data class and its two elements: Diagnostic Imaging Test and Diagnostic Imaging Report. This is a new data class as compared to USCDI v1. These data elements added a critical missing capability of health IT to capture and exchange structured and unstructured imaging test and report data for a patient.

vi. Encounter Information

USCDI v3 includes the Encounter Information data class, which includes five data elements: Encounter Type, Encounter Diagnosis, Encounter Time, Encounter Location, and Encounter Disposition. This is a new data class as compared to USCDI v1.

vii. Health Insurance Information

USCDI v3 includes the Health Insurance Information data class, which provides an opportunity for health IT to capture and exchange key elements of healthcare insurance coverage. This information can be useful for patient matching and record linkage, coverage determination, prior authorization, price transparency, claims and reimbursement efficiencies, and identifying disparities related to insurance coverage. This is a new data class as compared to USCDI v1. This data class includes seven data elements: Coverage Status, Coverage Type, Relationship to Subscriber, Member Identifier, Subscriber Identifier, Group Identifier, and Payer Identifier.

viii. Health Status Assessments

USCDI v3 includes a data class called Health Status Assessments, which contains four new data elements: Disability Status, Mental/Cognitive Status, Functional Status, and Pregnancy Status. This is a new data class as compared to USCDI v1. In USCDI v3, the Health Status Assessments data class also includes two data elements that have been recategorized, Health Concerns and Smoking Status, which were previously part of different data classes in USCDI. The Health Status Assessments data class provides a broader context for these data elements. The ability to capture and exchange data that represent the assessment performed and the assessment component results helps health care providers address inequities by being able to readily identify and address a patient's conditions characterized with these data.

ix. Laboratory

USCDI v3 includes Specimen Type and Result Status data elements, which have been added to the USCDI Laboratory data class to address public health reporting priorities. These new data elements are key components of laboratory reports and can help with ongoing public health needs, including Covid-19, MPox and future public health emergencies, to ultimately improve patient care.

x. Medications

USCDI v3 includes Dose, Dose Units of Measure, Indication, and Fill Status data elements, which have been added to the USCDI Medications data class in response to public feedback and because these data elements are necessary for certain CMS reporting programs and are also critical to certain ONC certification criteria (including the electronic prescribing certification criterion at § 170.315(b)(3)).

xi. Patient Demographics/Information

Based on submissions and comments during the USCDI update processes described above, ONC changed or added data elements in the Patient Demographics/Information data class.

USCDI v3 includes data elements Sexual Orientation and Gender Identity, which have been added to the USCDI Patient Demographics/Information data class. Previously, ONC adopted standards for Sexual Orientation in the demographics criterion in § 170.315(a)(5)(i)(D) and for Gender Identity in the demographics criterion in § 170.315(a)(5)(i)(E). These criteria include requirements to code Sexual Orientation and Gender Identity according to the adopted SNOMED CT® codes and HL7 Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor as referenced § 170.207(o)(1) and § 170.207(o)(2), respectively.

These codes reflect an attempt to exchange data regarding Sexual Orientation and Gender Identity in a consistent manner. Public feedback has, however, indicated that the required SNOMED CT® codes do not appropriately and accurately capture all applicable sexual

orientations or gender identities. We also understand that the existing standards reference specific codes from the HL7 Version 3 Standard, Value Set for NullFlavor, which are primarily used by health IT developers to indicate when there is not information available to represent Sexual Orientation or Gender Identity. The HL7 Gender Harmony Project has developed an informative document[39] that includes codes for Gender Identity such as "Nonbinary" that are not present in adopted values sets (§ 170.207(o)(2)). Additionally, representatives of the healthcare community and patient advocates have indicated a desire to expand the codes for Sexual Orientation and Gender Identity in the future to reflect the need to be more inclusive and to aid in identifying and addressing health disparities.

Accordingly, we propose to remove the requirement to use specific codes for representing Sexual Orientation and Gender Identity and have removed the codes as applicable vocabulary standards from USCDI v3. Rather, to continue to promote interoperability while also providing health care providers with flexibility to better support clinical care, certified health IT with Health IT Modules certified to criteria that reference § 170.213 would be required to be capable of representing Sexual Orientation and Gender Identity in SNOMED CT® when such information is exchanged as part of USCDI. We believe that it is best to let the health IT community develop the list of appropriate values for Sexual Orientation and Gender Identity, whether through implementation specifications or developing additional codes in SNOMED CT®.

We received strong support from commenters in response to our request during the Draft USCDI v3 public feedback period that the USCDI term Sex (Assigned at Birth) was too limiting for the industry. In subsequent exploration and analysis, we learned that this element is represented in different ways in a number of jurisdictions, so the meaning is unclear.

---

[39]https://confluence.hl7.org/download/attachments/81017270/HL7_GENDER_R1_INFORM_2021AUG.pdf?version=1&modificationDate=1639425849713&api=v2.

There was support to align the term in USCDI with the term Recorded Sex or Gender as part of the Gender Harmony Project. We understand that the term Recorded Sex or Gender is a more expansive term that defines the value of patient's sex recorded in administrative or legal documents, and indeed Sex (Assigned at Birth) could be considered as a specific type or recorded value with the identifier being assigned at birth. However, in order to be least disruptive to the industry, while at the same time, acknowledging the shortcomings of our current term, we have recharacterized the USCDI data element Sex (Assigned at Birth) to Sex. We note that this is presently a change in the name of the element and will have no immediate impact on health IT developers of certified health IT, which will continue to exchange the value of patient's sex they have been historically exchanging using USCDI. However, we anticipate this change to support future enhancements to improve precision in the meaning through work done by health IT developers of certified health IT.

USCDI v3 does not require the use of certain specific codes for representing Sex. As discussed previously, we propose to remove the requirement in § 170.315(a)(5)(i)(C) and § 170.315(b)(1)(iii)(G)(*3*) to code Sex according to the adopted value sets of HL7 Version 3 Value Sets for AdministrativeGender and NullFlavor as referenced in the value sets in § 170.207(n)(1). We propose instead to permit coding according to either the adopted value sets of HL7 Version 3 Value Sets for AdministrativeGender and NullFlavor as referenced in the value sets in § 170.207(n)(1) until December 31, 2025, or in accordance with the standard in proposed § 170.207(n)(2). These codes reflect an attempt to exchange Sex in a consistent manner. Our analysis has, however, indicated that the value sets do not appropriately and accurately capture all applicable values for Sex. Interested parties have indicated a desire to expand the codes for Sex in the future to be more inclusive and to aid in efforts to address health disparities. Accordingly, we no longer require the use of specific code sets for representing Sex and have removed the codes from USCDI v3. Rather, to continue to promote interoperability while also granting providers with flexibility to better support clinical care, certified health IT with Health

IT Modules certified to criteria that reference § 170.213 would be required to be capable of representing Sex in SNOMED CT when such information is exchanged as part of USCDI. We have similarly proposed to adopt the same changes for relevant certification criteria that reference these standards (*see* sections III.C.8 and III.C.9).

Finally, we have taken note of the substantial effort in this area to develop a clinically meaningful way for identifying a patient's sex from observable information (e.g., Clinical Observation, Radiology report, Laboratory report, genetic testing data) that may be suitable for clinical care, including the development of a new data element Sex for Clinical Use, which we may consider including in future standards adoption. We welcome public comment on this concept and approach. In addition, as noted in our proposals to the Patient Demographics and Observations certification criterion in § 170.315(a)(5), we have proposed to adopt the same changes for relevant certification criteria that reference these standards (*see* sections III.C.8 and III.C.9).

ONC also sought feedback on the value of adoption of an applicable vocabulary standard for patient addresses.[40] USCDI v1 required Current Address and Previous Address as discrete data elements, but there are no existing standards available for healthcare use cases. Through a collaboration between ONC and the standards development community, a new standard, the Unified Specification for Address in Health Care (US@),[41] emerged and was released in 2022. After receiving broad support from the public, ONC has incorporated the Project US@ Technical Specification version 1 as the applicable standard for Current Address and Previous Address in USCDI v3.

USCDI v3 includes six data elements added to the prior USCDI Patient Demographics/Information data class: Related Person's Name, Related Person's Relationship, Date of Death, Occupation, Occupation Industry, and Tribal Affiliation. Related Person's Name

[40] https://www.healthit.gov/sites/default/files/page/2022-01/Standards_Bulletin_2022-1.pdf#page=5.
[41] https://oncprojectracking.healthit.gov/wiki/pages/viewpage.action?pageId=180486153.

and Related Person's Relationship enable linkages between maternal and child records as well as identifying and linking other related persons, such as custodians and guardians. Date of Death supports patient matching, adverse event, public health, and vital records reporting. Occupation and Occupation Industry data elements were added to support public health, and to capture military service. Finally, Tribal Affiliation is captured by the Indian Health Service (IHS), an agency within the Department of Health and Human Services, to aid in the determination of eligibility for IHS services, care-coordination with non-tribal medical facilities, and identification of disparities in healthcare in and across American Indian and Alaska Native populations.

xii. Problems

As discussed in sub-section i of this section, USCDI v3 includes the SDOH Problems/Health Concerns data element added to the prior USCDI Problems data class. In addition, USCDI v3 includes Date of Diagnosis and Date of Resolution data elements added to the prior USCDI Problems data class to include timing elements for recorded and maintained problem lists within electronic health records.

xiii. Procedures

USCDI v3 includes the Reason for Referral data element added to the prior USCDI Procedures data class. This data element is already part of the Program requirements for the transitions of care certification criterion (§ 170.315(b)(1)(iii)(E)) in the ambulatory setting and is broadly implemented in health IT. As discussed in sub-section i of this section, the USCDI v3 also includes the SDOH Interventions data element added to the prior USCDI Procedures data class.

xiv. Updated versions of Vocabulary Standard Code Sets

In the 2015 Edition Final Rule, we established a policy for minimum standards code sets that update frequently throughout a calendar year at 80 FR 62612, and we have listed several standards as minimum standards code sets in 45 CFR part 170 subpart B. As with all adopted

minimum standards code sets, health IT can be certified to newer versions of the adopted baseline version minimum standards code sets for purposes of certification, unless the Secretary specifically prohibits the use of a newer version (see § 170.555 and 77 FR 54268). In USCDI v3, we included the most recent versions of the minimum standards code sets.

2. C-CDA Companion Guide Updates

We propose to adopt the HL7® CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes STU Companion Guide, Release 3 – US Realm in § 170.205(a)(6) (''C-CDA Companion Guide R3''). The C-CDA Companion Guide R3 provides supplemental guidance and additional technical clarification for specifying data in the C-CDA Release 2.1 for USCDI v2. However, it is our understanding that HL7 is working on updating the C-CDA R2.1 Companion Guide (Release 4) for USCDI v3. If the C-CDA Companion Guide Release 4 (R4) is published before the date of publication of the final rule, it is our intention to consider adopting the updated Companion Guide R4 that provides guidance and clarifications for specifying data in USCDI v3 since we propose to adopt USCDI v3 as the baseline in this proposed rule.

As mentioned above, HL7® has been updating the C-CDA Companion Guide to accommodate the new data classes and elements in each USCDI version. To allow developers to voluntarily update to USCDI v2, ONC included the C-CDA Companion Guide R3 in the SVAP Approved Standards List for 2022. ONC released the SVAP Approved Standards List for 2022 in June 2022. We anticipate that the C-CDA Companion Guide R4 would support updates included in proposed USCDI v3. We note that the adoption of the C-CDA Companion Guide R4 would align with our goal to increase the use of consistently implemented standards among health IT developers and improve interoperability. We propose to adopt the C-CDA Companion Guide R3 as a standard in § 170.205(a)(6) and incorporate it by reference in § 170.299. As stated above, if the C-CDA Companion Guide R4 is available at the time of publication of the final rule, we intend to consider adopting the C-CDA Companion Guide R4, which would support the updates included in proposed USCDI v3.

Consistent with our proposals in sections III.A and III.C.11, we propose to revise § 170.205(a)(5) to add that the adoption of the standard in § 170.205(a)(5) expires on January 1, 2025. Developers of certified health IT with Health IT Modules certified to criteria that reference § 170.205(a)(5) would have to update those Health IT Modules to § 170.205(a)(6) and provide them to customers by January 1, 2025. We clarify that under this proposal, for the time period up to and including December 31, 2024, HL7 CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2 would remain applicable as the minimum version required in the Program. This means that upon the effective date of a final rule, for the identified certification criteria, the following would apply as the minimum version for C-CDA for certification and compliance:

- HL7 CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2 (incorporated by reference in § 170.299) for the time period up to and including December 31, 2024,
- HL7 CDA® R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 3.

Further, we propose that Health IT Modules certified to the certification criteria below would need to update to the HL7 CDA® R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 3 in § 170.205(a)(6) by January 1, 2025:

- ‘‘transitions of care’’ (§ 170.315(b)(1)(iii)(A));
- ‘‘clinical information reconciliation and incorporation’’ (§ 170.315(b)(2)(i), (ii), and (iv));
- ‘‘care plan’’ (§ 170.315(b)(9)(ii));
- ‘‘view, download, and transmit to 3rd party’’ (§ 170.315(e)(1)(i)(A) and (B));
- ‘‘consolidated CDA creation performance’’ (§ 170.315(g)(6)(i)); and
- ‘‘application access—all data request’’ (§ 170.315(g)(9)(i)).

For the purposes of meeting that compliance timeline, we expect health IT developers to update their certified health IT without new mandatory testing and notify their ONC-ACB on the date at which they have reached compliance. Developers would also need to factor these updates into their next real world testing plan.

3. "Minimum Standards" Code Sets Updates

We established a policy in the 2015 Edition Final Rule for minimum standards code sets that update frequently (80 FR 62612). In prior rulemaking, we discussed the benefits of adopting newer versions of minimum standards code sets, including the improved interoperability and implementation of health IT with minimal additional burden (77 FR 54170). When determining whether to propose newer versions of minimum standards code sets, we consider the impact on interoperability and whether a newer version would require substantive effort for developers of certified health IT to implement. If adopted, newer versions of minimum standards code sets would serve as the baseline for certification and developers of certified health IT would be able to use newer versions of these adopted standards on a voluntary basis. We reiterate that while minimum standard code sets update frequently, perhaps several times in a single year, these updates are confined to concepts within the code system, not substantive changes to the standards themselves. We propose to adopt the following versions of the minimum standards codes sets listed below.

- § 170.207(a) – Problems

We propose to remove and reserve § 170.207(a)(3), IHTSDO SNOMED CT® International Release July 2012 and US Extension to SNOMED CT® March 2012 Release. We propose to revise § 170.207(a)(1), which is currently reserved, to reference SNOMED CT US Edition March 2022 and incorporate it by reference in § 170.299.

- § 170.207(c) – Laboratory tests

We propose to remove and reserve § 170.207(c)(2), Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.40. We propose to revise § 170.207(c)(1),

which is currently reserved, to reference LOINC Database version 2.72, February 16, 2022, and incorporate it by reference in § 170.299.

- § 170.207(d) – Medications

We propose to revise § 170.207(d)(1), which is currently reserved, to reference RxNorm July 5, 2022, Full Monthly Release and incorporate it by reference in § 170.299. We propose to reference the code sets specified in 45 CFR 162.1002(c)(1) which include International Classification of Diseases, 10th Revision, Clinical Modification (ICD-10-CM); International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS) (including The Official ICD-10-PCS Guidelines for Coding and Reporting); National Drug Codes (NDC); the combination of Health Care Financing Administration Common Procedure Coding System (HCPCS), as maintained and distributed by HHS, and Current Procedural Terminology, Fourth Edition (CPT-4), as maintained and distributed by the American Medical Association, for physician services and other healthcare services; Health Care Financing Administration Common Procedure Coding System (HCPCS) as maintained and distributed by HHS, for all other substances, equipment, supplies, or other items used in healthcare services; and Code on Dental Procedures and Nomenclature, in § 170.207(d)(4).

- § 170.207(e) – Immunizations

We propose to revise § 170.207(e)(1), which is currently reserved, to reference CVX – VaccinesAdministered, June 15, 2022, and incorporate it by reference in § 170.299. We also propose to revise § 170.207(e)(2), which is currently reserved, to reference NDC – Vaccine NDC Linker, updates through July 19, 2022, and incorporate it by reference in § 170.299.

- § 170.207(f) – Race and ethnicity

We propose to add § 170.207(f)(3) to reference CDC Race and Ethnicity Code Set Version 1.2 (July 2021) and incorporate it by reference in § 170.299.

- § 170.207(m) – Numerical references

We propose to revise § 170.207(m)(2), which is currently reserved, to reference the Unified Code of Units of Measure (UCUM), Revision 2.1, November 21, 2017, and incorporate it by reference in § 170.299.

- § 170.207(n) – Sex

As described in this proposed rule in sections III.C.1 and III.C.8, we propose to revise § 170.207(n)(2), which is currently reserved, to reference the version of SNOMED CT ® codes specified in § 170.207(a)(1). We also propose to add § 170.207(n)(3) to reference the version of LOINC ® codes specified in § 170.207(c)(1).

- § 170.207(o) – Sexual orientation and gender information

We propose to change the heading of § 170.207(o) from "sexual orientation and gender identity" to "sexual orientation and gender information" to acknowledge that § 170.207(o) may include standard code sets to support other gender related data items. Additionally, as described in this proposed rule in sections III.C.1 and III.C.8, we propose to add § 170.207(o)(3) to reference the version of SNOMED CT ® codes specified in § 170.207(a)(1) and to add § 170.207(o)(4) to reference the version of LOINC ® codes specified in § 170.207(c)(1) for Pronouns.

- § 170.207(p) – Social, psychological, and behavioral data

We propose to revise § 170.207(p)(1) through (8) to reference the version of LOINC® codes specified in proposed § 170.207(c)(1) instead of § 170.207(c)(3). We propose to revise § 170.207(p)(4), (5) and (7) and (8) to reference the version of the Unified Code of Units of Measure in proposed § 170.207(m)(2), instead of § 170.207(m)(1). We also propose to revise § 170.207(p)(6) to include a reference to the version of the Unified Code of Units of Measure in proposed § 170.207(m)(2).

- § 170.207(r) – Provider type

We propose to revise § 170.207(r)(2), which is currently reserved, to reference Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy, October 29, 2021, and incorporate it by reference in § 170.299.

- § 170.207(s) – Patient insurance

We propose to revise § 170.207(s)(2), which is currently reserved, to reference Public Health Data Standards Consortium Source of Payment Typology Code Set Version 9.2 (December 2020) and incorporate it by reference in § 170.299.

In addition to updating the minimum standards code sets listed above, we propose to update the certification criteria that reference those minimum standards. We propose to update some of the certification criteria that reference § 170.207(a) Problems, by replacing the reference to § 170.207(a)(4) in those criteria that reference it with a reference to the new proposed § 170.207(a)(1). These criteria include § 170.315(a)(12), (b)(1)(iii)(B)(*2*), (b)(6)(ii)(B)(*2*), (c)(4)(iii)(I), and (f)(4)(ii). We also propose to update § 170.315(f)(3)(ii) by replacing the reference to § 170.207(a)(3) with a reference to the new proposed § 170.207(a)(1). We propose to update the certification criteria that reference § 170.207(c) Laboratory Tests by replacing the references to § 170.207(c)(2) and (c)(3) in those criteria with a reference to the new proposed § 170.207(c)(1). These criteria include § 170.315(f)(3)(ii) and (f)(4)(ii).

We propose to update two certification criteria that reference § 170.207(e) Immunizations. We propose to update the certification criterion § 170.315(f)(1)(i)(B), which references § 170.207(e)(3), to instead reference the new proposed § 170.207(e)(1). We also propose to update the certification criterion § 170.315(f)(1)(i)(C), which references § 170.207(e)(4), by replacing the reference to § 170.207(e)(4) in that criterion with a reference to the new proposed § 170.207(e)(2).

We propose to update several certification criteria that reference § 170.207(f) Race and Ethnicity. We propose to update certification criteria that reference § 170.207(f)(2) to instead

reference the new proposed § 170.207(f)(3). These criteria include § 170.315(a)(5)(i)(A)(*1*) and (*2*) and § 170.315(c)(4)(iii)(H).

As described in sections III.C.1 and III.C.8 of this proposed rule, we propose to update criteria that reference § 170.207(n) Sex by updating criteria that reference § 170.207(n)(1) to reference the new proposed § 170.207(n)(2). More specifically, we propose to update § 170.315(a)(5)(i)(C) to reference § 170.207(n)(1) for the time period up to and including December 31, 2025, or to reference § 170.207(n)(2). We also propose to update § 170.315(c)(4)(iii)(G) to reference § 170.207(n)(2) and to update § 170.315(b)(1)(iii)(G)(*3*) to reference the standards adopted in § 170.213.

Additionally, as described in sections III.C.1 and III.C.8 of this proposed rule, we propose to update the criteria that reference § 170.207(o) Sexual orientation and gender information (as we propose to rename the criterion) by updating criteria that reference § 170.207(o)(1) and (2). We propose to replace the reference to § 170.207(o)(1) in § 170.315(a)(5)(i)(D) with a reference to the new proposed § 170.207(o)(3) and propose to replace the reference to § 170.207(o)(2) in § 170.315(a)(5)(i)(E) with a reference to the new proposed § 170.207(o)(3). More specifically, we propose to update § 170.315(a)(5)(i)(D) to reference § 170.207(o)(1) for the time period up to and including December 31, 2025, or to reference § 170.207(o)(3). We propose to update § 170.315(a)(5)(i)(E) to reference § 170.207(o)(2) for the time period up to and including December 31, 2025, or to reference § 170.207(o)(3).

We also propose to update § 170.315(c)(4)(iii)(C), which references § 170.207(r) Provider Type. Specifically, we propose to replace the reference to § 170.207(r)(1) in that criterion with a reference to the new proposed § 170.207(r)(2). We also propose to update § 170.315(c)(4)(iii)(E), which references § 170.207(s) Patient insurance. Specifically, we propose to replace the reference to § 170.207(s)(1) in that criterion with a reference to the new proposed § 170.207(s)(2).

4. Electronic Case Reporting

a. Background

Case reporting serves as early notification to Public Health Agencies (PHAs) for potential disease outbreaks and includes information that enables PHAs to start contact tracing and other prevention measures. Case reports include critical clinical information that is not included in syndromic surveillance or laboratory reporting and can help illuminate the impact of comorbidities, treatments, and variable access to care. Every state has laws requiring providers to submit case reports of specific reportable diseases and conditions. Electronic case reporting is the automated, real-time, bidirectional exchange of case report information between EHRs and PHAs.[42] Electronic case reporting uses standard codes to trigger the transfer of relevant clinical data to PHAs for case investigation and follow-up, including data on demographics, comorbidities, immunizations, medications, occupation, and other treatments. Most states do not require electronic submission of case reports; rather, case reporting often occurs through outdated manual methods (e.g., fax, email, or phone) which results in delays, underreporting, and incomplete or inaccurate case data.[43, 44] This manual case reporting also imposes burdens on health care providers, taking staff time away from patients to submit case reports and comply with state reporting requirements.

ONC established initial content exchange standards in 45 CFR 170.205(g)(1) and (g)(2) to support a version of HL7® v2 for "electronic submission to public health agencies for surveillance or reporting" in the 2010 "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology" Interim Final Rule (75 FR 2033). These standards were not specific to electronic case reporting; rather they supported the more generic submission of information to PHAs. The

---

[42] Centers for Disease Control & Prevention (CDC). Electronic Case Reporting Fact Sheet. Available at: https://www.cdc.gov/ecr/docs/eCR-Fact-Sheet-508.pdf.
[43] ONC. Interoperability Standards Advisory. Case Reporting to Public Health: https://www.healthit.gov/isa/case-reporting-public-health-agencies.
[44] Ashley Antonelli and Joseph Leonard. CMS is mandating new electronic case reporting requirements. Here's how providers can prepare. Advisory Board. https://www.advisory.com/blog/2021/12/electronic-case-reporting.

"transmission to public health agencies – electronic case reporting" certification criterion in § 170.315(f)(5) was later adopted in the 2015 Edition Final Rule to "support the electronic transmission of case reporting information to public health agencies" as part of the CMS EHR Incentive Programs (80 FR 62667).

In the ONC 2015 Edition Proposed Rule (80 FR 16804), we requested comment on whether to adopt a standardized method for electronic case reporting, including potentially adopting the "IHE Quality, Research, and Public Health Technical Framework Supplement, Structured Data Capture, Trial Implementation (September 5, 2014) standard" and the "HL7 FHIR Implementation Guide: SDC DSTU that would be balloted in mid-2015 in place of, or together with, the IHE Quality, Research, and Public Health Technical Framework Supplement" (80 FR 16855). In response to comments, we did not adopt a standard for this criterion in the 2015 Edition Final Rule, but instead outlined functional requirements that Health IT Modules would need to support for certification to the electronic case reporting criterion. These functional requirements included a requirement that a Health IT Module support the ability to "(1) consume and maintain a table of trigger codes to determine which encounters should initiate an initial case report being sent to public health to determine reportability; and (2) when a trigger is matched, create an initial case report that includes specific data (Common Clinical Data Set; encounter diagnoses; provider name, office contact information, and reason for visit, and an identifier representing the row and version of the trigger table that triggered the case report)" (80 FR 62667). In addition to establishing these functional requirements in the 2015 Edition Final Rule, we also described additional functionalities that would help support electronic case reporting to public health but did not adopt them as requirements for the ONC Health IT Certification Program (80 FR 62667); these functional requirements included: "(3) receive and display additional information, such as a "notice of reportability" and data fields to be completed; and (4) submit a completed form."

ONC described some of the context for standards development and the future for electronic case reporting. We stated "[a]s standards evolve . . . the future might include a FHIR-based approach. Therefore, we believe this overall initial certification approach establishes necessary flexibility within the ONC Health IT Certification Program related to electronic case reporting in that as technical approaches evolve to accomplish electronic case reporting they can be certified. In the future, we may be able to consider a specific standard for certification through rulemaking" (80 FR 62667).

In 2017, ONC established self-declaration as the demonstration method for electronic case reporting.[45] In the ONC Cures Act Final Rule (85 FR 25642), electronic case reporting was included as part of the Real World Testing Condition and Maintenance of Certification requirements (codified in 45 CFR 170.405), which require health IT developers with Health IT Modules certified to criteria specified in § 170.405(a) to "successfully test the real world use of those Health IT Module(s) for interoperability (as defined in 42 U.S.C.300jj(9) and § 170.102) in the type of setting in which such Health IT Module(s) would be/is marketed" (85 FR 25948). Health IT developers with Health IT Modules certified to applicable criteria have the flexibility to establish their own Real World Testing plan and submit results based on measures they develop. However, it is expected that developers use Real World Testing plans and results to demonstrate ongoing conformance to standards and functionality required as part of the Program, per 45 CFR § 170.405(b)(2)(i).

We also modified § 170.315(f)(5)(iii)(B) in the ONC Cures Act Final Rule to require Health IT Modules to support creation of electronic case reports based on (1) the data classes expressed in the standards in § 170.213, or (2) the Common Clinical Data Set (CCDS) until December 31, 2022 (85 FR 25667). This was proposed as part of a Program-wide effort to transition Health IT Modules certified to certification criteria that referenced the CCDS to

[45] https://www.healthit.gov/test-method/transmission-public-health-agencies-electronic-case-reporting.

instead support the USCDI v1 (85 FR 25670). ONC subsequently clarified that while either the CCDS or the USCDI v1 data set needed to be supported, "a health IT developer must attest to their product's ability to support the referenced standard(s) in § 170.315(f)(5)(iii)(B)(*1*) or (*2*). However, individual PHAs may require a subset of this data for reporting."[46]

b. Standards Landscape for Case Reporting

Since ONC adopted 45 CFR 170.315(f)(5) as a functional requirement for Health IT Modules in the 2015 Edition, standards development organizations (SDOs), public health, and interested parties within the healthcare industry have balloted several standards related to electronic case reporting. The standards were produced and developed through a collaborative effort among many partners, including CDC, the Council of State and Territorial Epidemiologists (CSTE), the Association of State and Territorial Health Officials (ASTHO), the Association of Public Health Laboratories (APHL), electronic health record (EHR) developers, and the Health Level Seven (HL7) Public Health (PH) Work Group.[47] These standards pertain to both HL7® FHIR and HL7® CDA and include multiple Implementation Guides (IGs).

Recognizing advancement of standards development in this area, ONC analyzed the currently balloted standards for potential inclusion in the existing 45 CFR 170.315(f)(5) criterion. ONC examined the following standards for potential inclusion as a part of this criterion:

- **HL7 FHIR® Implementation Guide: Electronic Case Reporting (eCR) – US Realm STU2 (HL7 FHIR eCR IG):**[48] The HL7 FHIR eCR IG contains multiple FHIR profiles that correspond to the HL7 CDA eICR and the HL7 CDA Reportability Response standards. This IG also includes profiles for electronic Reporting and Surveillance

[46] For further information see: § 170.315(f)(5) Certification Companion Guide available here: https://www.healthit.gov/test-method/transmission-public-health-agencies-electronic-case-reporting.
[47] See work group membership at: https://confluence.hl7.org/display/PHWG/Public+Health+Work+Group.
[48] http://build.fhir.org/ig/HL7/case-reporting/index.html.

Distribution (eRSD) that enables the electronic distribution of trigger codes and reporting guidance and parameters from public health to clinical care.

- **HL7 FHIR Electronic Initial Case Report (eICR) transaction and profile:**[49] The HL7 FHIR eCR IG specifies a standardized method for the communication of an eICR to a PHA using the HL7® FHIR standard. The eICR profiles are intended to contain the data elements necessary to initiate a public health investigation or other appropriate public health action based on a potentially reportable case identified by a healthcare organization.
- **HL7 FHIR Reportability Response (RR) transaction and profile:**[50] The HL7 FHIR eCR IG also describes a standardized method for a PHA to communicate a RR to a healthcare organization that initiated an eICR. The RR profiles can include determination of reportability information, contact information for the involved PHAs, requests for case investigation supplemental data that may not have been recorded in the process of care, condition-specific information from public health, and an acknowledgment that a report has been successfully conveyed. The IG notes that there may be several different intermediaries involved in the transmission of RR messages including Health Information Exchanges and Health Data Networks.

- **HL7 FHIR Electronic Reporting and Surveillance Distribution (eRSD) transaction and profiles:**[51] The HL7 FHIR eRSD profiles support the distribution of reporting guidance and trigger code value sets from PHAs to healthcare organizations. The eRSD profiles are specified in the HL7 FHIR eCR IG but are intended to be used by health IT that supports either CDA or FHIR-based approaches to electronic case reporting.[52] The

[49] http://build.fhir.org/ig/HL7/case-reporting/electronic_initial_case_report_eicr_transaction_and_profiles.html.
[50] http://build.fhir.org/ig/HL7/case-reporting/reportability_response_rr_transaction_and_profiles.html.
[51] http://build.fhir.org/ig/HL7/case-reporting/electronic_reporting_and_surveillance_distribution_ersd_transaction_and_profiles.html.
[52] See page 11 of CDA eICR IG, at: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=436.

eRSD profiles include an "eRSD Specification Library," which is composed of a constrained HL7 FHIR PlanDefinition resource and the Trigger Value Set Library, and an "eRSD Supplemental Library," which is composed of a RuleFilters library and a Supplemental Value Set library. These can be contained and transacted via a HL7 FHIR Bundle. The eRSD Specification Library, which can optionally be used in combination with the eRSD Supplemental Library, supports the distribution of reporting guidance and parameters, trigger code value sets, and more complex reporting rules to determine whether a condition may be reportable to public health. According to HL7, the eRSD profiles can support either CDA or FHIR-based approaches to electronic case reporting.[53]

- **HL7 CDA® R2 Implementation Guide: Public Health Case Report – the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1 – US Realm (HL7 CDA eICR IG)**[54]
    - **HL7 CDA Electronic Initial Case Report (eICR):** The purpose of the HL7 CDA eICR IG is to specify a standard for the creation of an eICR in Clinical Document Architecture, Release 2 (CDA R2) US Realm format. The eICR is intended to contain the data elements necessary to initiate a public health investigation or other appropriate public health action.
- **HL7 CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1 – US Realm (HL7 CDA RR IG)**[55]
    - **HL7 CDA Reportability Response (RR):** The HL7 CDA RR IG was produced and developed to specify a standard for a RR document using the HL7 CDA R2 standard and is a companion to the HL7 CDA eICR IG. The RR can function to: Communicate the reportability status, for the responsible PHA(s), of each condition included in the eICR; identify who (a PHA or an intermediary) prepared

[53] See page 11 of CDA eICR IG, at: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=436.
[54] https://www.hl7.org/implement/standards/product_brief.cfm?product_id=436.
[55] https://www.hl7.org/implement/standards/product_brief.cfm?product_id=470.

the RR; provide contact information for the responsible PHA(s); provide suggested or required clinical follow-up activities from the responsible PHA(s), including any additional reporting needs or infection control activities; and confirm eICR receipt and processing.

- **Reportable Conditions Trigger Codes Value Set for Electronic Case Reporting. RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022**[56]
    - The Reportable Condition Trigger Codes (RCTC) are a nation-wide set of standardized codes to be implemented within an EHR that provide a preliminary identification of events that may be of interest to PHAs for electronic case reporting. The RCTC are the first step in a two-step process to determine reportability. The RCTC are single factor codes that represent any event that may be reportable to any PHA in the United States. A second level of evaluation still must be done against jurisdiction-specific reporting regulations, to confirm whether the event is reportable and to which PHA or agencies. The RCTC currently includes ICD 10 CM, SNOMED CT, LOINC, RxNorm, CVX, and CPT codes, representing condition-specific diagnoses, resulted lab tests names, lab results, lab orders for conditions reportable upon suspicion, and medications for select conditions.

c. Proposed Updates to Case Reporting in § 170.315(f)(5)

We propose a deliberate path towards greater standardization and specification of electronic case reporting, moving from functional requirements to standards-based requirements in § 170.315(f)(5) to improve consistency of implementations and interoperability over time. Improvements in consistent implementation and case report interoperability would enable PHAs to have a vastly improved picture of where and when disease outbreaks occur. These standards

[56] https://ecr.aimsplatform.org/ehr-implementers/triggering/.

would also enable health care providers and PHAs to engage in better, bi-directional exchange of information.

In this rule, we propose to revise the criterion in § 170.315(f)(5) to adopt consensus-based, industry-developed standards. These proposed standards would supplement the functional, descriptive requirements in the present criterion in § 170.315(f)(5) for the time period up to and including December 31, 2024, and ultimately replace them. We note that these electronic standards are standards-based representations of the functional requirements described in the existing criterion in § 170.315(f)(5). We propose to allow certification to the existing version of the certification criterion, which we propose to move to § 170.315(f)(5)(i), or the revised version of the certification criterion in proposed § 170.315(f)(5)(ii) beginning on the effective date of the final rule, and to allow certification to only the revised certification criterion in § 170.315(f)(5)(ii) after December 31, 2024.

For the revised version of the certification criterion, we propose requirements in regulation text that align with the functionalities included in the specified CDA and FHIR-based IGs proposed for adoption for the purpose of electronic case reporting. We propose to adopt three standards-based requirements for Health IT Modules certified to the revised certification criterion in § 170.315(f)(5). Specifically, in § 170.315(f)(5)(ii) we propose that a Health IT Module enable a user to:

- Consume and process electronic case reporting trigger codes and parameters and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code value set in § 170.205(t)(4) contained in the eRSD Specification Library as specified in the HL7 FHIR eCR IG in § 170.205(t)(1);
- Create a case report consistent with at least one of the following standards:
    - The eICR profile of the HL7 FHIR eCR IG in § 170.205(t)(1), or
    - The HL7 CDA eICR IG in § 170.205(t)(2);

- Receive, consume, and process a case report response that is formatted to either the RR profile of the HL7 FHIR IG in § 170.205(t)(1) or the HL7 CDA RR IG in § 170.205(t)(3); and
- Transmit a case report electronically to a system capable of receiving an electronic case report.

For the proposal in § 170.315(f)(5)(ii)(A) requiring a system to consume and process trigger codes, we propose that a certified Health IT Module identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code value set in § 170.205(t)(4) contained in the eRSD Specification Library as specified in the HL7 FHIR eCR IG in § 170.205(t)(1) to support the functionality in § 170.315(f)(5)(ii)(A). We describe the standards and implementation specifications in further detail in the subsequent section of this proposed rule.

For the proposal in § 170.315(f)(5)(ii)(B) requiring a Health IT Module to enable a user to create a case report consistent with at least one of the proposed standards in that proposed certification criterion, we clarify that "at least," means that Health IT Modules must support either the HL7 CDA eICR IG (in § 170.205(t)(2)) or the eICR profile of the HL7 FHIR eCR IG (in § 170.205(t)(1)), or both the CDA and FHIR IGs for the purposes of certification. Our intent is that a certified Health IT Module supports at least one of these kinds of IGs, but we do not preclude a Health IT Module from supporting both. For the proposal in § 170.315(f)(5)(ii)(C) to require that a certified Health IT Module support the receipt, consumption, and processing of reportability responses, we propose that a certified Health IT Module may implement this capability for receipt of responses formatted to either the reportability response profile of the HL7 FHIR eCR IG in § 170.205(t)(1) or the reportability response profile of the HL7 CDA RR IG in § 170.205(t)(3). However, we seek comment on whether we should instead require Health IT Modules to implement this capability for reportability responses formatted to both standards. As part of these proposed standards-based requirements in § 170.315(f)(5)(ii), we reiterate that

Health IT Modules would need to follow the respective IG requirements for all “mandatory” and “must support” data elements listed in each IG, as applicable. Specifically, by “mandatory” we mean support for data elements with minimum cardinality requirements equal to or greater than “1.” By “must support,” we mean “must support” as it is defined in the referenced HL7 FHIR implementation specifications. For equivalency of “must support” data in CDA IGs, a certified Health IT Module must support data elements with minimum cardinality requirements equal to or greater than "1" or a conformance verb of "SHALL" even if null values are allowed by the applicable data elements in the referenced CDA IGs.

Additionally, we propose in § 170.315(f)(5)(ii) a fourth non-standards based functional requirement for Health IT Modules certified to § 170.315(f)(5)(ii). We propose in § 170.315(f)(5)(ii)(D) that such Health IT Modules be required to enable a user to electronically transmit a case report to a system capable of receiving case reports electronically. We emphasize that this fourth requirement is agnostic to the recipient of the electronic case report and does not prescribe a specific transport standard, reporting mechanism, or platform. We propose that certification to the updated criterion would be available for Health IT Modules upon the effective date of the final rule. In addition, because certification to § 170.315(f)(5)(i) would only be available through December 31, 2024, health IT developers with Health IT Modules certified to the § 170.315(f)(5) criterion based on meeting the requirements of § 170.315(f)(5)(i) would be required to update and provide their customers with a Health IT Module updated to the revised certification criterion by December 31, 2024, to keep their certification to § 170.315(f)(5) active, consistent with our proposals in sections III.A and III.C.11.

Finally, we note that for Health IT Modules certified to § 170.315(f)(5), the developer of such health IT must continue to demonstrate conformance to these requirements for Real World Testing plans and results per the requirements in § 170.405 regardless of whether the Health IT Module is certified to § 170.315(f)(5)(i) or (f)(5)(ii).

d. Proposed Adoption of Standards for Electronic Case Reporting

ONC has received feedback from numerous interested parties, including developers of certified health IT, PHAs, and federal partners, that it would be premature to identify a single set of standards for case reporting. We understand that many PHAs use systems that handle CDA-based messages and that many PHAs have not adopted FHIR-based messaging information systems. However, we also have heard that there is interest among some PHAs to leverage FHIR, and we see an opportunity to align requirements for electronic case reporting with other Program requirements that leverage FHIR for developers of certified health IT.

Given the emerging interest in FHIR, and the need to support current public health capabilities, we propose in § 170.315(f)(5)(ii)(B) to require a Health IT Module to create a case report for electronic transmission according to at least one of the following two HL7® standards: in accordance with the eICR profiles specified in the HL7 FHIR eCR IG in § 170.205(t)(1) or in accordance with the eICR profiles specified in the HL7 CDA eICR IG in § 170.205(t)(2). We anticipate that health IT developers would choose to support a CDA-based approach or a FHIR-based approach to support this criterion, but we would not want to preclude a developer from pursuing both approaches with its Health IT Module(s). We clarify that for purposes of Program requirements, a Health IT Module certified to § 170.315(f)(5) would not need to support both approaches; however, we acknowledge the possibility that a developer of certified health IT may choose to support both approaches to meet the needs of its customer base. As part of the proposed requirement in § 170.315(f)(5), we propose that Health IT Modules support all "mandatory" and "must support" data elements as applicable in either the eICR profiles of the HL7 FHIR eCR IG[57] or the HL7 CDA eICR IG,[58] depending on which approach they choose. We invite comment on our proposal to require that Health IT Modules certified to §

[57] Available at: http://hl7.org/fhir/us/ecr/artifacts.html#eicr-profiles.
[58] See page 73 of the HL7 CDA eICR IG, "6.3 Mapping of Data Elements to CDA R2 Templates" at: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=436.

170.315(f)(5) support at least the eICR profiles of the HL7 FHIR eCR IG or the HL7 CDA eICR IG.

We propose in § 170.315(f)(5)(ii)(C) to require that Health IT Modules certified to § 170.315(f)(5) support the receipt, consumption, and processing of reportability responses formatted according to the RR profiles defined in the HL7 FHIR eCR IG or the HL7 CDA RR IG. We seek comment on whether we should instead require Health IT Modules to have the capability to receive, consume and process a reportability response formatted to both standards. Again, as part of the proposed consume and process reportability response requirement in § 170.315(f)(5)(ii)(C), we propose that Health IT Modules support consuming and processing all "mandatory" and "must support" data elements as applicable in either the RR profiles of the HL7 FHIR eCR IG or the RR profiles of the HL7 CDA RR IG,[59] depending on which approach the developer chooses. Specifically, we note that Health IT Modules supporting a FHIR-based approach must support the RR profiles, and corresponding "mandatory," and "must support" data elements, according to section 10.0.2 of the FHIR eCR IG.[60] It is critical for the health IT industry to support clinicians or other appropriate personnel (e.g., infection preventionists) in receiving reportable response information in a usable format from public health, in order to enhance communication between the public health community and the healthcare community. Processing the reportability response will help clinicians access responses from public health, including where the PHA has deemed a case reportable.

We believe that the health IT industry eventually will coalesce with the public health community around a single set of standards, but for the near-term, we believe that both CDA-based and FHIR-based standards will be leveraged for eICR and RR, depending on the unique circumstances of geography, jurisdiction, and users of certified health IT. We reiterate that health IT developers may choose to support both CDA and FHIR-based approaches for electronic case

---

[59] See page 63 of the HL7 CDA RR IG, "6.3 Mapping of Elements to CDA R2 Templates." Available at: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=470*.

[60] Available at: http://hl7.org/fhir/us/ecr/artifacts.html#reportability-response-profiles.

reporting, but we only propose to require support of at least one of these approaches for Health IT Modules certified to § 170.315(f)(5) pursuant to the Program. Additionally, health IT developers may choose to support functionalities beyond these requirements depending on their approach to electronic case reporting. We invite comment on our proposal to require Health IT Modules certified to § 170.315(f)(5) to support at least the RR profiles of the HL7 FHIR eCR IG or the HL7 CDA RR IG.

Finally, we propose in § 170.315(f)(5)(ii)(A) that a Health IT Module certified to § 170.315(f)(5) support the consumption and processing of electronic case report trigger codes and parameters based on a match from Reportable Conditions Trigger Code value set in § 170.205(t)(4) received from the eRSD profiles as specified in the HL7 FHIR eCR IG in § 170.205(t)(1).

We understand that the eRSD profiles include both trigger codes, as described in the RCTC value set, and more complex reporting parameters. We understand that the basics of electronic case reporting require a health IT developer to use, at a minimum, reportable conditions as represented in the RCTC value set to match with a patient visit and/or encounter, so we propose to require that Health IT Modules support the eRSD profiles in the HL7 FHIR eCR IG proposed § 170.205(t)(1) using the RCTC value set in proposed § 170.205(t)(4).

We propose to require certified Health IT Modules to support the ability to consume and process the eRSD profiles, which include the RCTC value set, regardless of whether such a Health IT Module supports a FHIR-based or CDA-based approach to certification. As part of the proposal to require Health IT Modules to consume and process the eRSD profiles in § 170.315(f)(5)(ii)(A), we clarify that a Health IT Module must support consuming and processing all "mandatory" and "must support" data elements of the eRSD Specification Library and the eRSD Supplemental Library specified in section 10.0.3 of the HL7 FHIR eCR IG.[61]

[61] Available at: http://hl7.org/fhir/us/ecr/artifacts.html#ersd-profiles-instances.

We clarify that a certified Health IT Module need only support parsing and consuming the eRSD Specification Library and eRSD Supplemental Library because we understand that health IT developers may choose to either manually encode the electronic case reporting trigger logic into Health IT Modules or may support a more automated process for encoding the trigger logic into Health IT Modules. We request comment on this approach and on whether there is general support of the eRSD Specification Library and eRSD Supplemental Library for electronic case reporting triggering.[62]

Per documentation in the HL7 CDA eICR IG,[63] we believe that the HL7 FHIR eRSD profile can be used by certified Health IT Modules that leverage either the FHIR-based or CDA-based approaches we propose. We invite comment on the proposed adoption of the eRSD profiles for Health IT Modules certified to § 170.315(f)(5) and our understanding that the eRSD profiles can be used by Health IT Modules that implement a CDA-approach to electronic case reporting. We welcome comment on the eRSD profiles within the HL7 FHIR IG and its use by certified Health IT Modules that choose a CDA-based approach to certification.

We note that in the 2015 Edition Final Rule, we established a policy for minimum standards code sets that update frequently throughout a calendar year (80 FR 62612), and we have listed several standards as minimum standard code sets in 45 CFR part 170 subpart B. As with all adopted minimum standards code sets, health IT can be certified to newer versions of the adopted baseline version minimum standards code sets for purposes of certification, unless the Secretary specifically prohibits the use of a newer version (*see* § 170.555 and 77 FR 54268).

The RCTC value set comprises single factor codes that represent any event that may be reportable to any PHA in the United States. The RCTC value set currently includes ICD-10 CM, SNOMED CT, LOINC, RxNorm, CVX, and CPT, representing condition-specific diagnoses,

---

[62] See http://hl7.org/fhir/us/ecr/STU2.1/electronic_reporting_and_surveillance_distribution_ersd_transaction_and_profiles.html#suspected-reportability-criteria.

[63] See page 11 of HL7 CDA eICR IG at: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=436.

resulted lab tests names, lab results, lab orders for conditions reportable upon suspicion, and medications for select conditions. Given that the contents of the RCTC value set update frequently, we propose to recognize the RCTC value set as a minimum standard code set in § 170.205(t)(4), and we propose that the reference standard for the RCTC value set be established as RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022, IBR approved (incorporated by reference in § 170.299) (available at: https://ecr.aimsplatform.org/ehr-implementers/triggering/). This approach will have the practical impact of enabling ONC to reference a persistent version of the RCTC value set, establishing a baseline for use in the Program, and will enable developers of certified health IT to support newer or updated versions of RCTC value sets for their customers as soon as new releases are available, unless the Secretary prohibits the use of a newer version for certification. Given that the RCTC value set reflects both current and emerging reportable conditions, we believe it is important to frame it as a minimum standard code set, thus making newer versions available for frequent update by developers of certified health IT. At a minimum, we expect that Health IT Modules certified to § 170.315(f)(5)(ii) to support this reference version of the RCTC value set (RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022, IBR approved (incorporated by reference in § 170.299)). Health IT Modules certified to § 170.315(f)(5)(ii) may voluntarily support an updated version (e.g., a subsequent release) of the RCTC value set, and we anticipate that health IT developers would be incentivized by their customers to take advantage of this opportunity to voluntarily support updated versions of the RCTC value set because it will include new codes reflecting new or emerging infectious diseases. We note that there is no requirement to support the RCTC value set for Health IT Modules certified to § 170.315(f)(5)(i). We invite comment on these proposals and our assessment regarding the desirability of developers of certified health IT to use updated versions of the RCTC value set in their Health IT Modules.

The eCR FHIR IG is a relatively new standard with standard for trial use (STU1) status published on January 29, 2020, STU2 published on January 18, 2022, and an updated STU2

published on August 31, 2022. While we propose to adopt the eICR, RR, and eRSD profiles of the FHIR eCR IG as described in this section, we are also interested in receiving specific comments from the public regarding their experiences with implementation and use of the FHIR eCR IG.

We note that requiring standards in the proposed § 170.315(f)(5)(ii)(A), (B), and (C) for Health IT Modules certified to § 170.315(f)(5) will enable ONC to approve newer versions of these standards through SVAP per existing provisions at 45 CFR 170.405(b)(8) and 170.405(b)(9), which will enable health IT developers to voluntarily keep pace with the latest improvements in standards outside the timeframes dictated by the rulemaking process. We invite comment on the proposed adoption of these HL7 standards and IGs, including whether we should finalize only the FHIR-based standards and IGs or only the CDA-based standards and IGs, or both as proposed.

e. Proposal for Reporting

Finally, we propose in § 170.315(f)(5)(ii)(D) to require Health IT Modules certified to § 170.315(f)(5) to be capable of electronically reporting to a system that is capable of receiving case reports electronically. This proposed reporting function would be agnostic to a specific standard or reporting mechanism or platform. We note that all currently balloted HL7 standards directly reference optional use of a centralized decision support solution called the Reportable Condition Knowledge Management System (RCKMS) made available through the Association of Public Health Laboratories (APHL) Informatics Messaging Services (AIMS) platform.[64] We understand that many PHAs directly input their jurisdiction's reporting criteria into RCKMS through the AIMS platform, so that eICRs from a healthcare setting can be processed against those reporting criteria to determine if the case report is reportable and to which PHA(s) the report should be sent.

[64] https://www.rckms.org/.

At this time, ONC is not proposing to require Health IT Modules certified to § 170.315(f)(5) to specifically connect to AIMS or support RCKMS to meet the proposed requirements in § 170.315(f)(5)(ii)(D). While we understand the role AIMS and RCKMS play in a centralized, hub-and-spoke model for electronic case reporting, we propose that the functional requirements for § 170.315(f)(5)(ii)(D) remain agnostic as to which reporting platform and which decision support tool are used. However, we note that different PHAs are likely to have different reporting requirements, including specific systems, decision support logic, or both. While we are not requiring the use of a specific reporting platform, the certified functionality in § 170.315(f)(5)(ii)(D) requires that the Health IT Module be capable of transmitting electronic case reports consistent with the reporting requirement(s) established by a PHA. We know that some states and jurisdictions have implemented separate electronic reporting requirements that do not involve the use of the AIMS platform, RCKMS, or both, and we believe that reporting requirements should be determined by PHAs at this time. Therefore, developers of certified health IT can meet the requirements in § 170.315(f)(5)(ii)(D) by demonstrating that their Health IT Modules possess the capability to send a case report electronically to any system capable of receiving a case report. A developer of certified health IT could also elect to support more than one reporting option in a Health IT Module.

As stated previously, the primary motivation for proposing standards for electronic case reporting in § 170.315(f)(5) is to enable the use of SVAP to allow industry to leverage improved versions of standards on an expedited timeline, as the standards continue to evolve and mature. We encourage members of the standards development community to iterate and improve these HL7®-balloted standards for electronic case reporting so that the benefits of this technology may be widely shared.

5. Decision Support Interventions and Predictive Models

Since 2010, the Program has maintained a CDS certification criterion, consistent with the "qualified electronic health record" definition in section 3000(13) of the PHSA, which defines a

qualified EHR as an electronic record of health-related information on an individual that has the capacity to "provide clinical decision support" (42 U.S.C. § 300jj(13)(B)(i)). The initial requirements for the CDS certification criterion were intended to ensure that Health IT Modules support broad categories of CDS while being agnostic toward the intended use of the CDS beyond drug-drug and drug-allergy interaction checks. The initial CDS criterion required that a Health IT Module could: (1) implement rules, "according to specialty or clinical priorities;" (2) "automatically and electronically generate and indicate in real-time, alerts and care suggestions based upon clinical decision support rules and evidence grade;" and (3) track, record, and generate reports on the number of alerts responded to by a user (75 FR 2046).

In 2012, largely based on recommendations made by ONC's Health Information Technology Policy Committee (HITPC),[65] ONC established a new set of functionalities for Health IT Modules supporting CDS, including: (1) Display source or citation of CDS; (2) be configurable based on patient context (e.g., inpatient, outpatient, problems, meds, allergies, lab results); (3) be presented at a relevant point in clinical workflow; (4) include alerts presented to users who can act on alerts (e.g., licensed professionals); (5) be integrated with the EHR (i.e., not standalone). ONC finalized the current instantiation of the Program's CDS criterion in § 170.315(a)(9) and required Health IT Modules certified to that criterion to provide users with four source attributes related to each CDS intervention (80 FR 62622).

Since the adoption of the CDS criterion in § 170.315(a)(9), health IT implementation and technology resources used to support clinical decision-making have continued to evolve. Within healthcare today, predictive models are increasingly being used and relied upon to inform an array of decision-makers, including clinicians, payers, researchers, and individuals, and to aid decision-making through CDS.[66] In many cases, certified health IT is a key component and data

---

[65] Health Informational Technology Policy Committee (HITPC) Transmittal Letter to the National Coordinator. June 2011. https://www.healthit.gov/sites/default/files/facas/hitpc-stage-2-mu-recommendations.pdf#page=4.

[66] See e.g., American Hospital Association. "Surveying the AI Health Care Landscape" 2019. https://www.aha.org/system/files/media/file/2019/10/Market_Insights_AI-Landscape.pdf; Darshali A Vyas, et al., Hidden in plain sight—reconsidering the use of race correction in clinical algorithms § 383 (Mass Medical Soc

source of these predictive models, often providing the data used to build and train algorithms and serving as the vehicle to influence day-to-day decision-making.[67] Both structured and unstructured data generated by, and subsequently made available through certified Health IT Modules, power the training and real-world use of predictive models. Either as part of testing data or as real-time inputs into deployed predictive models, certified Health IT Modules provide data these predictive models need to work. Developers of certified health IT also create and deploy predictive algorithms or models for use in production environments through their Health IT Modules and, increasingly, such developers also enable other parties, including third-party developers and customers of the developer of certified health IT, to create and deploy predictive models through the developer's Health IT Modules. In turn, certified Health IT Modules are often the vehicle or delivery mechanism for predictive model outputs to reach users, such as clinicians, through decision support.

The National Academy of Medicine (NAM) described in a 2019 report how predictive models and other forms of artificial intelligence (AI) have the potential to represent the "payback" of using health IT "by facilitating tasks that every clinician, patient, and family would want, but are impossible without electronic assistance."[68] The NAM report also identified a crucial "need to present each healthcare AI tool along with the spectrum of transparency related to the potential harms and context of its use. Evaluating and addressing appropriate transparency, in each sub-domain of data, algorithms, and performance, and systematically reporting it, must be a priority."[69]

2020); Fact Versus Fiction: Clinical Decision Support Tools and the (Mis)use of Race. (2021); Goldhill, Olivia. Artificial intelligence can now predict suicide with remarkable accuracy, Quartz, (July 2022), https://qz.com/1001968/artificial-intelligence-can-now-predict-suicide-with-remarkable-accuracy/ (discussing the use of ML algorithms to predict and prevent suicide).

[67] See, e.g., Burdick, Hoyt, et al. "Effect of a sepsis prediction algorithm on patient mortality, length of stay and readmission: a prospective multicentre clinical outcomes evaluation of real-world patient data from US hospitals." *BMJ health & care informatics* 27.1 (2020).

[68] Michael Matheny, et al., Artificial intelligence in health care: the hope, the hype, the promise, the peril, WASHINGTON, DC: NATIONAL ACADEMY OF MEDICINE (2019).

[69] *Id.*

As the evolution of technology has continued, there has been a bi-partisan effort to ensure the Department and the Federal Government optimize the use of AI while working to address potential risks in the development and use of predictive models and AI, including efforts to promote transparency and notice, ensure fairness and non-discriminatory practices, and protect the privacy and security of health information.

In November of 2020, the Office of the Management and Budget released a Memorandum for the Heads of Executive Departments and Agencies on *Guidance for Regulation of Artificial Intelligence Applications*, which directed that "[w]hen considering regulations or policies related to AI applications, agencies should continue to promote advancements in technology and innovation, while protecting American technology, economic and national security, privacy, civil liberties, and other American values, including the principles of freedom, human rights, the rule of law, and respect for intellectual property."[70] This was followed by an executive order in December of 2020: E.O. 13960 *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*.[71] The executive order stated: "The ongoing adoption and acceptance of AI will depend significantly on public trust. Agencies must therefore design, develop, acquire, and use AI in a manner that fosters public trust and confidence while protecting privacy, civil rights, [and] civil liberties[.]" (85 FR 78939).

In June of 2021, the Government Accountability Office (GAO) published *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*, which specifically outlined key principles and actions "[t]o help entities promote accountability and responsible use of AI systems." This included outlining four principles for the framework, including governance, data, performance, and monitoring.[72]

---

[70] OMB – EOP - *Memorandum for the Heads of Executive Departments and Agencies on Guidance for Regulation of Artificial Intelligence* M-21-06, p. 6 (Nov. 17, 2020).
[71] E.O. No. 13960, 85 FR 78939: https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.
[72] GAO, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*: (June 2021), https://www.gao.gov/assets/gao-21-519sp.pdf. See generally *Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care*, (Nov. 2020), https://www.gao.gov/products/gao-21-7sp.

In September of 2022, the Biden-Harris Administration published *Principles for Enhancing Competition and Tech Platform Accountability*, which included a principle related to stopping discriminatory algorithmic decision-making.[73] In October of 2022, the Biden-Harris Administration published a *Blueprint for an AI Bill of Rights*, which outlines five principles, informed by public input, that should guide the design, use, and deployment of automated systems to protect the American public in the age of artificial intelligence. These principles are safe and effective systems; algorithmic discrimination protections; data privacy; notice and explanation; and human alternatives, consideration, and fallback.[74]

Finally, in February of 2023, E. O. 14901: *Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government* was issued *(*88 FR 10825-10833).[75] E.O. 14091 of Feb. 16, 2023, builds upon previous equity-related E.O.s, including E.O. 13985.[76] Section 1 of E.O. 14091 requires the Federal Government to "promote equity in science and root out bias in the design and use of new technologies, such as artificial intelligence." Section 8, subsection (f) of E.O. 14091 requires agencies to consider opportunities to "prevent and remedy discrimination, including by protecting the public from algorithmic discrimination."

A growing body of peer-reviewed evidence, technical and socio-technical expert analyses, and government activities and reports[77] focus on ensuring that the promise of AI and machine learning (ML) can equitably accelerate advancements in healthcare to improve the health and well-being of the American public. We are therefore proposing to incorporate new requirements into the ONC Health IT Certification Program for Health IT Modules that support

---

[73] See White House, *Principles for Enhancing Competition and Tech Platform Accountability*, Sept. 8, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/08/readout-of-white-house-listening-session-on-tech-platform-accountability/.

[74] The White House*, Blueprint for an AI Bill of Rights* (October 4, 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[75] E.O. 14091, 88 FR 10825-10833: https://www.federalregister.gov/documents/2023/02/22/2023-03779/further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal.

[76] E.O. 13985, 88 FR 7009: https://www.federalregister.gov/documents/2021/01/25/2021-01753/advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government.

[77] We discuss additional federal and HHS activities – including activities resulting from the executive orders – in the sub-section entitled "Relationship to Other Federal Agencies' Relevant Activities, Interests, and Regulatory Authority."

AI and ML technology. These requirements align with the Federal Government's efforts to promote trustworthy AI and the Department's stated policies on advancing equity in the delivery of health and human services.[78]

We believe that the continued evolution of decision support software, especially as it relates to AI- and ML-driven predictive DSIs, necessitates new requirements for the Program's CDS criterion. These include proposed requirements for new sets of information that are necessary to guide decision-making based on recommendations (outputs) from predictive DSIs, such as an expanded set of "source attributes" and information related to how intervention risk is managed by developers of certified health IT with Health IT Modules that enable or interface with predictive DSIs. We believe that these new sets of information would provide appropriate information to help guide decisions at the time and place of care, consistent with 42 U.S.C. § 300jj–11(b)(4).

Artificial Intelligence, Algorithms, and Predictive Models in Healthcare

We consider AI to encompass a broad and varied set of technologies that generally incorporate algorithms or statistical models. Early examples of AI in healthcare, sometimes referred to as "expert systems," were based on codified expert knowledge, logic models, and deterministic rules to recommend treatment for individuals, and systems of this type are widely used today to provide clinical decision support (CDS).[79] More recently, the use of AI based on statistical and related ML approaches to generate predictions (that are used in classifications, recommendations, and related outputs) has grown in healthcare. That growth has been propelled by what is sometimes referred to as the "AI Triad"[80] — improvements in data availability, algorithm effectiveness, and computing power — which allows complex models to be applied to

---

[78] HHS, Statements on New Plan to Advance Equity in the Delivery of Health and Human Services, April 14, 2022, https://www.hhs.gov/about/news/2022/04/14/hhs-statements-on-new-plan-advance-equity-delivery-health-human-services.html.

[79] See Edward H Shortliffe, et al., *An artificial intelligence program to advise physicians regarding antimicrobial therapy*, 6 COMPUTERS AND BIOMEDICAL RESEARCH (1973).

[80] Ben Buchanan, *The AI triad and what it means for national security strategy*, CENTER FOR SECURITY AND EMERGING TECHNOLOGY (2020). https://cset.georgetown.edu/research/the-aitriad-and-what-it-means-for-national-security-strategy.

large data sets. To date, the most successful application of these models in the domain of healthcare has focused on the processing of images to inform diagnosis.[81] However, they have already been applied to a wide range of healthcare use cases leveraging certified health IT, many times to aid decision-making.[82] The current and potential applications of AI to healthcare are vast ranging from interpretation of medical imaging; efficient allocation of scarce healthcare resources; improved diagnostic and prognostic accuracy; and reduced clinician burden and subsequent burnout.[83]

Within healthcare today, predictive models are increasingly being used to inform an array of key decision-makers, including clinicians, payers, researchers, and individuals, and to aid decision-making through CDS.[84] We describe the implementation of models to support or inform decision-making across the health industry as 'predictive' decision support interventions (DSI), though others have used the terms 'augmented intelligence,' 'automated decision-making,' or 'augmented decision-making,' to describe such tools and technologies.[85] Often, these predictive DSIs include a "human in the loop" or are otherwise used in conjunction with an expert's judgment, though in some cases, these tools could initiate clinical management that requires a clinician to contest.[86]

---

[81] Aggarwal, Ravi, et al. "Diagnostic accuracy of deep learning in medical imaging: A systematic review and meta-analysis." NPJ digital medicine 4.1 (2021): 1-23.

[82] See Romero-Brufau, Santiago, et al. "Implementation of artificial intelligence-based clinical decision support to reduce hospital readmissions at a regional hospital." Applied clinical informatics 11.04 (2020): 570-577; Sendak, Mark P., et al. "Real-world integration of a sepsis deep learning technology into routine clinical care: implementation study." *JMIR medical informatics* 8.7 (2020): e15182; Andrew L Beam & Isaac S Kohane, *Big data and machine learning in health care*, 319 JAMA (2018).

[83] See Michael Matheny, et al., Artificial intelligence in health care: the hope, the hype, the promise, the peril, WASHINGTON, DC: NATIONAL ACADEMY OF MEDICINE (2019); Davenport, Thomas, and Ravi Kalakota. "The potential for artificial intelligence in healthcare." *Future healthcare journal* 6.2 (2019): 94.

[84] See e.g., American Hospital Association. "Surveying the AI Health Care Landscape" 2019. https://www.aha.org/system/files/media/file/2019/10/Market_Insights_AI-Landscape.pdf; Darshali A Vyas, et al., Hidden in plain sight—reconsidering the use of race correction in clinical algorithms § 383 (Mass Medical Soc 2020); Fact Versus Fiction: Clinical Decision Support Tools and the (Mis)use of Race. (2021); Goldhill, Olivia. Artificial intelligence can now predict suicide with remarkable accuracy, Quartz, (July 2022), https://qz.com/1001968/artificial-intelligence-can-now-predict-suicide-with-remarkable-accuracy/ (discussing the use of ML algorithms to predict and prevent suicide).

[85] Elliott Crigger, et al., *Trustworthy Augmented Intelligence in Health Care*, 46 JOURNAL OF MEDICAL SYSTEMS (2022).

[86] This latter case is referred to as Level 2 Autonomous AI in CPT® Appendix S: Artificial Intelligence Taxonomy for Medical Services and Procedures (ama-assn.org), doi: 10.1164/rccm.202109-2092OC.

Increasingly, predictive DSIs are embedded into health IT systems including certified health IT, within a medical device, or as a standalone medical device.[87] In addition to informing treatment at the point-of-care (e.g., clinical guidelines, pathways, and CDS), predictive models can also form the basis for the 'back end' of DSIs used by integrated delivery systems, payers, and consumers including for administrative, payment, or operations workflows. These models thereby influence decisions beyond the point of care such as by prompting use of default order sets, prior authorization workflows, or recommending double-booking certain patients.[88]

The expanding use of and reliance on predictive models in healthcare are demonstrating value in many circumstances.[89] However, growing evidence indicates that predictive models introduce or increase the potential for a variety of risk types. The use of some predictive models can have unintended, adverse or negative impacts on patients, patient populations, or communities due to a range of factors related to model risk.[90]

In this proposed rule, model risk refers to the potential that an entity is negatively influenced by a potential circumstance or event based on incorrect, misused, or otherwise harmful model outputs and reports, the likelihood of those adverse consequences, and their magnitude.[91] Risks related to predictive models can impact healthcare decisions in a myriad ways, including models that: exhibit harmful bias; are broadly inaccurate; have degraded due to

---

[87] A device, as defined in section 201(h) of the FD&C Act, can include an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is, among other criteria, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease in man. The term "device" does not include software functions excluded pursuant to section 520(o) of the FD&C Act.

[88] See e.g., Michele Samorani, Shannon L. Harris, Linda Goler Blount, Haibing Lu, Michael A. Santoro (2021) Overbooked and Overlooked: Machine Learning and Racial Bias in Medical Appointment Scheduling. Manufacturing & Service Operations Management 0(0), https://pubsonline.informs.org/doi/10.1287/msom.2021.0999.

[89] Dean NC, Vines CG, Carr JR, et al. A Pragmatic Stepped-wedge, Cluster-controlled Trial of Real-time Pneumonia Clinical Decision Support. Am J Respir Crit Care Med. 2022 Mar 8.

[90] See e.g., Cutillo, C.M., Sharma, K.R., Foschini, L. *et al.* Machine intelligence in healthcare—perspectives on trustworthiness, explainability, usability, and transparency. *npj Digit. Med.* 3, 47 (2020), https://doi.org/10.1038/s41746-020-0254-2https://www.nature.com/articles/s41746-020-0254-2.

[91] See Bd. Governors Fed. Rsrv. Sys., Off. of Comptroller of the Currency, Supervisory Guidance on Model Risk Management, SR Letter 11-7, (April 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm and NIST, AI Risk Management Framework (AI RMF), January 2023, https://www.nist.gov/itl/ai-risk-management-framework.

model or data drift;[92] misuse of the model (incorrect or inappropriate use); or result in widening health disparities.[93] Several of these risks can be heightened by inattention to human factors, which can heighten the risk that models are not designed to effectively support their real-world use, that models are misinterpreted or misapplied by users, and that users do not have the necessary means to identify or alter models that are not effective or exhibit harmful bias.[94] The extent to which predictive models can be misused and provide low validity or biased predictions (outputs) has only recently come into sharper focus.[95]

One of the most consequential adverse events resulting from the use of predictive models relates to bias in the predictions of such models. While the use of AI has the potential to reduce unlawful discrimination caused by systemic biases,[96] it can also reinforce or introduce bias. When AI introduces or exacerbates bias, it can lead to discriminatory outcomes or decisions, violate anti-discrimination laws, and undermine public trust and confidence in AI.[97] Bias in predictive models and other forms of AI is defined as unequal performance among individuals across groups or unequal predictions for similar individuals belonging to specific groups and comparator groups.[98] The use of biased models has the potential to worsen disparities in health, access to healthcare, and the quality of healthcare for individuals or groups.

---

[92] Model drift has been defined as "the degradation of model performance due to changes in data and relationships between input and output variables." See https://www.ibm.com/cloud/watson-studio/drift. See e.g., Davis SE, Lasko TA, Chen G, Siew ED, Matheny ME. Calibration drift in regression and machine learning models for acute kidney injury. J Am Med Inform Assoc. 2017 Nov 1;24(6):1052, https://pubmed.ncbi.nlm.nih.gov/28379439/.

[93] See, e.g., *Bias at warp speed: how AI may contribute to the disparities gap in the time of COVID-19*: https://academic.oup.com/jamia/article/28/1/190/5893483.

[94] See Section 3.3 of NIST Special Publication 1270, "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence."

[95] Darshali A Vyas, et al., Hidden in plain sight—reconsidering the use of race correction in clinical algorithms § 383 (Mass Medical Soc 2020); Fact Versus Fiction: Clinical Decision Support Tools and the (Mis)use of Race. (2021).

[96] See Adnan Asar, *AI Could Reduce Racial Disparities in Healthcare*, Forbes (Oct. 1, 2021) (discussing algorithms that read knee x-rays and evaluate patient pain did a better job than doctors), https://www.forbes.com/sites/forbestechcouncil/2021/10/01/ai-could-reduce-racial-disparities-in-healthcare/?sh=3deb4cf75a4a.

[97] See Off. of Mgmt. & Budget, Exec. Off. of the President, Memorandum for the Heads of Executive Departments and Agencies on Guidance for Regulation of Artificial Intelligence Applications, M-21-06, p. 6 (Nov. 17, 2020).

[98] See Ninareh Mehrabi, et al., *A survey on bias and fairness in machine learning*, 54 ACM COMPUTING SURVEYS (CSUR) (2021); Jenna Wiens, et al., *Do no harm: a roadmap for responsible machine learning for health care*, 25 NATURE MEDICINE (2019); Ziad Obermeyer, et al., *Dissecting racial bias in an algorithm used to manage the health of populations*, 366 SCIENCE (2019);Michael Feldman, et al., Certifying and removing disparate impact

For example, a widely used algorithm designed to identify patients with high needs for healthcare systematically assigned lower scores to Black patients than to White patients, even when those individuals had similar numbers of chronic conditions and other markers of health.[99] In this instance, the model was designed to predict healthcare costs rather than individual's health, and bias emerged because healthcare costs are systematically lower for Black than White patients due to structural biases and differences in access to care. The application of this model to determine enrollment into preventive services may have led users to select far more White patients than Black patients of similar health, exacerbating health disparities. There are numerous other instances in which the deployment of AI technologies has been accompanied by concerns about whether and how societal biases are being perpetuated or amplified.[100] While an essential issue, concerns related to model fairness and bias are only one of several potential sources of potential risks related to predictive models.[101] The use of predictive models, including those that are part of DSIs, invariably present model risk (the potential that use of a model negatively influences an entity). This includes models performing differently among certain patients, populations, and communities without the user's knowledge or due to inappropriate use. Model

---

(2015);CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (Broadway Books. 2016).

[99] Ziad Obermeyer, et al., Dissecting racial bias in an algorithm used to manage the health of populations, 366 SCIENCE (2019).

[100] See, e.g., M. Evans and A. W. Mathews, "New York Regulator Probes UnitedHealth Algorithm for Racial Bias," Wall Street Journal, Oct. 2019, https://www.wsj.com/articles/new-york-regulator-probes-unitedhealth-algorithmfor-racial-bias-11572087601; M. A. Gianfrancesco, S. Tamang, J. Yazdany, and G. Schmajuk, "Potential Biases in Machine Learning Algorithms Using Electronic Health Record Data," JAMA Intern Med, vol. 178, no. 11, p. 1544, Nov. 2018, http://archinte.jamanetwork.com/article.aspx?doi=10.1001/jamainternmed.2018.3763; H. Ledford, "Millions of black people affected by racial bias in healthcare algorithms," Nature, vol. 574, no. 7780, pp. 608–609, Oct. 2019, 55/77 number: 7780 Publisher: Nature Publishing Group. [Online]. https://www.nature.com/articles/d41586-019-03228-6; T. Simonite, "How an Algorithm Blocked Kidney Transplants to Black Patients | WIRED," Wired, 2020, https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/.

[101] See NIST, AI RMF 1.0, https://www.nist.gov/itl/ai-risk-management-framework.

risk can lead to patient harm, bias, widening health disparities, discrimination,[102] inefficient resource allocation decisions, or ill-informed clinical decision-making.[103]

Model risk – and resulting harmful bias – may be driven by a number of potential factors, which we seek to address in this proposed rule. For instance, there may be additional bias introduced, either unintentionally or deliberately, by the developer of a DSI based on their vested interest in the outcome, clinical intervention, or recommendation. Developers of predictive models and decision support modules sometimes include pharmaceutical manufacturers, pharmacies, clinical laboratories, and other entities that have a financial interest in the treatment selected by health care providers. We note the Federal anti-kickback statute makes it a criminal offense to knowingly and willfully offer, pay, solicit, or receive any remuneration to induce, or in return for, the referral of an individual to a person for the furnishing of, or arranging for the furnishing of, any item or service reimbursable under a Federal health care program. The statute's prohibition also extends to remuneration to induce, or in return for, the purchasing, leasing, or ordering of, or arranging for or recommending the purchasing, leasing, or ordering of, any good, facility, service, or item reimbursable by a Federal health care program. Accordingly, if any individual or entity offers or provides remuneration to health IT developers, their

---

[102] See White House, *Principles for Enhancing Competition and Tech Platform Accountability*, Sept. 8, 2022, available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/08/readout-of-white-house-listening-session-on-tech-platform-accountability/ (noting a principle that includes stopping discriminatory algorithmic decision-making). See also U.S. Dept of Health & Human Servs., Office for Civil Rights, Notice of Proposed Rulemaking, Nondiscrimination in Health Programs and Activities, 87 FR 47824, 47880 (Aug. 4, 2022) https://www.federalregister.gov/documents/2022/08/04/2022-16217/nondiscrimination-in-health-programs-and-activities; Section 1557 of the Affordable Care Act, 42 U.S.C. § 18116 (prohibiting discrimination on the basis of race, color, national origin (including limited English proficiency), sex (including sexual orientation and gender identity), age, or disability in certain health programs or activities), Title VI of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000d *et seq*. (prohibiting discrimination on the basis of race, color, or national origin (including limited English proficiency) in federally funded programs or activities), Title IX of the Education Amendments of 1972, 20 U.S.C. §§ 1681 *et seq*. (prohibiting sex discrimination in federally funded education programs or activities), the Age Discrimination Act of 1975, 42 U.S.C. §§ 6101 *et seq*. (prohibiting age discrimination in federally funded programs or activities), Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. § 794 (prohibiting disability discrimination in federally funded programs or activities), and the Americans with Disabilities Act, 42 U.S.C. §§ 12101 *et seq*. (prohibiting disability discrimination by state and local government entities).

[103] See e.g., NIH, National Center for Advancing Translational Sciences (NCATS), *Bias Detection Tools in Health Care Challenge*, (October 2022), https://www.challenge.gov/?challenge=minimizing-bias-and-maximizing-long-term-accuracy-of-predictive-algorithms-in-healthcare; NIH, National Institute on Minority Health and Health Disparities, *Science Collaborative for Health disparities and Artificial intelligence bias Reduction* (ScHARe), https://www.nimhd.nih.gov/resources/schare/.

customers, or others (including patients) to arrange for the furnishing of any item or service or arrange for or recommend purchasing, leasing, or ordering any good, facility, service, or item payable in whole or in part under a Federal health care program may implicate and potentially violate the Federal Anti-Kickback Statute for both those who offer or pay and those who solicit or receive remuneration. This may include, for example, remuneration by third parties to developers of certified health IT for integrating or enabling DSI where one purpose is to increase sales of the third-party's products or services. Our existing certification criterion for clinical decision support in § 170.315(a)(9) includes a source attribute to describe the funding source of any evidence-based DSIs. In this proposed rule, we include the same transparency on funding source requirements within the proposed source attributes for the new DSI criterion in § 170.315(b)(11) as well as additional requirements described further in the summary of proposals in this section with the intent of support users in fully understanding the model risk in predictive DSI their Health IT Module enables or interfaces with.

Model risk occurs primarily for two reasons. First, the model may have fundamental errors and may produce inaccurate outputs when viewed against the design objective and intended uses. The mathematical calculation and quantification exercise underlying any model generally involves application of theory, choice of sample design and numerical routines, selection of inputs and estimation, and implementation in information systems. Errors can occur at any point in the software life cycle from design through implementation and after deployment. For instance, model developers may omit key data elements that are essential for accurately predicting outcomes in real-world environments. Or model developers may assume that data will be available at the time of model use, when in practice, that data is often not yet available. These oversights can lead to model outputs that may not be fair, appropriate, valid, effective, or safe, if implemented in real-world environments. In addition, shortcuts, simplifications, or approximations used to manage complicated problems could compromise the integrity and reliability of outputs from those calculations. Finally, the quality of model outputs depends on

the quality and representativeness of input data and assumptions, and errors in inputs or incorrect assumptions will lead to inaccurate outputs or outputs that vary in accuracy or effectiveness across different populations.[104]

Second, the model may be used incorrectly or inappropriately. Even a fundamentally sound model producing accurate outputs consistent with the design objective of the model may exhibit high model risk if it is misapplied or misused. Models by their nature are simplifications of reality, and real-world events may prove those simplifications inappropriate. This is even more of a concern if a model is used outside the environment for which it was designed. Decision makers need to understand the limitations of a model to avoid using it in ways that are not consistent with the original intent. Limitations come in part from weaknesses in the model due to its various shortcomings, approximations, and uncertainties. Limitations are also a consequence of assumptions underlying a model that may restrict the scope to a limited set of specific circumstances and situations.[105]

Greater transparency in model theory, assumptions, design, and evaluation could allow users of certified health IT to review model design and evaluation and determine whether a particular model is appropriate for their purposes. Despite the need for information about predictive model development processes, evaluations of performance, and risk management, this information is often unavailable to users and purchasers of certified health IT. This may be because such information does not exist, because it is not made available to those outside the organization that developed the model, or because there is a lack of industry consensus around what information should be available and to whom, among other potential reasons. In turn, complex predictive models are often referred to as 'black boxes' because it can be difficult or

---

[104] See Bd. Governors Fed. Rsrv. Sys., Off. of Comptroller of the Currency, Supervisory Guidance on Model Risk Management, SR Letter 11-7, (April 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm; Off. Comptroller Currency, Comptroller's Handbook: Model Risk Management (Aug. 2021), https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html.

[105] *Id.*

impossible to determine why the model arrives at a specific prediction.[106] Even simpler models, such as the Modification of Diet in Renal Disease (MDRD) Estimate Glomerular Filtration Rate (eGFR), can include difficult-to-observe validity or fairness issues that may lead to harm.[107]

In contrast to the U.S. financial services industry,[108] the U.S. healthcare industry does not have universally applicable, consistently applied framework(s), best practices, or norms for transparency about technical and performance aspects and organizational competencies (e.g., model risk management) in place for DSIs. Research has indicated that while there is a proliferation of industry "reporting guidelines" for various purposes and scopes within healthcare,[109] commonly used ML models developed by health IT developers frequently do not adhere to such guidelines.[110] This lack of adherence to voluntary "reporting guidelines" contributes to the lack of information available about predictive models, which can have negative consequences for users, patients, and the market underlying these models. Model developers are likely to have substantially greater information on the underlying quality of the models, hindering potential users' ability to select the model they would prefer with full information, or

---

[106] Leo Breiman, *Statistical modeling: The two cultures (with comments and a rejoinder by the author)*, 16 STATISTICAL SCIENCE (2001).

[107] Darshali A Vyas, et al., Hidden in plain sight—reconsidering the use of race correction in clinical algorithms § 383 (Mass Medical Soc 2020); Fact Versus Fiction: Clinical Decision Support Tools and the (Mis)use of Race. (2021).

[108] See e.g., Model Risk Management: New Comptroller's Handbook Booklet, https://www.occ.treas.gov/news-issuances/bulletins/2021/bulletin-2021-39.html; Consumer Financial Protection Bureau (CFPB), (February 23, 2022), https://files.consumerfinance.gov/f/documents/cfpb_avm_outline-of-proposals_2022-02.pdf (outlining CFPB's proposals and alternatives to prevent algorithmic bas in home valuations); See also Fed. Trade Comm'n, Using Artificial Intelligence and Algorithms (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.

[109] See for example, Mitchell, et al., Model cards for model reporting and Sendak, et al., Presenting machine learning model information to clinical end users with model facts labels, and Silcox, et al., AI-enabled clinical decision support software: a "Trust and Value Checklist" for clinicians, 1 NEJM CATALYST INNOVATIONS IN CARE DELIVERY (2020); Viknesh, Sounderajah, et al., Developing specific reporting guidelines for diagnostic accuracy studies assessing AI interventions: The STARD-AI Steering Group, 26 NATURE MEDICINE (2020). H Echo Echo Wang, et al., A bias evaluation checklist for predictive models and its pilot application for 30-day hospital readmission models, Journal of the American Medical Informatics Association: JAMIA (2022); Baptiste Vasey, et al., Reporting guideline for the early-stage clinical evaluation of decision support systems driven by artificial intelligence: DECIDE-AI, 377 BMJ (2022); Gary S Collins, et al., Protocol for development of a reporting guideline (TRIPOD-AI) and risk of bias tool (PROBAST-AI) for diagnostic and prognostic prediction model studies based on artificial intelligence, 11 BMJ OPEN (2021).

[110] Fifteen reporting guidelines are employed in Lu, et al., Low adherence to existing model reporting guidelines by commonly used clinical prediction models. medRxiv 2021.07.21.21260282; doi: https://doi.org/10.1101/2021.07.21.21260282.

to choose not to use any model given the limitations of available offerings.[111] In the absence of information about how models were developed and tested or are intended to function, many users will be unable to distinguish between products and may choose technologies that provide inaccurate information or predictions, or are ill-suited for a given task or context. In this context, adverse selection would occur when developers offering higher quality predictive models, or models that provide more balanced performance across a representative sample of input data, are not adequately rewarded in the market because health care providers and other potential users do not fully believe or understand the model developers' quality claims. This ultimately leads to high-quality, high-cost model developers to exit the market.[112] Interested parties within the industry have identified numerous and varied areas of potential concerns between the optimal use of predictive models in healthcare and the real world deployment of such technologies.[113] These concerns stem from a range of issues including incomplete or non-representative training data, inconsistent and absent model performance validation, scarcity of transparency regarding the composition, semantics, provenance, and quality of data used to develop AI tools, and underdeveloped organizational competencies or resources to surface and address ethical and fairness issues that arise from AI tool deployment, among others.[114] We fundamentally agree with these assertions, and as we consider the shared goals expressed by multiple vantage points of this discussion, we believe that significant progress towards optimizing the use of predictive models in healthcare decision-making is attainable.

We are aware of existing and emerging efforts to establish guidelines, frameworks, and principles to encourage optimization of predictive models in healthcare, including recent industry

---

[111] George A Akerlof, *The market for "lemons": Quality uncertainty and the market mechanism*, *in* UNCERTAINTY IN ECONOMICS (1978).
[112] Id. At David Dranove & Ginger Zhe Jin, *Quality disclosure and certification: Theory and practice*, 48 JOURNAL OF ECONOMIC LITERATURE (2010).
[113] See, e.g., Michael Matheny, et al., *Artificial intelligence in health care: the hope, the hype, the promise, the peril*, WASHINGTON, DC: NATIONAL ACADEMY OF MEDICINE (2019).
[114] See also The Council of Europe's Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO), Impact of Artificial Intelligence on the Doctor-Patient Relationship, https://www.coe.int/en/web/bioethics/report-impact-of-ai-on-the-doctor-patient-relationship.

recognition for evaluation, monitoring, and guardrails.[115] In addition, many organizations have adopted a set of high-level principles for their AI-driven technology to inform decisions in an ethical fashion and cause no harm. States are also concerned about AI, algorithms, and predictive models and have taken action,[116] including proposing state legislation.[117] Further, many State Attorneys General also provided extensive comments on the *Nondiscrimination in Health Programs and Activities* proposed rule to recommend more stringent oversight of algorithm-based discrimination.[118] Similarly, national and international governing bodies have identified a need for enhanced oversight and advanced tools and metrics to aid in adherence to best-practice guidelines.[119]

---

[115] See, e.g., John Halamka, Suchi Saria, Nigam Shah. STAT. Health-related artificial intelligence needs rigorous evaluation and guardrails, https://www.statnews.com/2022/03/17/health-related-ai-needs-rigorous-evaluation-and-guardrails/; Price II, William Nicholson and Sachs, Rachel and Eisenberg, Rebecca S., New Innovation Models in Medical AI (February 11, 2021). 99 Wash. U. L. Rev. 1121 (2022), U of Michigan Public Law Research Paper No. 21-009, https://ssrn.com/abstract=3783879 or http://dx.doi.org/10.2139/ssrn.3783879; Cardiovascular Quality and Outcomes: 2022; Health AI Partnership (HAIP), https://dihi.org/health-ai-partnership-an-innovation-and-learning-network-to-facilitate-the-safe-effective-and-responsible-diffusion-of-health-ai-software-applied-to-health-care-delivery-settings/. See generally Petersen C, Smith J, Freimuth RR, Goodman KW, Jackson GP, Kannry J, Liu H, Madhavan S, Sittig DF, Wright A. Recommendations for the safe, effective use of adaptive CDS in the US healthcare system: an AMIA position paper. J Am Med Inform Assoc. 2021 Mar 18;28(4):677-684, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7973467/.

[116] See e.g., State of California Department of Justice, Press Release. Attorney General Bonta Launches Inquiry into Racial and Ethnic Bias in Healthcare Algorithms (Aug. 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-launches-inquiry-racial-and-ethnic-bias-healthcare; California Privacy Protection Agency, *Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking*, (February 2023), https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf.

[117] See e.g., Brookings Institute Commentary. *How California and other states are tackling AI legislation* (March 2023), https://www.brookings.edu/blog/techtank/2023/03/22/how-california-and-other-states-are-tackling-ai-legislation/?utm_campaign=Brookings%20Brief&utm_medium=email&utm_content=251387757&utm_source=hs_email; Office of the Attorney General for District of Columbia, (December 2021), *Stop Discrimination by Algorithms Act of 2021*, https://oag.dc.gov/sites/default/files/2021-12/DC-Bill-SDAA-FINAL-to-file-.pdf.

[118] Comment from Attorneys General of California, New York, Massachusetts, and nineteen other States, HHS-OS-2022-0012, HHS-OS-2022-0012-0001, 2022-16217: https://www.regulations.gov/comment/HHS-OS-2022-0012-73216.

[119] See, e.g., H.R. 6580 – 117th Congress (2021-2022), Algorithmic Accountability Act of 2022; European Union AI Act, https://artificialintelligenceact.eu/ (proposing European law on AI); Organisation for Economic Cooperation and Development (OECD), OECD AI Principles, https://oecd.ai/en/ai-principles; OECD, Recommendation of the Council on Artificial Intelligence, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449; Word Health Organization (WHO), Ethics and governance of artificial intelligence for health, (June 2021), Pan American Health Organization (PAHO), CE168/11 – Policy on the Application of Data Science in Public Health Using Artificial Intelligence and Other Emerging Technologies, (May 2021), https://www.who.int/publications/i/item/9789240029200; https://www.paho.org/en/documents/ce16811-policy-application-data-science-public-health-using-artificial-intelligence-and; NIH NCATS, Bias Detection Tools in Health Care Challenge, (October 2022), https://www.challenge.gov/?challenge=minimizing-bias-and-maximizing-long-term-accuracy-of-predictive-algorithms-in-healthcare.

We believe predictive DSIs can promote positive outcomes and avoid harm when those DSIs are FAVES. We refer to DSIs that are fair, appropriate, valid, effective, and safe as FAVES. Fair DSIs do not exhibit biased performance, prejudice, or favoritism toward an individual or group based on their inherent or acquired characteristics.[120] Appropriate DSIs are well matched to the specific contexts and populations to which they are applied.[121] Valid DSIs have been demonstrated to estimate targeted values accurately and as expected in both internal and external data.[122] Effective DSIs have demonstrated meaningful benefit in real-world conditions.[123] And safe DSIs are free from any unacceptable risks, including risks to privacy and security, and are DSIs for which the probable benefits outweigh any probable risks.[124] Together, we refer to predictive DSIs and models that are FAVES as high-quality. We believe that the rigorous evaluation of predictive DSIs and models, and the subsequent transparent reporting of those evaluations, can support potential implementers and users to more easily determine FAVES models,[125] leading to greater use of FAVES models and consequently, benefit more patients. In contrast, a failure to undertake such evaluation can lead to harmful or, at best, unhelpful models. One important example comes from recent evidence that has documented widespread use of predictive models that likely provide low validity predictions—that is, predictions that are often incorrect and so may not meaningfully inform decisions, may raise

---

[120] Alvin Rajkomar, et al., Ensuring fairness in machine learning to advance health equity, 169 ANNALS OF INTERNAL MEDICINE (2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6594166/.
[121] Richard Ribón Fletcher, et al., Addressing fairness, bias, and appropriate use of artificial intelligence and machine learning in global health, 3 FRONTIERS IN ARTIFICIAL INTELLIGENCE (2021), https://www.frontiersin.org/articles/10.3389/frai.2020.561802/full.
[122] Collins, Gary S., et al. "Transparent reporting of a multivariable prediction model for individual prognosis or diagnosis (TRIPOD): the TRIPOD statement." *Journal of British Surgery* 102.3 (2015): 148-158.
[123] Amit G Singal, et al., A primer on effectiveness and efficacy trials, 5 CLINICAL AND TRANSLATIONAL GASTROENTEROLOGY (2014).
[124] Cf. ISO 14971, which considers safety to be "free from unacceptable risks." If the product is a device as defined in section 201(h) of the FD&C Act, there may be different or additional requirements that apply.
[125] FAVES aligns with the five principles of the *Blueprint for an AI Bill of Rights.* The Blueprint includes two additional principles of "Notice and Explanation" and "Human Alternatives, Consideration, and Fallback", pertaining to implementation by users of health IT, which, while important are outside the scope of the certification criterion functionality. See The White House, *Blueprint for an AI Bill of Rights*, (October 2022) https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

safety issues, or potentially cause harm.[126] For instance, one study highlighted the relatively poor performance of a predictive model widely used to detect sepsis onset in "external validation," that is, when it was evaluated on data generated from a health system that was not the initial source for training and test data used to develop and internally validate the model.[127] The goal of our proposals, described herein, and as aligned with our authority, is to assist in addressing the gaps between the promise and peril of AI in health articulated in the aforementioned NAM report.

Objectives of the Proposals to Address Predictive Modeling in DSI

Our proposals in § 170.315(b)(11) are intended to introduce much-needed information transparency to address uncertainty regarding the quality of predictive DSIs that certified Health IT Modules enable or interface with, so that potential users have sufficient information about how a predictive DSI was designed, developed, trained, and evaluated to determine whether it is trustworthy. We propose a dual emphasis for transparency on (1) the technical and performance aspects of predictive DSIs and (2) the organizational competencies employed to manage risks for predictive DSIs. Together, this information would support potential users to make more informed decisions about whether and how to use predictive DSIs in their decision-making given the specifics of their context, patients and needs. We consider the information included in these proposed transparency requirements as a prerequisite to determine the quality of predictive models. In addition, such transparency would provide essential information needed to determine whether and how to use the predictive model's outputs. Our proposals are not aimed at approving or guaranteeing the quality of predictive DSIs or the models they are based on. Instead, our proposals are intended to provide users and the public greater information, available in a consistent manner, on whether predictive DSIs are fair, appropriate, valid, effective, and

---

[126] Casey Ross, STAT. AI gone astray: How subtle shifts in patient data send popular algorithms reeling, undermining patient safety, 2022, available at: https://www.statnews.com/2022/02/28/sepsis-hospital-algorithms-data-shift; Generalizability of Cardiovascular Disease Clinical Prediction Models: 158 Independent External Validations of 104 Unique Models, https://www.ahajournals.org/doi/10.1161/CIRCOUTCOMES.121.008487.
[127] Andrew Wong, et al., *External validation of a widely implemented proprietary sepsis prediction model in hospitalized patients*, 181 JAMA INTERNAL MEDICINE (2021).

safe. We believe that the resulting transparency from the proposed requirements for the certification criterion in § 170.315(b)(11) described in this section would promote the design, development, and deployment of high-quality predictive models in that they adhere to FAVES principles.[128] We further anticipate that a long-term outcome of such transparency would be increased public trust and confidence in predictive DSIs, so that users, including healthcare systems, clinicians, and patients, can expand the use of these technologies in safer, more appropriate, and more equitable ways. We refer readers to "Decision Support Interventions and Predictive Models" in section VIII.C.1.a of this proposed rule for a discussion about the estimated value associated the impacts of the decision support proposals and efforts to promote high-quality predictive DSIs.

We do not propose to establish or define regulatory baselines, measures, or thresholds of FAVES for predictive DSIs. Instead, we propose, as part of the proposed certification criterion in § 170.315(b)(11), to establish requirements for information that would enable users, based on their own judgment, to determine if a predictive DSI that is enabled by or interfaced with a Health IT Module is acceptably fair, appropriate, valid, effective, and safe. We understand that numerous and parallel efforts led by industry groups are developing methods to evaluate predictive DSIs for fairness, appropriateness, validity, effectiveness, and safety, among other kinds of evaluations. These efforts are also devising means to communicate measures of FAVES through model cards,[129] model nutrition labels,[130] datasheets,[131] data cards,[132] or algorithmic audits.[133] However, these efforts lack consensus and have not been widely or consistently

---

[128] See Rogers, Parker, et al. "Optimizing the Implementation of Clinical Predictive Models to Minimize National Costs: Sepsis Case Study." *Journal of Medical Internet Research* 25 (2023): e43486.
[129] Mitchell, Margaret, et al. "Model cards for model reporting." Proceedings of the conference on fairness, accountability, and transparency. 2019.
[130] Sendak MP, Gao M, Brajer N, Balu S. Presenting machine learning model information to clinical end users with model facts labels. NPJ Digit Med. 2020 Mar 23;3:41. Doi: 10.1038/s41746-020-0253-3.
[131] Gebru, Morgenstern, Vecchione, et al, Datasheets for Datasets, https://arxiv.org/abs/1803.09010.
[132] FaccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency (June 2022) Pages 1776–1826, https://dl.acm.org/doi/proceedings/10.1145/3531146.
[133] See James Guszcza, et al., Why We Need to Audit Algorithms. Harvard Business Review. Nov. 28, 2018. https://hbr.org/2018/11/why-we-need-to-audit-algorithms; Xiaoxuan Liu, et al., *The medical algorithmic audit*, THE LANCET DIGITAL HEALTH (2022). See generally Outsider Oversight: Designing a Third-Party Audit Ecosystem for

implemented to date. Thus, while we believe it is premature to propose requirements for specific measures or thresholds for FAVES, our proposed requirements would enable consistent and routine access to source attribute information about technical and performance dimensions specifically relevant to FAVES, which would support users to make informed decisions about whether and how to use predictive DSIs.

While we believe that transparency regarding the technical and performance dimensions of the predictive DSI is needed, we also believe that transparency regarding the organizational and socio-technical competencies employed by those who develop predictive DSIs is foundational for users to determine whether their predictive DSI is FAVES. Therefore, in addition to the proposed requirements for predictive DSI-specific source attributes, we also propose that developers of certified health IT with Health IT Modules that enable or interface with predictive DSIs and that are certified to § 170.315(b)(11), employ or engage in intervention risk management practices, subsequently making summary information about these practices available publicly. We propose three intervention risk management practices: (1) risk analysis, (2) risk mitigation, and (3) governance. Overall, we identify these practices to promote transparency regarding how the developer of certified health IT analyzes and mitigates risks, at the organization level, including proposals that would have such developers establish policies and implement controls for governance, including how data are acquired, managed, and used in predictive DSIs.

Whereas our proposals for source attributes in § 170.315(b)(11)(vi)(C) are intended to bring transparency into the technical and performance dimensions of the predictive DSI, such as underlying details of the predictive model, how the model was trained, and how its outputs were validated, the proposals for intervention risk management in § 170.315(b)(11)(vii) would focus on the developer of certified health IT's organizational competencies employed, and would bring

---

AI Governance, ID Raji, P Xu, C Honigsberg, D Ho – Proceedings of the 2022 AAAI/ACM Conference on AI, 2022, https://dl.acm.org/doi/pdf/10.1145/3514094.3534181.

transparency into the socio-technical dimensions of the predictive DSI. Together, transparency regarding the technical and performance details of a predictive DSI, as well as the organizational competencies of the developer of certified health IT to manage risks for a predictive DSI are intended to contribute to the trustworthiness of these emerging and important technologies.

The proposed requirements for the certification criterion in § 170.315(b)(11) would also support health equity by design[134] by, for example, (1) emphasizing transparency regarding the use of specific data elements relevant to health equity[135] in predictive DSIs; (2) enabling users to review whether and how the predictive DSI was tested for fairness; and (3) enabling transparency about how developers of certified health IT manage risks related to fairness for the predictive DSIs their Health IT Modules enable or interface with. Specifically, we propose that when evidence-based and predictive DSIs include Patient Observations and Demographics data, Social Determinants of Health data, and Health Status Assessments data, the certified Health IT Modules enable a user to review these data as part of the source attribute requirements in § 170.315(b)(11)(vi)(A). We also propose, as part of source attribute requirements for Health IT Modules that enable or interface with one or more predictive decision support interventions, that users have transparency into how and whether a predictive DSI's recommendation or output was measured for fairness in test data, external data (if available), and local data (if available) in § 170.315(b)(11)(vi)(C)(*3*)(*ii*),(*iv*), and (C)(*4*)(*iii*), respectively.

We believe the existing scope and structure of the Program are fit for these purposes because the Program has existing requirements to make transparent information regarding the authorship, bibliography, and other kinds of "source attribute" information for evidence-based decision support and linked referential intervention types. By requiring developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) to display additional source

---

[134] See "Embracing Health Equity by Design" ONC, February 2022: https://www.healthit.gov/buzz-blog/health-it/embracing-health-equity-by-design.

[135] See HHS's Strategic Approach to Addressing Social Determinants of Health to Advance Health Equity – At a Glance (April 2022), https://aspe.hhs.gov/sites/default/files/documents/aabf48cbd391be21e5186eeae728ccd7/SDOH-Action-Plan-At-a-Glance.pdf.

attributes on evidence-based DSIs, to display source attribute information on the predictive DSI(s) within their certified products, and to disclose approach(es) to intervention risk management in a publicly accessible manner, these proposals would have an important impact on the Department's efforts to address disparities and bias that may be propagated through DSIs. Consequently, we hope to enhance market transparency and encourage trust across the software development life cycle (SDLC) of DSIs in healthcare. This transparency would serve as a foundation for establishing consistency in information availability, improving overall data stewardship, and guiding the appropriate use of data derived from health information about individuals.

We are being intentional with the level of prescriptiveness in our proposals because these are nascent technologies with enormous potential benefit. Thus, we seek to establish appropriate guardrails for information transparency about predictive DSIs that do not undercut the value that could be offered to patients and clinicians from such promising technologies.

b. Summary of Proposals

We propose the certification criterion, "decision support interventions (DSI)" in § 170.315(b)(11). The DSI criterion is a revised certification criterion as it serves as both an iterative and replacement criterion for the "clinical decision support (CDS)" criterion in § 170.315(a)(9). We believe that the continued evolution of decision support software, especially as it relates to AI- and ML-driven predictive models, necessitates new requirements and a new name for the Program's CDS criterion. We propose to revise the name of the CDS criterion to "decision support interventions" to reflect the various and expanding forms of decision support that certified Health IT Modules enable or interface with. Increasingly, DSIs include use cases or are intended to support decision-making across all areas of healthcare, including early detection of disease, automating billing procedures, facilitating scheduling, supporting public health disease surveillance, and other uses beyond traditional CDS. We intend for the DSI criterion to

be inclusive of the wide variety of use cases that Health IT Modules may support moving forward.

As part of the DSI criterion, we propose to add in § 170.315(b)(11)(v) "predictive decision support interventions" and propose to add a corresponding definition for that term to § 170.102. In addition to predictive DSIs, we propose to include in § 170.315(b)(11) the list of current intervention types in § 170.315(a)(9), including evidence-based decision support in § 170.315(b)(11)(iii) and linked referential DSI in § 170.315(b)(11)(iv). Together, we believe these intervention types reflect the variety of DSIs increasingly enabled by or interfaced with, certified Health IT Modules.

In addition to proposing to adopt all source attributes listed in § 170.315(a)(9)(v) in § 170.315(b)(11), we also propose in § 170.315(b)(11)(vi)(A)(*5*) through (*7*) to include new source attributes for evidence-based DSIs in § 170.315(b)(11)(iii). In § 170.315(b)(11)(vi)(A)(*5*) through (*7*) we propose that Health IT Modules enable users to review what, if any, of the following data elements were used in the DSI: Patient Demographics and Observations data specified in paragraph § 170.315(a)(5)(i), including data on race, ethnicity, language, sexual orientation, and gender identity; SDOH data elements as expressed in the standards in § 170.213; and the data elements of the Health Status Assessments data class as expressed in the standards in § 170.213. We note that the Health Status Assessments data class includes several data elements, including Health Concerns, Functional Status, Disability Status, Mental or Cognitive Status, Pregnancy Status, and Smoking Status, as part of the USCDI v3 proposed for adoption in § 170.213(b). We also note that SDOH data elements include SDOH Assessment, SDOH Goals, SDOH Problems/Health Concerns, and SDOH Interventions as part of the USCDI v3 in proposed § 170.213(b). We do not propose any changes to the source attributes for linked referential DSIs in § 170.315(b)(11)(vi)(B) from what is currently in § 170.315(a)(9).

We propose that the new evidence-based DSI source attributes in § 170.315(b)(11)(vi)(A)(*5*) through (*7*) would also pertain to predictive DSIs in §

170.315(b)(11)(v) that are enabled by or interface with certified Health IT Modules, by means of a cross-reference in § 170.315(b)(11)(vi)(C). In § 170.315(b)(11)(vi)(C)(*1*) through (*4*), we also propose several additional source attributes for Health IT Modules that enable or interface with predictive DSIs, as described in paragraph § 170.315(b)(11)(v)(A). These additional source attributes that pertain to predictive DSIs, would include (1) intervention details, such as a description of the output and intended use of the intervention; (2) intervention development details, such as input features, training and test data details, and process(es) used to ensure fairness in development of the intervention, as well as external validation process(es), if available; (3) quantitative measures of intervention performance, such as validity and fairness of prediction in test data and references to any evaluations of the intervention on outcomes; and (4) ongoing maintenance of intervention implementation and use, including an update schedule and to the extent practicable, how well the intervention works (i.e., its validity and fairness) in the specific setting for which it is designed or deployed in.

We believe that these additional source attributes would better support the transparency of predictive DSIs and that such information is necessary for users to decide whether and how to use the predictive DSI, including whether to apply the predictive DSI to individual patients.

Given the potential of a growing market of third-party developed predictive DSIs and development of predictive DSI by customers of developers of certified health IT, we expect that Health IT Modules certified to § 170.315(b)(11) would provide users with source attribute information from these other parties. In circumstances where the developer of certified health IT does not receive source attribute information, we propose in § 170.315(b)(11)(vi)(D) that Health IT Modules clearly indicate when source attributes related to DSIs developed by others are not available for the user to review. We believe it is important that users be made aware when source attribute information is missing or unknown. We propose in § 170.315(b)(11)(vi)(E) that Health IT Modules enable users to author attributes and revise attributes beyond what is proposed in § 170.315(b)(11)(vi)(A) and § 170.315(b)(11)(vi)(C) to support the ongoing evolution of what

source attributes are important to users to make informed decisions regarding the DSI's recommendation(s).

We propose in § 170.315(b)(11)(vii) to require developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) that enable or interface with predictive DSIs (i.e., developers that attest "Yes" in § 170.315(b)(11)(v)(A) for one or more modules) to employ or engage in and document information regarding their intervention risk management (IRM) practices. These practices are listed in proposed § 170.315(b)(11)(vii)(A)(*1*) through (*3*). We propose three categories of IRM practices, including "risk analysis," in § 170.315(b)(11)(vii)(A)(*1*), "risk mitigation," in § 170.315(b)(11)(vii)(A)(*2*), and "governance," in § 170.315(b)(11)(vii)(A)(*3*) for each predictive DSI, as defined in § 170.102, they enable or interface with. We propose in § 170.315(b)(11)(vii)(B) that developers of certified health IT compile detailed documentation regarding the results of IRM practices listed in § 170.315(b)(11)(vii)(A). As an additional requirement of that provision, we propose that developers of certified health IT must make detailed documentation available to ONC upon request from ONC for any predictive decision support intervention, as defined in § 170.102, that the Health IT Module enables or interfaces with. In § 170.315(b)(11)(vii)(C), we propose that developers of certified health IT submit summary information related to their IRM practices described in § 170.315(b)(11)(vii)(A) to ONC-ACBs via publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. We propose in § 170.315(b)(11)(vii)(D) that health IT developers subject to these requirements review annually and, as necessary, update their documentation described in § 170.315(b)(11)(vii)(B) and (b)(11)(vii)(C). The proposed requirement to make summary information regarding IRM practices publicly accessible is similar to requirements related to API documentation requirements in § 170.315(g)(9)(ii). We believe disclosure of summary information regarding IRM practices is necessary for users to evaluate the organizational competencies of those parties that develop predictive DSIs, further improving users'

understanding of the steps that have been taken to mitigate negative impacts or prevent future harm and better support the transparency of predictive DSIs.[136] We also propose a new Principle of Proper Conduct for the ONC-ACBs in § 170.523(f)(1)(xxi) to require ONC-ACBs to report the proposed summary information in § 170.315(b)(11)(vii)(C), that they received from health IT developers of certified health IT, on the Certified Health IT Product List (CHPL) for the applicable certified Health IT Modules. We believe this new Principle of Proper Conduct is consistent with existing public disclosure requirements under the Program (e.g., 45 CFR 170.523(f)(1)(xii) and § 170.523(f)(1)(xx)) and will help ensure accountability for the public availability of information in § 170.315(b)(11)(vii)(C).

Additionally, we propose in § 170.315(a)(9)(vi) that the adoption of the CDS criterion, for purposes of the Program, expires on January 1, 2025. This timeline would support our proposal that developers of certified health IT must certify their Health IT Modules to § 170.315(b)(11) by December 31, 2024, if they wish such Health IT Modules to meet the newly proposed Base EHR definition and ensure continuity for customers using Health IT Modules currently certified to § 170.315(a)(9).

Finally, we propose in § 170.405(a) to require health IT developers of certified health IT with a Health IT Module certified to § 170.315(a)(9) to submit real world testing plans and results consistent with § 170.405 for the period until the CDS criterion is no longer part of the Program. We note that developers of certified health IT with a Health IT Module certified to any of the criteria in § 170.315(b) are already subject to requirements in § 170.405, thus Health IT Modules certified to § 170.315(b)(11) would be subject to the requirements in § 170.405.

c. Proposed Requirements for Decision Support Interventions (DSI) Certification Criterion

[136] For example, NIST developed a voluntary AI Risk Management Framework (AI RMF) and Playbook. The AI RMF provides a flexible, structured, and measurable process to address AI risks prospectively and continuously throughout the AI life cycle, offering guidance for the development and use of trustworthy and responsible AI. Activities are organized as govern, map, measure, and manage risks. See https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook.

i. Proposed Structural Revisions and New Criterion Categorization

We propose to adopt the certification criterion "decision support interventions," (DSI) in § 170.315(b)(11) as a "revised certification criterion" according to the proposed definition in § 170.102. The proposed new criterion in 170.315(b)(11) is a revised version of 45 CFR 170.315(a)(9), "clinical decision support (CDS)." We propose to adopt in § 170.315(b)(11) the structural paragraphs currently in § 170.315(a)(9) with modifications that reflect an array of contemporary functionalities, data elements, and software applications that certified Health IT Modules enable or interface with to aid decision-making in healthcare. We propose that the policies established in § 170.315(a)(9)(i) through (iv) will be included as § 170.315(b)(11)(i) through (iv) with modifications described later in this preamble. We propose to introduce a new intervention type in § 170.315(b)(11), predictive decision support interventions, with a corresponding definition in § 170.102 for predictive decision support interventions.

We believe that these modifications to § 170.315(a)(9), proposed in § 170.315(b)(11), reflect a functionality that is better categorized as part of the "care coordination certification criteria," as opposed to the "clinical certification criteria," supported by the Program. Hence, we propose to adopt the decision support intervention certification criterion in the "care coordination criteria" section adopted within § 170.315(b). The capabilities included within the certification criterion in § 170.315(a)(9) are unlike other certification criteria currently adopted in the "clinical" section in that the functionality expressed in the criterion does not result in enabling a user to "record," "change," and "access" specific data types. Rather, the functionality in § 170.315(a)(9) is more complex and multi-faceted. The primary functionality of both § 170.315(a)(9) and the proposed § 170.315(b)(11) is to ensure that multiple decision support intervention types are: (1) supported through interaction with certified health IT, and (2) configurable based on a specified set of data types (including data listed from the § 170.315(a)(5) demographics criterion). Additionally, the existing and proposed criteria specify that Health IT Modules must support the availability of an intervention's source attributes for users to review.

In this regard, ONC's existing CDS criterion and the proposed criterion in § 170.315(b)(11) are more like the care coordination criteria in § 170.315(b)(1) "transitions of care" and § 170.315(b)(2) "clinical information reconciliation and incorporation." Further, to be enabled, interventions in § 170.315(a)(9) must rely on a wide array of problems, medications, demographics, laboratory tests and vital signs – both generated in the source system and received through a transition of care or referral.

We propose modifications to the "Base EHR" definition in § 170.102 to identify the dates when § 170.315(b)(11) replaces § 170.315(a)(9) in the Base EHR definition. In keeping with the proposal to modify the Base EHR definition in § 170.102, we propose that the adoption of § 170.315(a)(9) as part of the Program would expire January 1, 2025. We note that if we finalize these proposals, developers of certified health IT with Health IT Modules certified to § 170.315(a)(9) who wish for those Health IT Modules to continue to meet the Base EHR definition would need to certify those Health IT Modules to § 170.315(b)(11) by December 31, 2024, which is the effective date we propose elsewhere in this preamble to modify the Base EHR definition to include § 170.315(b)(11).

As a consequence of proposing to adopt this criterion in § 170.315(b), we note that developers of certified health IT with Health IT Module(s) certified to § 170.315(b)(11) would be required to submit real world testing plans and corresponding real world testing results, consistent with § 170.405, demonstrating the real world use of each DSI type the developer of certified health IT supports in § 170.315(b)(11), including evidence-based decision support (§ 170.315(b)(11)(iii)), linked referential (§ 170.315(b)(11)(iv)), and predictive DSI (§ 170.315(b)(11)(v)) as applicable. We refer readers to 85 FR 25766 for further explanation and discussion regarding real world testing. We also note that we propose in a separate section to include § 170.315(a)(9) as part of the applicable certification criteria for real world testing in § 170.405(a). We invite comment on these proposals.

ii. Proposed § 170.315(b)(11)(ii) Decision Support Configuration

We propose in § 170.315(b)(11)(ii) to establish "decision support configuration," requirements based on what is currently in § 170.315(a)(9)(ii) with modifications and additional requirements. To reflect ONC's focus on the USCDI and to acknowledge the varied data for which DSIs may be enabled, we propose that data elements listed in § 170.315(b)(11)(ii)(B)(*1*)(*i*) through (*iii*) and (*v*) through (*viii*) be expressed according to the standards expressed in § 170.213, including the proposed USCDI v3, as proposed elsewhere in this rule. We propose to reference the USCDI in § 170.315(b)(11)(ii)(B)(1) to define the scope of the data "at a minimum." We note the intention is to establish baseline expectations that Health IT Modules certified to § 170.315(b)(11) must support DSIs that use those data elements listed in § 170.315(b)(11)(ii)(B)(*1*). We are not establishing requirements for specific interventions to be supported, only that Health IT Modules certified to § 170.315(b)(11) be capable of supporting interventions that use those listed data elements. This proposed requirement would pertain to both evidence-based DSIs and predictive DSIs that are enabled by or interfaced with a certified Health IT Module, including any predictive DSIs that are developed by users of the certified Health IT Module. We propose to adopt in § 170.315(b)(11) the existing reference in § 170.315(a)(9)(ii)(B)(*1*)(*iv*) to demographic data in § 170.315(a)(5)(i). These proposals are intended to support scenarios where, for example, a clinician may want to leverage their collection of "SDOH problems," which are data elements included as part of the Problems data class in USCDI v3 in § 170.213(b), for decision support. In such a scenario, we would expect the Health IT Module certified to § 170.315(b)(11) to support such DSIs based on their conformance to § 170.315(b)(11)(ii)(B) and report SDOH Problem data element(s) as source attribute information, discussed further in this section.

Additionally, we propose to include two USCDI data classes not currently found in § 170.315(a)(9)(ii)(B)(*1*). In § 170.315(b)(11)(ii)(B)(*1*)(*vii*) - (*viii*), we propose to include the Procedures and Unique Device Identifier(s) for a Patient's Implantable Device(s) data classes, respectively, as expressed in the standards in § 170.213, including the proposed USCDI v3. We

believe that data regarding a patient's procedures and whether a patient has an implantable medical device, as indicated by a unique device identifier (UDI) can play a significant role in contemporary DSIs; hence, we propose to require that Health IT Modules would support data from the Procedures data class and the Unique Device Identifier(s) for a Patient's Implantable Device(s) data class as an input to DSIs. The addition of UDI complements medications and proposed procedures as an important focal point for various decision support including those related to MRIs, post-implant clinical care, among other care scenarios. Making these changes would ensure that DSIs leverage USCDI data elements, and these changes include a reasonable scope of USCDI data elements used in contemporary DSIs, such as SDOH Problems/Health Concerns. We invite comment on the additional data classes described in § 170.315(b)(11)(ii)(B)(*1*)(*vii*).

We note that in our 2015 Edition Proposed Rule, we proposed to adopt new functionality that would require a Health IT Module certified to § 170.315(a)(9) to be able to record at least one action taken, and by whom it was taken, when a CDS intervention is provided to a user (e.g., whether the user viewed, accepted, declined, ignored, overrode, provided a rationale or explanation for the action taken, took some other type of action not listed here, or otherwise commented on the CDS intervention) (80 FR 16821). We also proposed that a Health IT Module certified to § 170.315(a)(9) be able to generate either a human readable display or human readable report of the responses and actions taken and by whom when a CDS intervention is provided (80 FR 16821). We received mixed comments in response to our proposal for this functionality, and commenters stated that current systems already provide a wide range of functionally to document decisions concerning CDS interventions (80 FR 62622). We did not finalize these proposed functionalities (for a "feedback loop") in the 2015 Edition Final Rule, but believe it is important to do so now.

Research indicates that simple "feedback loops" on the performance of DSIs implemented at the point of care can have important impacts on the safety, appropriateness, and

effectiveness of those interventions.[137, 138] For example, this functionality is important for users' ability to monitor the outcomes of the technology's use—e.g., to understand how often and under what circumstances users override the DSI's outputs or recommendations and to include the outcome of an action in response to a DSI as a component of quality measurement. During the 2015 Edition rulemaking process, ONC proposed a functionality that would require a Health IT Module to be able to record at least one action taken and by whom when a CDS intervention is provided to a user (*e.g.,* whether the user viewed, accepted, declined, ignored, overrode, provided a rationale or explanation for the action taken, took some other type of action not listed here, or otherwise commented on the CDS intervention) (80 FR 16821). In the 2015 Edition Final Rule, we noted that many commenters stated that current systems already provide a wide range of functionality to enable providers to document decisions concerning CDS interventions and that such functionality is unnecessary to support providers participating in the EHR Incentive Programs (80 FR 62622).

While we are aware that some health care providers have implemented functionalities to enable "feedback loops," we understand through conversations with interested parties that such functionality is far from commonplace or that information regarding the use of CDS interventions is standard across industry. Subsequent to the 2015 Edition Final Rule, additional evidence has confirmed the effectiveness of this functionality. Consequently, we propose to adopt in § 170.315(b)(11)(ii)(C) a new functionality to enable users to provide electronic feedback data based on the information displayed through the DSI. We propose that a Health IT Module certified to § 170.315(b)(11) must be able to export such feedback data, including but not limited to the intervention, action taken, user feedback provided (if applicable), user, date, and location, so that the exported data can be associated with other relevant data. We believe the

---

[137] Adam Wright, et al., *Best practices for preventing malfunctions in rule-based clinical decision support alerts and reminders: results of a Delphi study*, 118 International journal of medical informatics (2018).

[138] See John D McGreevey III, et al., Reducing alert burden in electronic health records: state of the art recommendations from four health systems, 11 APPLIED CLINICAL INFORMATICS (2020); Juan D Chaparro, et al., Reducing interruptive alert burden using quality improvement methodology, 11 APPLIED CLINICAL INFORMATICS (2020).

proposed feedback data identified for export represents a minimum set that users would find valuable for evaluation of DSIs they use. However, we welcome comment on the proposed scope of these feedback data, utility for evaluation of their DSIs, and the potential for such data to be used in conjunction with quality metrics.

We propose that such feedback data be available for export by users for analysis in a computable format, so that it can be associated with other relevant data, such as diagnosis, other inputs into the DSI, and the outputs of the DSI for a particular patient, to evaluate and improve DSI performance. We note that "computable format," is consistent with current requirements in § 170.315(b)(10)(i)(D) for EHI Export, and we clarify that "computable format" is also referred to as "machine readable," in other contexts, which is not synonymous with "digitally accessible."[139] In addition to quality improvement of the DSI, such an export would facilitate research, associating feedback data with other relevant data, and linking the DSI to patient health outcomes, including assisting in identifying and reducing health disparities and possible discriminatory outcomes. This proposal would not require specific formatting requirements for such feedback mechanisms. We invite comment on these proposals.

iii. Proposed § 170.315(b)(11)(iii) Evidence-based Decision Support Interventions

We propose in § 170.315(b)(11)(iii) to establish "evidence-based decision support interventions," with a minor revision to current requirements that are part of the CDS criterion in § 170.315(a)(9)(iii). This proposal would replace the current construct in § 170.315(a)(9)(iii), which states a Health IT Module must enable evidence-based decision support interventions "based on each one and at least one combination of" the data referenced in paragraphs § 170.315(a)(9)(ii)(B)(*1*)(*i*) through (*vi*). We propose that Health IT Modules supporting evidence-based DSIs must have the ability to support "any," meaning all, of the revised data referenced in paragraphs § 170.315(b)(11)(ii)(B)(*1*)(*i*) through (*viii*). This proposal would broaden the scope of

[139] See also 85 FR 25879 discussion of machine readable.

data elements that Health IT Modules must support when enabling evidence-based DSIs to include data expressed by the standards in § 170.213, which is proposed to include USCDI v3 elsewhere in this preamble.

This proposal would not prescribe the intended use of the evidence-based DSI. Rather, this subparagraph, in combination with the data referenced in § 170.315(b)(11)(ii)(B)(*1*), represent the scope of evidence-based DSIs and scope of data that Health IT Modules certified to § 170.315(b)(11) should enable for purposes of certification under our Program. We invite comment on this proposal.

iv. Proposed § 170.315(b)(11)(iv) Linked Referential CDS

We propose to replicate what is currently in § 170.315(a)(9)(iv) as § 170.315(b)(11)(iv) with a modification to reference the criterion in § 170.315(b)(11) wherever the current reference is to § 170.315(a)(9). We propose no further changes at this time. This proposal therefore reflects the capabilities included in the CDS criterion for which health IT developers of certified health IT have years of familiarity and can find, for comparison purposes in 45 CFR 170.315(a)(9). However, we welcome comment regarding the functionalities and standards listed in § 170.315(a)(9)(iv), the HL7 Context Aware Knowledge Retrieval Application ("Infobutton") standards, including whether linked referential CDS are commonly used with, or without, the named standards in § 170.315(a)(9)(iv)(A)(*1*) and (*2*) and whether we should continue to require use of these standards.

v. Proposed § 170.315(b)(11)(v) Predictive Decision Support Interventions

We propose to reference a new intervention type, "predictive decision support intervention," in § 170.315(b)(11)(v), and we propose a corresponding definition in § 170.102. We also propose in § 170.315(b)(11)(v)(A) that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) attest "yes" or "no" as to whether their Health IT Module enables or interfaces with one or more predictive DSIs based on any of the data expressed in the

standards in § 170.213, including USCDI v3 as proposed elsewhere in this preamble. Below we discuss our proposal in § 170.102 for a definition of predictive DSIs to provide necessary context for our proposals for attestation in § 170.315(b)(11)(v).

Proposed definition of predictive decision support intervention

We propose a definition of "predictive decision support intervention" in § 170.102 to mean "technology intended to support decision-making based on algorithms or models that derive relationships from training or example data and then are used to produce an output or outputs related to, but not limited to, prediction, classification, recommendation, evaluation, or analysis."

Such predictive DSIs are based on the use of predictive model(s). In this proposed rule, "model" refers to a quantitative method, system, or approach that applies statistical, economic, bioinformatic, mathematical, or other techniques (e.g., algorithm or equations) to process input data into quantitative estimates. Models are simplified representations of real-world relationships among observed characteristics, values, and events. Predictive models are those that have 'learned' relationships from a training or historic data source, generally using some form of statistical or machine learning approach. Predictive models are then used to predict unknown values such as scores, classifications, recommendations, or evaluations using electronic data based on the relationships learned in the training data.[140] Other terms that may be used in healthcare to describe this area and may have similar meanings include 'clinical algorithm,' 'automated decision-making system,' or 'augmented decision-making' tools or technologies, although some of these terms may also be used to refer to evidence-based DSIs. Our use of the term predictive DSI is not tied to a specific use case, such as those that fall under treatment (clinical or medical purpose), payment (financial) or health care operations (administrative), nor those that support clinical research or public health,[141] but rather encompasses the broad forms

[140] Cf. https://www.gartner.com/en/information-technology/glossary/predictive-modeling.
[141] See 45 CFR 164.501 and 45 CFR 164.512(b).

that DSIs can take, including but not limited to alerts, order sets, flowsheets, dashboards, patient lists, documentation forms, relevant data presentations, protocol or pathway support, reference information or guidance and reminder messages.[142]

We intend for our use of the phrase "intended to support decision-making" to be interpreted broadly and to encompass technologies that require users' interpretation and action as well as those that initiate management and require action to contest. Our use of predictive DSI is not tied to the level of risk or degree to which the predictive DSI informs or drives treatment, is relied upon by the user, relates to time sensitive action, or whether the predictive DSI is augmentative or autonomous.[143]

We intentionally use the term "predictive decision support intervention" in addition to the Program's existing and parallel use of the term "evidence-based decision support intervention," for example as used in § 170.315(a)(9)(iii). We differentiate predictive DSIs as those that support decision-making by learning or deriving relationships to produce an output, rather than those that rely on pre-defined rules based on expert consensus, such as computable clinical guidelines, to support decision-making. This distinction is not meant to convey that predictive DSIs are without evidence or that such interventions have not demonstrated clinical effectiveness. We expect that predictive DSIs will be supported by a robust evidence base, which may include prospective clinical trials, observational studies, and other evidence published as peer-reviewed literature describing the intervention's purpose, intended use, and performance. We seek comment on whether this definition effectively delineates between DSIs that would be considered predictive versus those that are evidence-based DSIs, to use existing terminology.

---

[142] Agency for Healthcare Research and Quality, *Section 4 - Types of CDS Interventions*: https://digital.ahrq.gov/ahrq-funded-projects/current-health-it-priorities/clinical-decision-support-cds/chapter-1-approaching-clinical-decision/section-4-types-cds-interventions.

[143] *See generally* IMDRF | Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations: https://www.imdrf.org/documents/software-medical-device-possible-framework-risk-categorization-and-corresponding-considerations.
See AMA | CPT® Appendix S: Artificial Intelligence Taxonomy for Medical Services and Procedures: https://www.ama-assn.org/system/files/cpt-appendix-s.pdf for definitions of "augmentative" and "autonomous"; ANSI/CTA Standard, The Use of Artificial Intelligence in Health Care: Trustworthiness ANSI/CTA-2090: https://shop.cta.tech/collections/standards/products/the-use-of-artificial-intelligence-in-healthcare-trustworthiness-cta-2090?_ga=2.195226476.1947214965.1652722036-709349392.1645133306.

We propose a definition of predictive DSI that would cover a wide variety of techniques from algebraic equations to machine learning and natural language processing (NLP). For example, the proposed definition would include the Acute Physiology and Chronic Health Evaluation IV (APACHE IV) model. That model, which predicts in-hospital mortality for patients in intensive care units, was initially trained and validated in data from 45 hospitals including over one hundred thousand individuals in 2006.[144] Similarly, models designed to estimate risk of a first Atherosclerotic Cardiovascular Disease, trained and validated on pooled cohorts of large studies, would meet the proposed definition.[145] Because these models used multiple regression methods, the trained model can be expressed as a relatively simple algebraic equation.

Our proposed definition would also include more complex predictive models leveraging machine learning. For example, readmission models developed by combining multiple Naïve Bayes algorithms or deep unified networks trained and validated on over ten thousand individuals and resulting in models that can be applied to patients in operational contexts would meet the proposed definition of a predictive DSI.[146] This definition would include predictive DSIs that use adaptive, online or unlocked models, that is, models that continue to adapt when exposed to new data, as well as those that are locked to the relationships learned in training data. This definition would also include predictive DSIs that use NLP and large language models (LLMs) (sometimes referred to as generative AI),[147] like GPT-3 and LaMDA that power chatbots

---

[144] Zimmerman, Jack E., et al. "Acute Physiology and Chronic Health Evaluation (APACHE) IV: hospital mortality assessment for today's critically ill patients." Critical care medicine 34.5 (2006): 1297-1310.

[145] Goff Jr, David C., et al. "2013 ACC/AHA guideline on the assessment of cardiovascular risk: a report of the American College of Cardiology/American Heart Association Task Force on Practice Guidelines." *Circulation* 129.25_suppl_2 (2014): S49-S73.

[146] Sara Bersche Golas, et al., *A machine learning model to predict the risk of 30-day readmissions in patients with heart failure: a retrospective analysis of electronic medical records data*, 18 BMC MEDICAL INFORMATICS AND DECISION MAKING (2018); Khader Shameer, et al., Predictive modeling of hospital readmission rates using electronic medical record-wide machine learning: a case-study using Mount Sinai heart failure cohort (World Scientific 2017).

[147] See McKinsey & Company, What is generative AI? (January 2023), https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai?cid=other-eml-ofl-mip-mck&hlkid=87d4afa80191467ab4807f2084f75dc3&hctky=12683708&hdpid=42989045-434a-40cd-ab7e-3d75ebf84ed8.

like ChatGPT and Bard, respectively.[148] The definition would not be limited based on the specific nature of the data to be processed; for instance, models that analyze text or images are included.[149]

Predictive models represent one widely used form of AI, but do not include all AI. Our proposed definition would not include the computer readable implementation of clinical guidelines or similar types of knowledge except when those guidelines—and the interventions implemented based on them—incorporate a predicted value, such as a predicted risk, in guiding clinical decision-making. We note that, in this proposed rule, the term "intervention" in "prediction decision support intervention" is not intended to mean an intervention (medicine, medical procedure, or medical treatment) as the term is used in the practice of medicine,[150] but rather, an intervention occurring within a workstream, including but not limited to alerts, order sets, flowsheets, dashboards, patient lists, documentation forms, relevant data presentations, protocol or pathway support, reference information or guidance, and reminder messages. Our use of the term intervention is consistent with how the Program has used the term in § 170.315(a)(9).

As proposed in § 170.102, the definition of a predictive decision support intervention would not include simulation models that use modeler-provided parameters rather than training data or unsupervised machine learning techniques that do not predict an unknown value (i.e., are not labeled) among other technologies. For instance, the use of an unsupervised learning model within decision support would not meet our definition of a predictive DSI, nor would the use of developer-supplied parameters to simulate operating-room usage and develop an effective

---

[148] See generally Primack, Dan. Here come the robot doctors. (January 18, 2023), https://www.axios.com/2023/01/18/chatgpt-ai-health-care-doctors; OpenAI, ChatGPT: https://openai.com/blog/chatgpt/; Pichai, Sundar. Optimizing Language Models for Dialogue, (Feb. 6, 2023) https://openai.com/blog/chatgpt/; https://blog.google/technology/ai/bard-google-ai-search-updates/.

[149] Prakash M Nadkarni, et al., *Natural language processing: an introduction*, 18 JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION (2011); Thomas M Maddox & Michael A Matheny, Natural language processing and the promise of big data: small step forward, but many miles to go § 8 (Am Heart Assoc 2015); Xiong Liu, et al., Predicting heart failure readmission from clinical notes using deep learning (IEEE 2019).

[150] The ONC Program's use of the term "intervention" is different from "clinical intervention" as defined under FDA regulation that includes a range of regulated products, such as a medication or medical device. We note that there may be a software-as-a-medical device (SaMD) that is considered a "clinical intervention" and subject to FDA authority.

scheduling strategy. We seek comment on whether the definition should be scoped to include these or other additional forms of decision-making algorithms, tools, and models. We request comment on whether there are prominent models (e.g., simulation models, unsupervised learning models) used to support decision-making in healthcare that are not effectively captured under the proposed definition of a predictive DSI, and, if so, whether it is feasible and appropriate to include such models in the scope of this proposed rule.

Attestation for predictive decision support interventions

In § 170.315(b)(11)(v)(A), we propose that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) attest "yes" or "no" to whether their Health IT Module enables or interfaces with predictive DSIs based on any of the data expressed in the standards in § 170.213. This attestation requirement would have the effect of permitting developers of certified health IT to certify to § 170.315(b)(11) without requiring their Health IT Modules to enable or interface with predictive DSIs. However, for those developers of certified health IT that attest "yes" as described in § 170.315(b)(11)(v)(A), we describe further in this section applicable requirements related to such developers and their Health IT Modules.

By way of example, we expect that developers of certified health IT should attest "yes," if any of the following are true: (1) the developer develops (self-develops) predictive DSIs for use in their certified Health IT Module; (2) the developer's Health IT Module enables or interfaces with predictive DSIs developed by its end users or customers, such as a healthcare organization or medical center; or (3) the developer's Health IT Module enables or interfaces with predictive DSIs developed by a third-party content provider or developer, such as a technology firm that specializes in predictive model development.

We clarify that "enables" means that the developer of certified health IT has the technical capability to support a predictive model or DSI within the developer's Health IT Module. We understand that predictive DSIs can be configured in various ways, including as user-developed or third party-developed applications for use within or as a part of a Health IT Module. We also

understand that predictive DSIs can be developed by a developer of certified health IT for use within or as a part of their own Health IT Module. We clarify that applications developed by other parties and self-developed applications that are used within or as a part of a Health IT Module would mean that the Health IT Module is considered to "enable" predictive DSIs. For example, if the calculations or processing for a predictive DSI occur within the Health IT Module, either through a standalone application developed by other parties or an application self-developed by a developer of certified health IT for use within a Health IT Module, we would consider this "enabling." We clarify that this technical capability to support a predictive model or DSI includes instances where predictive DSIs are enabled by default and instances where they can be enabled by users. We propose that if a developer's Health IT Module enables predictive DSIs, based on any of the data expressed in the standards in § 170.213, then a developer of certified health IT must attest "yes," in § 170.315(b)(11)(v)(A).

In contrast, we clarify that "interfaces with" means that the Health IT Module facilitates either (1) the launch of a predictive model or DSI or (2) the delivery of a predictive model or DSI output(s) to users when such a predictive model or DSI resides outside of the Health IT Module. For example, scenarios where the calculations for a predictive DSI occur outside the Health IT Module, and the predicted value or output gets sent to or through a Health IT Module, or to or through an application used within or as part of a Health IT Module, would be considered to "interface with." We would also consider a Health IT Module to "interface with," a predictive DSI in scenarios where an application is launched from a certified Health IT Module, including through the use of a single sign-on functionality. If a developer of certified health IT 's Health IT Module interfaces with predictive DSIs based on any of the data expressed in § 170.213, then a developer of certified health IT must attest "yes," to § 170.315(b)(11)(v).

We are aware that some organizations may use USCDI data exported or sourced from a certified Health IT Module to develop data-driven advanced analytics leveraging predictive models or technologies to provide insights for healthcare. In such circumstances, our proposed

requirements would only pertain if the output of the predictive model subsequently interfaced with a Health IT Module. The proposed requirement would not establish requirements for predictive technologies that are not enabled or do not interface with a Health IT Module.

We note that developers of certified health IT with a Health IT Module that enables or interfaces with predictive DSIs that use any of the data expressed in the proposed standards in § 170.213 must attest "yes" in § 170.315(b)(11)(v) if their Health IT Module(s) is certified to § 170.315(b)(11). We also propose as part of this attestation requirement in § 170.315(b)(11)(v) the option for a developer of certified health IT to attest "no," affirming the Health IT Module does not enable or interface with predictive DSIs that use any of the data expressed in the proposed standards in § 170.213. Should a developer of certified health IT's Health IT Module enable or interface with predictive DSIs that use only data elements outside the scope of the standards in § 170.213, we propose that the developer of certified health IT may attest "no." We invite comment on this proposal and whether the descriptions of "enable," or "interface with," are appropriately scoped to reflect the design, development, and use of these emerging technologies in healthcare.

Finally, we note that developers of certified health IT that attest "no" in § 170.315(b)(11)(v) would still be required to conform to the full scope of this criterion, including the provision of source attribute information as described in § 170.315(b)(11)(vi)(A) and (B) through their Health IT Module. The attestation requirement in § 170.315(b)(11)(v) is constructed to make support of predictive DSIs optional for a Health IT Module certifying to § 170.315(b)(11) and to establish conditional requirements if the developer of certified health IT with a Health IT Module attests "yes." Developers of certified health IT that attest "yes" in § 170.315(b)(11)(v) would be required to provide source attribute information through their Health IT Module in § 170.315(b)(11)(vi)(C), which includes by reference those source attributes listed in § 170.315(b)(11)(vi)(A) and employ or engage in intervention risk management practices as discussed in § 170.315(b)(11)(vii). We invite comment on these proposals.

vi. Proposed § 170.315(b)(11)(vi) Source Attributes

We propose in § 170.315(b)(11)(vi) that Health IT Module certified to § 170.315(b)(11) enable a user to review a plain language description of source attribute information as indicated at a minimum via direct display, drill down, or link out from a Health IT Module. This requirement would be for source attribute information pertinent to each DSI type: evidence-based DSIs in (b)(11)(iii), linked referential DSIs in (b)(11)(iv), and source attributes required for Health IT Modules that enable or interface with predictive DSIs as defined in § 170.102 when a certified health IT developer attests "yes" to the "predictive decision support interventions attestation" in § 170.315(b)(11)(v). We note that § 170.315(g)(3) "safety-enhanced design," applies to the existing § 170.315(a)(9) criterion and in keeping with that applicability, we propose that safety-enhanced and user-centered design processes described in § 170.315(g)(3) would apply to the new certification criterion proposed in § 170.315(b)(11) as well. We propose to update § 170.315(g)(3) accordingly to reference the proposed § 170.315(b)(11). We believe that requiring developers of certified health IT to make available the source attributes information referenced at those sections via direct display, drill down, or link out from their certified Health IT Modules would have an important impact in enabling informed and appropriate selection of DSIs for implementation and use. Addressing quality uncertainty similarly underlies the rationale for certification of all Health IT Modules. We discuss proposed revisions and additions to source attributes later in this section. We invite comment on this proposal.

vii. Proposed § 170.315(b)(11)(vi)(A) Source Attributes - Demographic, SDOH, and Health Status Assessment Data Use

We propose to include as source attributes in § 170.315(b)(11)(vi)(A)(*1*) through (*4*) the source attributes currently found in § 170.315(a)(9)(v)(A)(*1*) through (*4*). Additionally, we propose that the use of three additional specific types of data in a DSI be included as source attributes in § 170.315(b)(11)(vi)(A) – Demographic data elements in §

170.315(b)(11)(vi)(A)(*5*), SDOH data elements in § 170.315(b)(11)(vi)(A)(*6*), and Health Status Assessment data elements in § 170.315(b)(11)(vi)(A)(*7*). We note that "types of data in a DSI" means that the DSI includes any of these data as inputs or otherwise expressly rely on any of these data in generating an output or outputs. By proposing to modify the source attributes in § 170.315(b)(11)(vi)(A) relative to the existing attributes in § 170.315(a)(9)(v)(A), we expect that information would be made available to users if the specific data elements within these three data types were used in the DSI.

We propose in § 170.315(b)(11)(vi)(A)(*5*) that the use of Patient Demographics and Observations data identified in proposed § 170.315(a)(5)(i) be included as a source attribute. As noted in the Background section, demographic data, especially race, ethnicity, and preferred language (REL) and sexual orientation and gender identity, can influence how effective the DSI is for a given patient population and use case.

We propose in § 170.315(b)(11)(vi)(A)(*6*) that the use of SDOH data, represented in the proposed standards in § 170.213, be included as a source attribute. Specifically, we propose that if any of the four SDOH data elements that are part of USCDI v3 are used in a DSI, then they should be reported as part of the source attributes proposed in § 170.315(b)(11)(vi)(A)(*6*). These elements include "SDOH Assessment," "SDOH Goals," "SDOH Interventions," and "SDOH Problems/Health Concerns." We note that SDOH data elements are not categorized as a single data class in the USCDI, rather they are included across several different data classes in USCDI v3. We note that during the period of time when USCDI v1 is referenced in § 170.213, a Health IT Module certified to USCDI v1 is not required to include these and other data elements specific to USCDI v3 as part of source attributes.

We propose in § 170.315(b)(11)(vi)(A)(*7*) that the use of Health Status Assessment data represented in the standards in § 170.213 be included as source attributes. The data elements included in the Health Status Assessments data class include Health Concerns, Functional Status, Disability Status, Mental/Cognitive Status, Pregnancy Status, and Smoking Status. We believe

that SDOH and Health Status Assessment data will play a greater role in DSIs moving forward and including the use of these data elements as source attributes would provide much-needed transparency. We again note that during the period of time when USCDI v1 is referenced in § 170.213, a Health IT Module certified to USCDI v1 is not required to include these and other data elements specific to USCDI v3 as part of source attributes.

Including the use of REL, Sexual Orientation, Gender Information, SDOH, and Health Status Assessment data elements as part of source attributes for each DSI, so that information about them can be provided to users, as proposed in § 170.315(b)(11)(vi), would greatly improve the possibility of identifying and mitigating the risks of employing both evidence-based and predictive DSIs for patient care, including those related to exacerbating racial disparities and promoting bias. We encourage readers to review the Background of this section, III.C.5, for more discussion and evidence for relevant examples of such risks. We invite comment on these additions to source attributes in § 170.315(b)(11)(vi)(A), and we invite comment on additional data classes and elements, reflected in the standards in § 170.213, that ONC should consider including as source attributes.

We propose in § 170.315(b)(11)(vi) that all source attribute information must be available, as applicable, for user review via direct display, drill down, or link out from the Health IT Module when the intervention is developed by the developer of the Health IT Module. The intent of this proposed requirement is to enable users to make a more informed decision regarding whether and how a DSI should be used. For example, an evidence-based DSI that is based on Joint National Committee (JNC) Hypertension guidelines should indicate for the user of the certified Health IT Module that the DSI output (recommendation) for the first-line hypertension therapy incorporates Race so that the user is aware that the DSI's recommendation for Black patients and non-Black patients differs. Historically, we have not made the expectation that source attribute information be available via drill down or link out an explicit requirement, but we required that such information be available to end-users for CDS interventions (77 FR

54215). We understand that source attribute information may be presented in varied ways at various points of workflow and contain varying levels of detail and do not intend to limit the options by which this information can be made available. However, through conversations with interested parties, we learned that source attribute information is not routinely available to users at the point of care, so we propose to require source attribute information be available at a minimum, via direct display, drill down, or link out now to better ensure consistency in source attributes information availability.

We encourage developers of certified health IT to consider a hierarchy of users' needs when making these attributes available for users. Consistent with prior ONC discussion related to existing § 170.315(a)(9)(v) requirements for source attributes (77 FR 54215), the proposal would not require the automatic display of source attributes information when a recommendation, alert, or decision support output is presented that resulted from a DSI. We invite comment on this proposal.

viii. Proposed § 170.315(b)(11)(vi)(C) Source Attributes for Predictive Decision Support Intervention

As stated in the previous section, we propose in § 170.315(b)(11)(vi) to establish "source attributes" requirements. In this section we discuss proposals to include additional source attributes for predictive DSIs as we propose to define them in § 170.102. Specifically, we propose to add new source attributes in § 170.315(b)(11)(vi)(C) for all predictive DSIs that are enabled by or interface with certified Health IT Modules certified to § 170.315(b)(11). These source attributes are intended to provide users with greater insight into the model incorporated into a particular predictive DSI and will provide information for an array of uses, including in support of so-called "model cards" or algorithm "nutrition labels" that have been described by others.[151] This proposed requirement would apply to developers of certified health IT that, under

[151] Mitchell, Margaret, et al. "Model cards for model reporting." *Proceedings of the conference on fairness, accountability, and transparency*. 2019.

proposed § 170.315(b)(11)(v)(A), attest "yes" to enabling or interfacing with a DSI that meets the definition of a predictive DSI as proposed in § 170.102.

We believe additional transparency for predictive DSIs that enable or interface with Health IT Modules is appropriate because these DSIs often involve relatively opaque computational processes to arrive at the predictions on which such DSIs are based and rely on specific data and populations to learn relationships between features of the data. While the use of such models has enormous potential to improve many aspects of the healthcare delivery system including treatment, payment, health care operations (TPO); research; and public health activities, it can also result in harm, bias, or unlawful discrimination, as discussed earlier in this preamble in section III.C.5.a. This can be especially true in instances where the user is not fully informed of the potential limitations of the model, where there is potential misalignment between the user's application of the model and its intended use, where known inappropriate uses of the model are not communicated, or when the model is specified to accomplish known tasks without meeting the intended outcome.[152]

In developing proposed source attributes for predictive DSIs, we sought to balance prescriptiveness and flexibility. Our selection of proposed attributes was guided by review of existing model reporting guidelines, including fourteen different sets of recommendations for information to be reported on models and related standards.[153] In our review, we emphasized attributes that (1) were most commonly included in the reviewed reporting guidelines, (2) we believe would be most interpretable by both health IT professionals and users, (3) were focused on identifying issues of bias, and (4) were intended to show that the model would perform effectively outside of the specific context in which it was developed. In describing the proposed source attributes below, we have provided information on what we believe should be included in

---

[152] Sendak, et al., NPJ DIGITAL MEDICINE, (2020); Victoria Krakovna, et al., *Specification gaming: the flip side of AI ingenuity*, April 21. 2020.

[153] See, e.g., Lu, et al., Low adherence to existing model reporting guidelines by commonly used clinical prediction models, medRxiv 2021.07.21.21260282; ANSI/CTA-2090 The Use of Artificial Intelligence in Health Care: Trustworthiness; ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence.

each attribute based on our understanding of the current best practices in this area; however, given the varied technologies, applications, and contexts in which predictive DSIs may be used, we have sought to keep requirements sufficiently flexible to meet varied use cases.

The proposals in § 170.315(b)(11)(vi)(C) would not require disclosing or sharing intellectual property (IP) existing in the developer's health IT (including other parties' intellectual property). For example, the proposed requirement would not require developers of certified health IT (or any other model developers, for example, models developed by third parties or customers of the developer of certified health IT) to provide information about or report any details of the specific code, pipeline, statistical processes, or algorithms used to generate model predictions, which might be considered the developer's intellectual property. Instead, the proposed requirement would have developers of certified health IT report source attribute information related to data that was used to train the model, the proper (intended) use of the model, and the performance of the model as assessed through validation and fairness metrics. In this regard, the proposed source attributes are intended to establish consistent categories of minimum information availability that potential users need to make informed decisions regarding their use of a predictive DSI. We view this proposal as complementary to transparency efforts in other areas for product users such as nutrition labels, medication fact labels, and clinical trial results, which also focus on inputs, demonstrated value, and proper use.[154]

Proposed new source attributes for predictive DSI

We propose to add fourteen new source attributes for predictive DSIs that enable or interface with Health IT Modules. These include attributes that describe the models (sources) on which predictive DSIs are based in four broad categories: in § 170.315(b)(11)(vi)(C)(*1*) Intervention Details, in § 170.315(b)(11)(vi)(C)(*2*) Intervention Development, in § 170.315(b)(11)(vi)(C)(*3*) Quantitative Measures of Intervention Performance, and in §

[154] Sendak MP, Gao M, Brajer N, Balu S. Presenting machine learning model information to clinical end users with model facts labels. NPJ Digit Med. 2020 Mar 23;3:41. doi: 10.1038/s41746-020-0253-3. PMID: 32219182; PMCID: PMC7090057.

170.315(b)(11)(vi)(C)(*4*) Ongoing Maintenance of Intervention Implementation and Use. We describe the proposed specific attributes to be made available to users below. We also reiterate that we propose that this criterion remain subject to safety-enhanced design requirements for user centeredness by proposing changes to § 170.315(g)(3).

Consistent with our proposals in § 170.315(b)(11)(vi), we propose that these new source attributes listed in § 170.315(b)(11)(vi)(C) would be in plain language and available for user review via direct display, drill down, or link out from a Health IT Module certified to § 170.315(b)(11) and for which the developer attested "yes" in § 170.315(b)(11)(v)(A).

For six of the listed source attributes, we propose to include a phrase noting that information must be provided "if available." These include source attributes we propose in § 170.315(b)(11)(vi)(C)(*2*)(*iii*), (b)(11)(vi)(C)(*3*)(*iii*), (b)(11)(vi)(C)(*3*)(*iv*), (b)(11)(vi)(C)(*3*)(*v*). (b)(11)(vi)(C)(*4*)(*ii*), and (b)(11)(vi)(C)(*4*)(*iii*). Proposing flexibility to report on these source attributes "if available," reflects our understanding that the relevant information for these source attributes may not be available because, for instance, the related evaluation has not been conducted, such as in local data. We do not seek to prohibit the use of such models for lack of evaluation or validation, but our proposal intends to ensure that users are aware when such information exists and, if not, that the users understand the related attribute information is not available. In instances where information related to one of these six source attributes is not available, we propose in § 170.315(b)(11)(vi)(D)(*1*) that a Health IT Module clearly indicate when this information is not available for a user to review. While we do not prescribe how a Health IT Module must indicate that an attribute is missing, we clarify that the Health IT Module must communicate an attribute is missing unambiguously and in a conspicuous manner to a user.

We propose to require that information be provided for the remaining eight attributes that do not include the "if available" phrase, except as described in § 170.315(b)(11)(vi)(D). We note that developers of certified health IT that develop predictive DSIs for use in their Health IT Modules must provide this information and, if necessary, establish processes and protocols to

generate or gather the eight attributes that do not include the "if available" phrase. We note that the eight attributes that do not include the "if available" phrase reflect information that is routinely generated during model planning, development, and testing. These attributes are often commonly reported in academic validation studies of predictive models in healthcare and relate to information readily available for model creators, developers, or owners to report to users or customers. However, we clarify that we are establishing two affirmative actions: (1) developers of certified health IT that develop their own predictive DSIs, that are enabled by or interface with a Health IT Module, must generate or gather the proposed source attribute information in § 170.315(b)(11)(vi)(C); and (2) report the proposed source attribute information.

Intervention Details

We propose three source attributes related to details of predictive models and their proper use in § 170.315(b)(11)(vi)(C)(*1*) "Intervention Details." These source attributes are designed to convey information about how the model is incorporated into healthcare organizations' and into users' workflows, so that the model is presented at a time and for a population that would benefit from use of a predictive DSI based on the model. The following are descriptions of the proposed subsections related to Intervention Details:

- § 170.315(b)(11)(vi)(C)(*1*)(*i*) "Output of the intervention," is a description of the value that the model produces as an output, including whether the output is a prediction, classification, or other type of output. Users evaluating the model or deciding whether to use it should know what the model is predicting to ensure that the output is directly relevant to the way in which the users intend to use it. The absence of this information could greatly increase the risk that the model is misused or that its output is assumed to relate to something other than the 'label' (the target the model is predicting, e.g., the outcome the model is trained to predict as it has occurred and been recorded in historic or training data) the model was trained to predict.

The output of the model is the predicted value of the 'label' (outcome) that the model is trained on to make a prediction. An example would be to describe that the model is trained on patients labeled as either experiencing or not experiencing a readmission for heart failure within 30-days of initial discharge in training data where that event is known. The trained model would then produce as its output the likelihood that an individual will be readmitted among individuals recently discharged (for whom the event is not yet known). The absence of this information could greatly increase the risk that the model is misused or that its output is assumed to relate to something other than the label the model was trained to predict. Specifying the output allows users to determine if the output is appropriate or may inherently reflect low validity or bias because of concerns about the process that produces an output in the training data.[155] Recent evidence has shown that selecting a label and output—healthcare costs—that was created through biased historical and social processes that were reflected in the training data produced biased predictions when used to identify patients with high healthcare needs for preventive care.[156]

- § 170.315(b)(11)(vi)(C)(*1*)(*ii*) "Intended use of the intervention," is a description of the intent of the model developers in how the model is meant to be deployed and used, including its intended role in the identified use case. Whereas the "output of the intervention" describes the "what" that the model predicts, this attribute is about the "how," "to what end," "where," and "for whom" the model is designed and should be used. Information on intended use should clarify: (1) whether the model is intended for specific or general tasks and what those tasks are; (2) who the intended patient population is; (3) who the intended users of the model are, as well as the intended action of the user;

---

[155] Wei Luo, et al., *Guidelines for developing and reporting machine learning predictive models in biomedical research: a multidisciplinary view*, 18 JOURNAL OF MEDICAL INTERNET RESEARCH (2016); Christina Silcox, et al., *AI-enabled clinical decision support software: a "Trust and Value Checklist" for clinicians*, 1 NEJM CATALYST INNOVATIONS IN CARE DELIVERY (2020).

[156] Ziad Obermeyer, et al., *Dissecting racial bias in an algorithm used to manage the health of populations*, 366 SCIENCE (2019).

(4) the role of the model (e.g., whether it informs, augments, or replaces clinical management), which may be most clearly conveyed through use of a taxonomy such as those described by the International Medical Device Regulators Forum (IMDRF), American Medical Association, Consumer Technology Association, and others;[157] and (5) the logic underlying the model (for instance, the exact question the algorithm is supposed to answer, how it fits into specific clinical decision-making, and in what ways the inputs are appropriate to answer that question and, if appropriate, how that logic is associated with how the model should be used.

A description of how the model should be used can inform how the model is deployed in healthcare settings and help assure users that the model is fit for the purpose they are using it for. The absence of this information could greatly increase the risk that the model is deployed or used in situations that the model developers did not intend and that may result in invalid predictions or harm to the intended beneficiaries (model subjects, e.g., patients). For example, using a model whose described output is "predicted risk of death" to triage patients to higher acuity care may be inappropriate if the model learned the risk of death based on whether those patients were previously effectively triaged. In this example, prior triage decisions are incorporated into the model's prediction, and this could lead to invalid predicted risk of death.[158] Information clarifying that the intended use is for post-triage management decisions could be useful to avoid this inappropriate use.

- § 170.315(b)(11)(vi)(C)(*1*)(*iii*) "Cautioned out-of-scope use of the intervention," is a description of tasks, situations, or populations to which the model developer cautions a

---

[157] IMDRF | Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations: https://www.imdrf.org/documents/software-medical-device-possible-framework-risk-categorization-and-corresponding-considerations. AMA | CPT® Appendix S: Artificial Intelligence Taxonomy for Medical Services and Procedures: https://www.ama-assn.org/system/files/cpt-appendix-s.pdf.
CTA | ANSI/CTA Standard, The Use of Artificial Intelligence in Health Care: Trustworthiness ANSI/CTA-2090: https://shop.cta.tech/collections/standards/products/the-use-of-artificial-intelligence-in-healthcare-trustworthiness-cta-2090?_ga=2.195226476.1947214965.1652722036-709349392.1645133306.
[158] Sendak, et al., NPJ DIGITAL MEDICINE, (2020).

user against applying the predictive model. An example of a description could be "this model is intended for use on inpatients only. Insufficient patient data in the emergency department may lead to poor model performance in that context." This description should include known risks, inappropriate settings, inappropriate uses, or known limitations of the model. To the extent possible, the description should inform users about tasks, situations or populations related to the intended use of the model in which the model may not perform as expected. Paired with information on the intended use source attribute proposed in § 170.315(b)(11)(vi)(C)(*1*)(*ii*), a description of out-of-scope uses is important to inform use of models and avoid potential misinterpretation of model output by healthcare organization leaders and clinicians, thereby ensuring potential harm is avoided.[159]

Intervention Development

We propose three source attributes related to model development in § 170.315(b)(11)(vi)(C)(*2*), "Intervention Development." These proposed attributes relate to describing steps in the model design and development process to provide users with a sense of how well the model is likely to perform across diverse patients and environments (e.g., diverse clinical care settings, technologies, and work/treatment patterns). The following are descriptions of the proposed source attributes related to Intervention Development:

- § 170.315(b)(11)(vi)(C)(*2*)(*i*) "Input features of the intervention including description of training and test data" is a description of the data on which the model learned relationships (often called the training data or training set) and the data on which the model was tested during development (often called the test data or test set). This description should include: (1) exclusion and inclusion criteria that influenced who was included in data sets; (2) statistical characteristics—including sample size—of the demographic and other key variables in these data (including those listed in

[159] Mitchell, et al. 2019; Sendak, et al., NPJ DIGITAL MEDICINE, (2020).

§ 170.315(b)(11)(vi)(A), as the developer views as appropriate) to assess representativeness; (3) the source and clinical setting from which the data was generated, which should be described so that the relevance of the data to the deployed setting and the potential for bias in that setting can be considered; (4) the extent of missing values in the training and testing data sets; and (5) other attributes related to data quality, such as the comprehensiveness of the data and the process of collecting the data should be included as the developer determines what is relevant while examining the data during pre-processing, creation, and testing of the model.

The information listed above is similar to requirements for clinical trials to report information on the baseline data of the sample included in the trial. Beyond the information above, the description of this source attribute should include what data is expected to be present for the model to generate accurate predictions. This description should allow users to evaluate whether sufficient data is available for the model to make valid predictions.

Descriptions of training and test data could allow model users to ensure that the development data the model was trained on had sufficient patients similar to those for whom the model would be used to inform effective model predictions. Predictive models developed using datasets that are not broadly representative may learn relationships applicable only to some groups. Those models are then likely to perform well only within those groups. For example, models predicting heart attack onset trained on data containing few women may perform poorly because diagnostic patterns are different for women.[160] Displaying information on the data sets that models were trained on could also help identify ethical issues in the data set.[161]

---

[160] Charles Maynard, et al., *Gender differences in the treatment and outcome of acute myocardial infarction: results from the Myocardial Infarction Triage and Intervention Registry*, 152 ARCHIVES OF INTERNAL MEDICINE (1992); Viola Vaccarino, et al., *Sex-based differences in early mortality after myocardial infarction*, 341 NEW ENGLAND JOURNAL OF MEDICINE (1999).

[161] Karen L Boyd, *Datasheets for Datasets help ML Engineers Notice and Understand Ethical Issues in Training Data*, 5 PROCEEDINGS OF THE ACM ON HUMAN-COMPUTER INTERACTION (2021); Mitchell, et al. 2019.

- § 170.315(b)(11)(vi)(C)(*2*)(*ii*) "Process used to ensure fairness in development of the intervention" is a description of the approach the model developer has taken to ensure that the model output is fair—that is, that the output is not unduly biased toward an individual or group based on an individual's or group's inherent or acquired characteristics. For example, this attribute might state that in pre-processing the data before training the model, the developers employed a "disparate impact remover" transformation across race or ethnicity groups based on a well-known approach.[162]

  This description should include approaches to manage, reduce, or eliminate bias in models and could be similar to a brief synopsis of risk mitigation practices and outcomes related to fairness for this DSI, as described further in the intervention risk management practices proposed in § 170.315(b)(11)(vii)(A)(*1*) through (*3*). Many such approaches exist; however, there is no universal best process to ensure fairness.[163] We believe it is a best practice for approaches to fairness to be informed by privacy-related needs because of concerns that some fairness enhancing approaches could increase privacy risks.[164] Providing information on what approaches were applied to address potential bias in model development would allow users to better evaluate whether model developers have adequately considered and addressed risk of bias in model development, and therefore the likelihood of bias in the model, which could potentially result in bias model outputs and patient outcomes if the model is used.

- § 170.315(b)(11)(vi)(C)(*2*)(*iii*) "External validation process, if available" is a description of how and in what source, clinical setting, or environment a model's validity and fairness has been assessed other than the source training and testing data. This should include a description of: (1) who conducted the external testing (e.g., the model

---

[162] Feldman, et al. 2015.
[163] Jon Kleinberg, et al., *Inherent trade-offs in the fair determination of risk scores*, ARXIV PREPRINT ARXIV:1609.05807 (2016); Mehrabi, et al., ACM COMPUTING SURVEYS (CSUR), (2021).
[164] Hongyan Chang & Reza Shokri, On the privacy risks of algorithmic fairness (IEEE 2021).

developer, developer of certified health IT, or an independent third party); (2) the setting from which the external data was derived; (3) the demographics of patients in external data; and (4) a brief description of how external validation was carried out.

A description of the external validation process undertaken can allow users to consider how well the model has been shown to perform, and in particular, how well it performs in similar settings as presented by independent parties.[165] Model performance measured in novel data sources, measured by independent third-parties, or both, conveys a stronger signal that the model is likely to perform well in new environments compared to models that are tested only by the developer or tested only within a test data set split from the training data but originating from the same data source as the original training data set.[166]

Quantitative Measures of Intervention Performance

We propose five source attributes relevant to validation or evaluation of the performance (including accuracy, validity, and fairness) of the predictive model and evaluation of its effectiveness in § 170.315(b)(11)(vi)(C)(*3*) "Quantitative measures of Intervention Performance."

- § 170.315(b)(11)(vi)(C)(*3*)(*i*) "Validity of prediction in test data," is the presentation of the measure or set of measures related to the model's validity (often referred to as performance) when tested in data derived from the same source as the initial training data. These measures show that the model is accurate because its output aligns with observed values in data where label values are known. These measures show whether the model's predictions (intended outcome) match the actual outcomes.

---

[165] Richard D Riley, et al., *External validation of clinical prediction models using big datasets from e-health records or IPD meta-analysis: opportunities and challenges*, 353 BMJ (2016); Wong, et al., JAMA INTERNAL MEDICINE, (2021).

[166] Silcox, et al., NEJM CATALYST INNOVATIONS IN CARE DELIVERY, (2020); Hernandez-Boussard, et al., JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION, (2020).

Selection of measures should be guided by the model developer's consideration of what measures might be most meaningful and relevant to users of the model according to the expected use of the model and the technical knowledge of expected users and implementation teams. For example, sensitivity, specificity, and positive predictive values—which are generally familiar to clinicians through experience with diagnostic tests—might be preferred versus area under the receiver operator curve and area under the precision-recall curve for binary classifiers, which less directly relate to the performance of models as implemented at specific thresholds.

This proposal would not prescribe the specific performance or validation measures to be used or included as part of the source attributes requirements but would require that some performance or validation measure(s) be used and included in the source attribute. Numerous measures exist to measure validity and performance because of the variety of types of predictive models, their outputs, and intended uses. It is likely that selection of informative performance measures would depend on model type and task (e.g., prediction, classification, recommendation or other). For instance, mean-squared error might be the appropriate measure for models predicting continuous values while recall at rank k, mean average precision at rank k, or similar measures might be appropriate for recommender systems.

Information on the model's measured performance is important to users for determining how much weight to apply to its prediction, given that predictive DSIs are based on models and data that they have learned from and generally do not rely on clinical guidelines to support the model's decision-making, as discussed earlier in this section and in the definition of predictive DSI proposed in § 170.102.

- § 170.315(b)(11)(vi)(C)(*3*)(*ii*) "Fairness of prediction in test data," is the presentation of the measure or set of measures related to the model's fairness (evaluation of fairness in a

model) in terms of the accuracy of its output across certain groups in data derived from the same source as the initial training data.

Evaluation of the fairness of models is one essential component in ensuring that models are not producing biased predictions or resulting in biased impacts to individuals. Numerous approaches and related measures exist to measure the fairness of model outputs. Examples of potential fairness measures include positive predictive parity, false positive error rate balance and false negative error rate balance, equivalent calibration within groups, and mean residual difference. The relevant groups or factors across which fairness should be established are also likely to vary from one model to the next, and model developers would need to determine which factor their model's performance should be evaluated or stratified by. Likely candidates include but are not limited to race, ethnicity, preferred language, sex, gender information, sexual orientation, religion, age, national origin, disability, veteran status, and genetic information or additional information related to care that has historically been stigmatized such as reproductive or behavioral health information.[167] Similar to measures related to validation described above, measures should be selected based on their relevance to users and the model task or function. The appropriateness of these approaches would depend on the specific context. This proposal would not prescribe the specific fairness measures to be used or presented (reported) because we are unaware of universal measures that would be applicable to all predictive DSIs. However, we reiterate that our proposals would require that some fairness measure(s) be used or presented. We seek comment on whether specific measures of fairness would be relevant across all predictive DSIs.

- § 170.315(b)(11)(vi)(C)(*3*)(*iii*) "Validity of prediction in external data, if available," is the presentation of the same or similar measures used to report model validity in test data

[167] See section III.C.10. See also Blueprint for an *AI Bill of Rights* (October 4, 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/#discrimination (discussing algorithmic discrimination protections).

in § 170.315(b)(11)(vi)(C)(*3*)(*i*) except that these measures relate to validity measured in data external to—that is, from a different source than—the primary training data. As noted above, validity as tested in data from sources external to the initial training and test data (which are often drawn from the same source), especially when evaluated by independent parties, provides more confidence in the performance of the model in different environments. It is therefore important for users to see measures related to model performance outside the development data or to be clearly informed when the model has not been evaluated in external data.

- § 170.315(b)(11)(vi)(C)(*3*)(*iv*) "Fairness of prediction in external data, if available," is the presentation of the same or similar measures used to report model fairness in test data described in § 170.315(b)(11)(vi)(C)(*3*)(*ii*) except that these measures relate to fairness measured in external data (i.e., data from a different source than the primary training data). Fairness in external data, especially when evaluated by an independent party, provides more confidence that the model would produce useful predictions in different environments and for diverse populations. It is therefore important for users to be able to view measures related to model performance outside the development environment or to be informed when the model has not been evaluated in external data.
- § 170.315(b)(11)(vi)(C)(*3*)(*v*) "References to evaluation of use of the model on outcomes, if available," are bibliographic citations or links to evaluations of how well the intervention, or model on which it is based accomplished specific objectives such as reduced morbidity, mortality, length of stay or other important outcomes. We are aware that the impacts of predictive models on outcomes are not always evaluated. We are therefore requiring source attribute information on the use of the model on outcomes "if available." Clearly labeling when that information is not available would be important to inform users as they implement and use the model.

Although it is important to assess a model's performance and fairness, the best indicator of whether and how the model should be used will come from evidence of its impact on health outcomes and other goals (e.g., operational efficiency) from various means of evaluating efficacy and effectiveness, including clinical trials. However, rigorous evaluations of impact may be limited in scope and context or diversity, for instance, due to challenges related to clinical trial recruitment and participation or biases in the populations treated by health centers best poised to conduct real-world evidence studies. These issues may impact a broad range of clinical evaluations, and potentially limit the external validity of evidence supporting use of some therapies as well as, in this context, some predictive DSIs.[168] These challenges may be particularly acute in the evaluation of predictive DSIs because predictive models may perform substantially differently in novel environments.[169] Therefore, evidence from the evaluation of outcomes from model outputs is best coupled with measures of the model's validity and fairness as described above.

Ongoing Maintenance of Intervention Implementation and Use

We propose three source attributes related to the "ongoing maintenance of intervention implementation and use," in § 170.315(b)(11)(vi)(C)(*4*). The following are descriptions of the proposed source attributes related to ongoing maintenance of intervention implementation and use:

- § 170.315(b)(11)(vi)(C)(*4*)(*i*) "Update and continued validation or fairness assessment schedule," is a description of the process and frequency by which the model's performance is measured and monitored in the local environment and corrected when risks related to validity and fairness are identified. It is therefore similar to a synopsis of

[168] See FDA, Enhancing the Diversity of Clinical Trial Populations – Eligibility Criteria, Enrollment Practices, and Trial Designs Guidance for Industry, (November 2020), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/enhancing-diversity-clinical-trial-populations-eligibility-criteria-enrollment-practices-and-trial.
[169] Steyerberg & Harrell, JOURNAL OF CLINICAL EPIDEMIOLOGY, (2016).

risk analysis and mitigation practices described later in this preamble and applies to the individual DSI. This information would be similar to a synopsis of a plan for controlled changes of the model.[170] A description of which measures are used to assess validity, across which specific groups fairness is evaluated, and by what criteria poor performance or low fairness would be identified are important to inform users of the likely value of model predictions. Information should also include how often performance is evaluated and how often the model is updated to provide users with insight into the likelihood that the model may have degraded (i.e., no longer provides valid or accurate predictions) since it was last updated.

- § 170.315(b)(11)(vi)(C)(*4*)(*ii*) "Validity of prediction in local data, if available," is the presentation of the same or similar measures used to report model validity in test and external data in § 170.315(b)(11)(vi)(C)(*3*)(*i*) and (*iii*), except that these measures are derived in local data and that model validity in the local environment is monitored over time. As noted above, validity in local data may differ from validity in either test or external data and when available, provides additional confidence in the performance of the model within the setting, population, and context most relevant to users. Local validity measures should be included when available. However, we understand that it is likely that local evaluation of model performance may not be feasible in all contexts. For instance, small practices or critical access hospitals may lack the resources, staff, population, and sample sizes to effectively evaluate performance in the local environment.[171]

---

[170] See FDA, *Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML)-Enabled Device Software Functions*, Draft Guidance, (April 2023), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial?utm_medium=email&utm_source=govdelivery; FDA, *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)*, Discussion Paper and Request for Feedback, https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf.

[171] Wong et al. External Validation of a Widely Implemented Proprietary Sepsis Prediction Model in Hospitalized Patients. *JAMA Intern Med.* 2021;181(8):1065–1070. doi:10.1001/jamainternmed.2021.2626.

- § 170.315(b)(11)(vi)(C)(*4*)(*iii*) "Fairness of prediction in local data, if available," is the presentation of the same or similar measures used to report model validity in test and external data in § 170.315(b)(11)(vi)(C)(*3*)(*ii*) and(*iv*), except that these measures are derived in local data. We include the reporting of fairness as an individual source attribute distinct from validity because users should be informed, separately from issues of overall validity, of the observed fairness of the model in the local environment to identify how likely it is that the model is providing valuable predictions for the type of individual about whom the model is being used to inform a decision. Because of concern that model performance in local implementations may differ substantially from performance in test and even external data, several groups have highlighted the importance of evaluating fairness of models within local information systems to ensure that model performance in the specific environment of their use is similar to performance in other data.[172]

We believe these proposed additional source attributes are necessary to enhance information transparency about the fairness, appropriateness, validity, effectiveness, and safety of predictive DSIs, so that users can make informed decisions about their application and use. As noted above, we have sought a balance between limited prescriptiveness and sufficient detail to enable robust and broadly applicable reporting of information on source attributes to users. We request comment on whether there are items contained within the proposals described above that we should explicitly require as elements of source attributes information. In particular, we request comment on whether to divide the proposed "intended use" source attribute in § 170.315(b)(11)(vi)(C)(*1*)(*ii*) described above into multiple attributes including a statement of the intended use, the role of the model in decision-making, the logic underlying the model (including

[172] Silcox, et al., NEJM CATALYST INNOVATIONS IN CARE DELIVERY, (2020); Sendak, et al., NPJ DIGITAL MEDICINE, (2020); *Variable generalization performance of a deep learning model to detect pneumonia in chest radiographs: a cross-sectional study;* Andrew Wong, et al., *External validation of a widely implemented proprietary sepsis prediction model in hospitalized patients*, 181 JAMA INTERNAL MEDICINE (2021).

information on the clinical rationale, which could allow users or implementers to evaluate whether the logic underlying the model is applicable to the individual and context in which they are using the model), the intended users, and the intended patient population or object of the model. We also request comment on whether to divide the proposed "input features of the intervention" source attribute in § 170.315(b)(11)(vi)(C)(*2*)(*i*) into multiple attributes including information on inclusion and exclusion criteria, demographics, data source or setting, data quality, missingness, and data that must be available to facilitate prediction. We similarly request comment on whether to divide the proposed "external validation process" at source attribute § 170.315(b)(11)(vi)(C)(*2*)(*iii*) into sub-elements related to who conducted the evaluation, the setting, demographics of the data, and the process.

Because the proposed source attributes described here and the intervention risk analysis and mitigation practices proposed in § 170.315(b)(11)(vii)(A) cover closely related topics, such as processes and measures related to fairness and validity, it is likely that some of the information used to provide descriptions of source attributes, would be substantially similar or identical to information the developer of certified health IT uses to describe their IRM practices as described later in § 170.315(b)(11)(vii). In particular, this may be the case with information related to the "Process used to ensure fairness in development of the intervention" proposed in § 170.315(b)(11)(vi)(C)(*2*)(*ii*), the "External validation process" proposed in § 170.315(b)(11)(vi)(C)(*2*)(*iii*), and "Update and continued validation or fairness assessment schedule" proposed in § 170.315(b)(11)(vi)(C)(*4*)(*i*). This parallel structure is intentional to support alignment and not intended to be duplicative; rather it reflects that source attributes and IRM practices information would be available in different media (through a Health IT Module versus a publicly available hyperlink), to different individuals (potential users of the predictive DSI versus the public) and likely reviewed at different times (when using or implementing the predictive DSI versus more general availability). We encourage developers to consider these

differing media, audiences, and uses when considering the type and depth of information to report for each item.

In this proposed rulemaking, we are also considering requirements that would enable a user to review via direct display, drill down, or link out from the Health IT Module additional source attributes beyond the fourteen attributes proposed and discussed above. Some of these additional attributes relate to facets of intervention risk management practices in § 170.315(b)(11)(vii), as discussed in section III.C.5.c.x. There are many voluntary reporting guidelines developed by industry, academia, and other interested parties designed to facilitate evaluation of predictive models, their output, and in some cases their impact, and the relevance of results of those evaluations to specific contexts, patients, and clinical decisions. However, these reporting guidelines do not uniformly highlight the same type of information to make available about a model. Based on our review of available literature and documentation, interested party input, and in consultation with the Agency for Healthcare Research and Quality (AHRQ) and Food and Drug Administration (FDA), we believe that the following additional source attributes could help achieve our stated objectives, and we are considering requiring certified Health IT Modules to enable a user to review information about these additional source attributes via direct display, drill down, or link out from the certified Health IT Module, consistent with proposed requirements in § 170.315(b)(11)(vi):

Intervention Details

- Information on the explainability (defined as the ability to explain a 'black box' model, often through the use of a second model[173]), or interpretability of the model, which means models that are directly understandable by their intended users and often subject to some constraints that make it easier to follow relationships within the data and how predictions were generated (we note that this information would be available if we adopt the

[173] Cynthia Rudin, *Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead*, 1 NATURE MACHINE INTELLIGENCE (2019).

proposed intervention risk management in § 170.315(b)(11)(vii), but we are considering requiring this information as source attributes);

- Information on whether a DSI meets the definition of a medical device under the FDA definition according to an internal review or because it has been reviewed by FDA in a premarket submission;[174]
- Any known ethical considerations related to data acquisition and use (e.g., information on consent from individuals whose data is used during model development and validation);[175]

Intervention Development

- Specifics on the source of the output or information presented through the DSI, including whether it was derived from meta-analysis, other synthesis of clinical studies, statistical modeling, AI/ML techniques, or some other method, and details on the type of model used, and model-building procedures;[176]
- Details on how model prediction and classification cut-points were selected relative to defined outcomes (e.g., how "high" risk groups were defined or what threshold was used to recommend a given course of action, such as selection of a therapy);
- Security and privacy-preserving approaches included in model development (e.g., how personal identifiers were removed or masked);[177]
- List of data elements or data classes used in the model and how they were used in the model in terms of categories or transformation;

---

[174] *See* FDA discussion on device software functionality, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software.
[175] See also section III.C.5.c.xi of this proposed rule "Data Practices and Governance: Ethical, Legal, and Social Implications of Data Collection and Use."
[176] See also FDA, *Clinical Decision Support Software Final Guidance* (September 2022), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software?utm_medium=email&utm_source=govdelivery.
[177] See also section III.C.5.c.xi of this proposed rule "Data Practices and Governance: Ethical, Legal, and Social Implications of Data Collection and Use."

- Model verification, usually associated with simulation models and defined as the process of confirming through the provision of objective evidence that specified requirements have been fulfilled and that model implementation accurately represents the developer's conceptual description of the model (which may reflect information in the intended use of the intervention and output of the intervention source attributes) and its solution;

Quantitative Measures of Intervention Performance

- Model calibration or calibration curve, which represent the relationship between predicted values generated by the model and observed probabilities;
- Confidence intervals or other measures of uncertainty related to measures of performance, fairness, and effectiveness, which would provide more information on the precision of evaluations and assure users that reported performance was unlikely to have been achieved by chance;
- Model reliability, using reliability to mean the "ability of an item to perform as required, without failure, for a given time interval, under given conditions."[178]
- Prediction intervals or other measures of uncertainty around the prediction generated, which would help inform users of the precision of a given prediction and whether the true value may vary widely or narrowly from the predicted estimate;

Ongoing Maintenance of Intervention Implementation and Use

- Information on data quality and completeness,[179] which would be useful to ensure that the model is effectively implemented;[180]
- Whether the model incorporates data generated from the setting it has been deployed in and uses it to update the model in real-time, sometimes referred to as a model being 'online' or 'unlocked'.

---

[178] See ISO/IEC TS 5723:2022, https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:5723:ed-1:v1:en:term:3.2.12.
[179] See section III.C.5.c.xi of this proposed rule "Technical Standards and Data Management: Electronic Data Source, Capture, and Use."
[180] See *supra* note, 176.

- For online or unlocked models, any additional organizational or technical controls in place to evaluate the impact of the online or unlocked updating and results of that evaluation.
- For online or unlocked models, the controls in place to update the descriptions of source data to reflect the changing composition of the data.

We are soliciting comments in this proposed rulemaking on whether we should require developers of certified health IT with Health IT Modules certified to proposed § 170.315(b)(11) to make all source attributes information in the proposed § 170.315(b)(11)(vi) publicly available or accessible, for example, on a website, similar to the existing API documentation requirement in § 170.315(g)(10)(viii)(B). We are considering whether the public availability of this information is necessary to effectively improve the emerging market for predictive DSIs, or is necessary to ensure public confidence in predictive DSIs by enabling research use of source attribute information. For example, without this information, certified health IT purchasers (e.g., health care providers) may find it hard to effectively understand and determine whether models they are considering are FAVES or to anticipate the issues they may face when using the predictive DSI. This lack of transparency also could limit incentives for developers of certified health IT to improve their products and can potentially lead to practices that interfere with the flow of health information and the use of predictive DSIs to improve care. Accordingly, we solicit comment on whether we should require health IT developers of certified health IT with Health IT Modules certified to proposed § 170.315(b)(11) to make source attribute information available for the general public. We solicit comment on whether having this information publicly available would be beneficial for potential users that purchase models or associated technology or software, and would help inform them prior to procurement of certified health IT and procurement of predictive DSIs integrated with certified health IT. We also solicit comment on whether having this information publicly available would improve public confidence in predictive DSIs by enabling research on source attribute information. We also welcome any

comments on whether there should be a requirement to provide machine readable or computable versions of this information. We believe that such a requirement could improve consistency and comparability of source attribute information across Health IT Modules certified to proposed § 170.315(b)(11), regardless of whether these source attributes are made publicly available or are only made directly available to a developer of certified health IT's customers.

We welcome comment on whether we should require a certain format or order in which these attributes must appear to users. We note that we are presenting these source attributes here in preamble and in proposed regulation text according to how a developer may encounter them as part of the software or product development life cycle. We are not aware of widely agreed upon best practices for the format in which these elements or source attributes information should be displayed. However, we are aware of industry efforts to standardize a format to display information about technology in the form of a "model card" or "nutritional label" for healthcare.[181] We solicit comment on the desirability and feasibility of requiring a standardized format to display and communicate source attributes information as a requirement of the Program. We also request comment on how to ensure that users are aware that this information is available for them to review and how users can readily and easily access information about these source attributes as part of their overall workflow.

We solicit feedback on additional opportunities to help bring algorithmic transparency and improved trustworthiness in health IT design, development, and implementation as well as user needs for the procurement, implementation, and use of such technology. We are aware of a growing trend in industry and academia aiming to identify and address various algorithmic biases through audits.[182] Audits are often described as being performed by independent (or even

---

[181] See, e.g., Stat News, Health-related artificial intelligence needs rigorous evaluation and guardrails, (March 2022), https://www.statnews.com/2022/03/17/health-related-ai-needs-rigorous-evaluation-and-guardrails/?utm_source=STAT+Newsletters&utm_campaign=ac551f3b51-health_tech_COPY_01&utm_medium=email&utm_term=0_8cab1d7961-ac551f3b51-153157394.

[182] See James Guszcza, et al. *Why We Need to Audit Algorithms. Harvard Business Review*. (Nov. 28, 2018). https://hbr.org/2018/11/why-we-need-to-audit-algorithms; Xiaoxuan Liu, et al., *The medical algorithmic audit*, THE LANCET DIGITAL HEALTH (2022). See generally Outsider Oversight: Designing a Third Party Audit Ecosystem for

adversarial) third parties, certified practitioners, and by a normalized set of rules.[183] We support facilitating continuous monitoring over time, sometimes referred to as "algorithmovigilance," and an overall life cycle approach to analyzing and monitoring algorithm-driven healthcare for effectiveness and equity.[184] We believe the proposed source attribute requirements in § 170.315(b)(11)(vi) would provide much-needed information to aid algorithmic audits and algorithmovigilance. We also solicit comment on testing or assessment tools that might further support transparency and trustworthiness including: consensus metrics and technical standards for evaluating fairness (assessing for bias) and validating performance (including testing performance in different populations and evaluating applicability or generalizability) of predictive models that are enabled by or interface with Health IT Module(s) prior to and during deployment; development and engineering of algorithmic impact assessments (AIAs); development of documentation of datasets used, such as datasheets for datasets and data cards as well as tools that could be useful in these areas so that Health IT Modules certified to § 170.315(b)(11) can demonstrate it meets a given requirement on an ongoing basis.

We understand that any data used by developers of certified health IT and other parties in the development of DSIs should be used in ways that balance data use interests with patients' interests. For example, model developers should use data for training and testing consistent with applicable law, patients' expectations, and any patient consent or preference given. We invite the public to read section III.C.5.c.xi of this proposed rule for the discussion about data collection and use. We are aware that digital and algorithmic literacy is important, including to help detect and mitigate bias. In turn, potential subjects (patients) of automated decisions could benefit from information about how these technologies function and are used in healthcare.

AI Governance ID Raji, P Xu, C Honigsberg, D Ho - Proceedings of the 2022 AAAI/ACM Conference on AI …, 2022, https://dl.acm.org/doi/pdf/10.1145/3514094.3534181.

[183] See, e.g., International Organization for Standardization. Guidelines for auditing management systems. https://www.iso.org/obp/ui/#iso:std:iso:19011:ed-3:v1:en.

[184] See Embi, Peter, Algorithmovigilance—Advancing Methods to Analyze and Monitor Artificial Intelligence–Driven Health Care for Effectiveness and Equity, (April 2021), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2778569.

Patients want to know if AI is being used in their care, and understand how and why it is being used in their care.[185] We understand an emerging trend is for health care providers to inform patients about the use of these technologies, including predictive DSIs, in making decisions about their care.[186] We support patients being informed about technologies that directly affect individuals or their health information and understand transparency can increase public trust and confidence in technology. In turn, we solicit comment on whether existing Program requirements in the Communications condition and maintenance of certification requirements in § 170.403 are sufficient to ensure open and transparent discussion regarding the use of predictive DSIs in patient care – including discussion between users of certified health IT and patients. We are especially interested in whether we should require developers of certified health IT to provide the technical capability for users to support patients electronically accessing underlying source attribute information (e.g., through a patient portal) for predictive DSIs or otherwise indicate to a patient when a predictive DSI was used to make decisions about the patient in the course of the patient's care. We also are interested in learning more about how to incorporate the patient perspective and overall engagement meaningfully and sustainably. Specifically, we are interested in comments on how to improve the public's awareness of their ability to obtain information about any use of predictive DSI—or other emerging technologies—in their healthcare and summary information about IRM practices associated with such use through the HIPAA Privacy Rule individual's right of access.[187] Similar to when a patient wants to obtain access to more than just test results from a clinical laboratory that is a covered entity (health plans, health care clearinghouses, or health care providers that conduct standard electronic transactions),[188] if a patient requests access to their information held by a health care provider, the designated record set (DRS) could include, for example, the underlying data used to generate recommendations

---

[185] See, e.g., https://www.radiologybusiness.com/topics/healthcare-management/business-intelligence/consumers-anticipate-better-healthcare-through.
[186] See, e.g., AHRQ-funded patient-centered CDS Innovation Collaborative (CDSiC), https://cds.ahrq.gov/cdsic.
[187] 45 CFR 164.524.
[188] See definition of "covered entity" at 45 CFR 160.103.

about their healthcare, underlying information about any use of predictive DSI generated as part of the healthcare decision, and other information (e.g., summary information about intervention risk management practices) associated with such use of a predictive DSI.[189]

ix. Proposed § 170.315(b)(11)(vi)(D) Missing Source Attribute Information

We believe that source attributes proposed in § 170.315(b)(11)(vi)(A), (B), and (C) are foundational for users' understanding of the DSI regardless of whether the intervention developer is a developer of certified health IT, a customer of the developer of certified health IT, an academic health system, integrated delivery network, a third-party software developer, or other party. This belief underpins our proposed requirements in § 170.315(b)(11)(vi) that certified Health IT Modules enable a user to review a plain language description of all source attribute information in § 170.315(b)(11)(vi)(A) through (C) via direct display, drill down, or link out. However, as discussed previously, we understand there may be circumstances where a developer of certified health IT may not have information pertaining to a source attribute for a Health IT Module to enable such user review. We, therefore, propose in § 170.315(b)(11)(vi)(D) that a certified Health IT Module must clearly indicate when a source attribute listed in § 170.315(b)(11)(vi)(A), (B), and (C), as applicable, is not available for the user to review, including two specific circumstances. First, we propose in § 170.315(b)(11)(vi)(D)(*1*) that for source attributes in § 170.315(b)(11)(vi) that include the "if available" phrase, a Health IT Module must clearly indicate when such source attribute is not available for review. Second, we propose in § 170.315(b)(11)(vi)(D)(*2*) that when a Health IT Module enables or interfaces with a DSI developed by other parties that are not developers of certified health IT, that Health IT Module must clearly indicate when any source attribute listed in § 170.315(b)(11)(vi)(A), (B), or (C), as applicable, is not available for the user to review. This means that a certified Health IT

[189] See, e.g., OCR's HIPAA FAQs 2048 and 2049, https://www.hhs.gov/hipaa/for-professionals/faq/2048/does-an-individual-have-a-right-under-hipaa/index.html; https://www.hhs.gov/hipaa/for-professionals/faq/2049/does-an-individual-have-a-right-under/index.html.

Module that enables or interfaces with a DSI developed by other parties that are not developers of certified health IT must clearly indicate when any attribute listed in § 170.315(b)(11)(vi)(A), (B), or (C) is not available for the user to review, regardless of whether the DSI is a predictive DSI, as defined at § 170.102, an evidence-based DSI, as described at § 170.315(b)(11)(iii), or a linked referential DSI, as described at § 170.315(b)(11)(iv).

We clarify that "other parties," in § 170.315(b)(11)(vi)(D)(*2*) includes any party that develops a DSI, a model, or an algorithm that is used by a DSI and is not a developer of certified health IT. These can include, but are not limited to: a customer of the developer of certified health IT, such as an individual health care provider, provider group, hospital, health system, academic medical center, or integrated delivery network; a third-party software developer, such as those that publish or sell medical content or literature used by a DSI; or researchers and data scientists, such as those who develop a model or algorithm that is used by a DSI.

We reiterate that while we do not prescribe how a certified Health IT Module must indicate that an attribute is missing, we clarify that the certified Health IT Module must communicate an attribute is missing unambiguously and in a conspicuous manner to a user. We note that these "other parties" may or may not have a contractual relationship with the developer of certified health IT. However, we seek comment on whether we should require developers of certified health IT with Health IT Modules that enable or interface with predictive DSIs to display source attributes for other parties with which the developer of certified health IT has a contractual relationship.[190]

When predictive DSIs are developed by other parties, rather than the developer of the certified Health IT Module, we recognize that it may not be feasible for developers of certified health IT to have access to or possess information about each source attribute required in § 170.315(b)(11)(vi)(C), available for user review. Therefore, we propose to allow developers of

[190] See the definition of "business associate" at 45 CFR 160.103.

certified health IT with Health IT Modules that enable or interface with predictive DSIs that are developed by other parties to clearly indicate when any source attribute information is not available for user review. Consistent with prior discussion regarding third-party developed evidence-based DSIs (77 FR 54215), we anticipate that developers of certified health IT would obtain information on the predictive DSI from the model developers, owners, or creators in most instances. This is consistent with what we have historically expected, noting in the 2014 Edition Proposed Rule that it would be the third party from which the developer of certified health IT would get this information (77 FR 54215). We also noted in the 2014 Edition Proposed Rule that "The absence of [bibliographic] information is . . . valuable information and may (or may not) cause the [user] to heed or ignore the guidance. Note that our goal here is not to assess the quality or evidence basis of decision support, but to enable the [user] to do so." We also stated, "In cases where [funding source] information is unknown, then the [user] should have access to the fact that this information is unknown" (77 FR 54215).

We believe that indicating the absence of information on source attributes would provide an important signal to users that the model may not have been rigorously developed and evaluated. This signal would provide motivation to developers to perform the tasks necessary to generate information relevant to each source attribute and to provide that information to health IT developers of certified health IT or their customers for incorporation into the source attributes information about the model to be made available for user review as discussed earlier in the section and proposed in § 170.315(b)(11)(vi). We invite comment on these proposals.

We are aware of some standards related to DSIs, such as CDS Hooks v1.0, that could invoke decision support from within a clinician's workflow, and that include a source attribute field designed to include URLs to relevant supporting documentation.[191] We are also aware that the emerging Evidence-Based Medicine on FHIR project includes a more detailed resource

[191] See https://cds-hooks.hl7.org/.

structure for the presentation of source information related to a recommendation.[192] We request comment on whether those or related standards could support provision of information on source attributes for DSIs, including predictive DSIs, to meet the proposed requirement in § 170.315(b)(11)(vi) for source attributes information to be available for user review, either in the form of "drill-down" links, link out, or through direct display within the certified Health IT Module.

x. Proposed § 170.315(b)(11)(vi)(E) Authoring and Revising Source Attributes

We propose in § 170.315(b)(11)(vi)(E) that Health IT Modules certified to § 170.315(b)(11) support the ability for a limited set of identified users to author (i.e., create) and revise source attributes and information provided for user review beyond what is proposed in § 170.315(b)(11)(vi)(A) and (C). This proposed requirement would pertain to source attributes related to both evidence-based DSIs and predictive DSIs that are enabled by or interfaced with a certified Health IT Module, including any predictive DSIs that are developed by users of the certified Health IT Module. This means, for example, a hospital that develops its own predictive DSI that is interfaced with a certified Health IT Module would be able to create new or revise existing source attributes information related to that predictive DSI that is made available through the certified Health IT Module without the developer of certified health IT's direct involvement. This would also mean that, following a local evaluation of a predictive DSI created by a developer of certified health IT, a health organization would have the ability to add a new attribute (for instance) named "local reliability" for display within the certified Health IT Module and include information on this additional attribute of the organization's predictive DSI or model and that this information would be made available through and within the certified Health IT Module for display to users. While we are not proposing to require a developer of certified health IT to be directly involved in the authoring or revision of source attribute information provided

[192] https://confluence.hl7.org/display/CDS/EBMonFHIR.

for user review, we are proposing that the certified Health IT Module would need to support the technical ability for a limited set of identified users to create new or revised attribute information alongside other source attribute information proposed in § 170.315(b)(11)(vi)(A) and (C). As described in the examples above, we envision that innovative source attributes, reflective of local circumstances, could be authored by users without direct development support from the developer of certified health IT. Like all source attributes we proposed in § 170.315(b)(11)(vi), these authored source attributes should be available "via direct display, drill down, or link out from a certified Health IT Module."

As previously noted, multiple reporting guidelines exist for predictive models and there is no single list of agreed upon attributes for model transparency.[193] We believe the proposed source attributes information in § 170.315(b)(11)(vi)(C) would represent a useful floor, baseline, or minimum level of information to enable consistent transparency of predictive DSIs. We similarly believe that the proposed source attributes in § 170.315(b)(11)(vi)(A) represent a useful floor, baseline, or minimum level of information to enable transparency for evidence-based DSIs. However, we are aware of trends towards shareable and interoperable decision support that may result in a need for local customization of the source attributes describing the DSI or require additional information on a local instantiation of a DSI.[194] We believe health systems, health care providers, and other users of DSIs should have the capability to customize and expand the source attributes displayed for a DSI to meet their specific needs and at their discretion. Allowing for user revision would also ensure that the information available through source attributes can be updated in a timely manner and remain informative. We invite comment on this proposal.

Display of predictive DSI source attributes

---

[193] Sendak, et al., NPJ DIGITAL MEDICINE, (2020); Mitchell, et al. 2019; Hernandez-Boussard, et al., JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION, (2020); Norgeot, et al., NATURE MEDICINE, (2020); Gary S Collins, et al., *Transparent reporting of a multivariable prediction model for individual prognosis or diagnosis (TRIPOD): the TRIPOD statement*, 102 JOURNAL OF BRITISH SURGERY (2015).

[194] See, e.g., https://cds.ahrq.gov/cdsconnect.

In the previous sections, we propose that developers of certified health IT would make source attributes available for DSIs their Health IT Modules enable or interface with. We are aware that several technical architectures exist to provide outputs of predictive and evidence-based models to certified health IT or otherwise use these models as the back-end of DSIs that are subsequently delivered through a certified product.[195] These approaches could be used to deliver the output of models developed by customers of the developer of certified health IT health care providers to their own health IT—a common approach at academic medical centers and one that may be more widely used as the underlying technology becomes more ubiquitous. These approaches could also be used to deliver model output or a DSI developed by third-party developers, which we believe already occurs at a wide scale and anticipate would grow increasingly pervasive as the market for effective predictive decisions support interventions continues to grow.

We request comment on whether developers of certified health IT would be able to differentiate clearly between other-party DSIs that they implement into their Health IT Modules and make available to their customers versus those other-party products that their customers purchase, develop, or otherwise integrate without direct involvement of the developer of certified health IT.

xi. Proposed § 170.315(b)(11)(vii) Intervention Risk Management (IRM) requirements for Predictive Decision Support Interventions

We propose in § 170.315(b)(11)(vii) to establish "intervention risk management" requirements. We propose to require in § 170.315(b)(11)(vii) that by December 31, 2024, a developer of certified health IT that attests "yes" in § 170.315(b)(11)(v)(A) employs or engages

[195] Julian Gruendner, et al., *KETOS: Clinical decision support and machine learning as a service–A training and deployment platform based on Docker, OMOP-CDM, and FHIR Web Services*, 14 PLOS ONE (2019); Mohammed Khalilia, et al., Clinical predictive modeling development and deployment through FHIR web services § 2015 (American Medical Informatics Association 2015); *CDS Hooks*, https://cds-hooks.org/.

in the following IRM practices for all predictive decision support interventions, as defined in § 170.102, that the developer's certified Health IT Module enables or interfaces with:

- In § 170.315(b)(11)(vii)(A)(*1*) Risk Analysis, we propose that developers of certified health IT analyze potential risks and adverse impacts associated with a predictive decision support intervention for the following characteristics: validity, reliability, robustness, fairness, intelligibility, safety, security, and privacy;
- In § 170.315(b)(11)(vii)(A)(*2*) Risk Mitigation, we propose that developers of certified health IT implement practices to mitigate risks, identified in accordance with § 170.315(b)(11)(vii)(A)(*1*), associated with a predictive decision support intervention; and
- In § 170.315(b)(11)(vi)(A)(*3*) Governance, we propose that developers of certified health IT establish policies and implement controls for predictive decision support intervention governance, including how data are acquired, managed, and used in a predictive decision support intervention.

We propose in § 170.315(b)(11)(vii)(B) that developers of certified health IT compile detailed documentation of intervention risk management practices listed in § 170.315(b)(11)(vii)(A) and upon request from ONC make available such detailed documentation for any predictive DSI that their certified Health IT Module enables or interfaces with. We also propose in § 170.315(b)(11)(vii)(C) to require developers of certified health IT to submit summary information to their ONC-ACB regarding IRM practices listed in proposed § 170.315(b)(11)(vii)(A) via publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. Consistent with Program implementation for similar documentation requirements (84 FR 7484), we clarify that for this proposed summary information in § 170.315(b)(11)(vii)(C), the required documentation would need to be submitted to ONC-ACBs for review prior to issuing a certification.

Finally, we propose in § 170.315(b)(11)(vii)(D) to require that developers of certified health IT review annually and, as necessary, update both detailed documentation and summary

information. We propose in § 170.315(b)(11)(vii) to establish a deadline of December 31, 2024, for developers of certified health IT with Health IT Modules to which the proposed requirements in that section apply to engage in intervention risk management practices and develop both detailed documentation and summary information. This proposed deadline corresponds with our proposal in § 170.315(a)(9)(vi) and supports our proposal to update the Base EHR definition in § 170.102, as discussed in section III.C.5.c.xii.

Background on risk management and connection to other § 170.315(b)(11) proposals

Model development is not a straightforward or routine technical process. The experience and judgment of developers, as much as their technical knowledge, greatly influence the appropriate selection of inputs and processing components. The training and experience of developers exercising such judgment affects the extent of model risk. In addition, even with skilled modeling and robust validation, model risk cannot be eliminated, so other tools should be used to manage model risk effectively. Among these are establishing limits on model use, monitoring model performance, adjusting or revising models over time, and supplementing model results with other analysis and information.[196] IRM efforts should prioritize the minimization of potential negative impacts, and may need to include human intervention in cases where the predictive DSI cannot detect or correct errors.[197]

Overall, the proposals in § 170.315(b)(11)(vii)(A) are intended to promote the management of risks in pursuit of predictive DSI trustworthiness. Trustworthy predictive DSIs, models that are FAVES, mitigate risks and contribute to benefits for people, organizations, and systems. Trustworthy predictive DSIs should achieve a high degree of control over risk while retaining a high level of performance quality. Achieving this goal requires a comprehensive approach to intervention risk management. Risk management can drive developers and users to

[196] Bd. Governors Fed. Rsrv. Sys., Supervisory Guidance on Model Risk Management, SR 11-7 (Apr. 4, 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm.
[197] See NIST, AI RMF, January 2023, https://www.nist.gov/itl/ai-risk-management-framework.

understand and account for the inherent uncertainties and inaccuracies in their models and systems, which in turn can improve their overall performance and trustworthiness.[198]

We note that a central component of effective risk management lies in a clear acknowledgment that risk mitigation, rather than risk avoidance, is often the most effective factor in managing such risks.[199] We also note that risks to any software or information-based system also apply to predictive DSIs, including important concerns related to cybersecurity, privacy, safety, and infrastructure. Consequently, many activities related to managing risk for predictive DSIs are common to managing risk for other types of software development and deployment.[200] We believe that predictive DSI risk should be managed like other types of risk, continuously across the SDLC. For example, under the FDA's existing Quality System (QS) regulation, the FDA has current good manufacturing practice (CGMP) requirements for medical device manufacturers to integrate risk management activities throughout their QS and across the total product life cycle (TPLC).[201] Likewise, we believe it is critical for developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) that enable or interface with predictive DSIs to establish risk management strategies that address their own unique risks and circumstances. We encourage the use of a framework to help facilitate intervention risk management. For example, the intent and approach to govern, map, measure, and manage risks, defined in the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF), the draft AI RMF Playbook, and Special Publication 1270: "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence" can be applied when complying with proposed requirements in § 170.315(b)(11)(vii)(A).[202]

---

[198] *Id.*
[199] *Id.*
[200] See NIST, AI Risk Management Framework (AI RMF), January 2023, https://www.nist.gov/itl/ai-risk-management-framework.
[201] See 21 CFR part 820. See also, FDA Proposed Rule Medical Devices; Quality System Regulation Amendments, https://www.federalregister.gov/documents/2022/02/23/2022-03227/medical-devices-quality-system-regulation-amendments.
[202] See https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf; https://pages.nist.gov/AIRMF/; and https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

Given a lack of healthcare sector-specific guidance and the nascency of several emerging efforts for risk management of predictive software, our proposals in § 170.315(b)(11)(vii)(A) would not require a specific framework, guideline, or approach that such developers of certified health IT must use – only that they employ or engage in IRM practices in accordance with proposed requirements in § 170.315(b)(11)(vii)(A) through (D). In the proposals and related preamble, we have sought a balance between prescriptiveness and sufficient description to enable robust reporting of information on IRM practices. Within this preamble, we have described several items that we believe are best practices. We request comment on whether there are best practices or other items contained within the proposals in § 170.315(b)(11)(vii)(A) that should be explicitly required. We invite comment on the proposals in § 170.315(b)(11)(vii)(A) to require developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) and that attest "Yes" in accordance with our proposal in § 170.315(b)(11)(v)(A) to employ or engage in IRM practices for all predictive DSIs that their certified Health IT Modules enable or interface with, without being prescriptive as to how such practices must be carried out.

We view our proposals for risk management of predictive DSIs in § 170.315(b)(11)(vii) as complementary to our proposals for predictive DSI source attributes in § 170.315(b)(11)(vi)(C). The proposed source attributes information requirement is meant to provide users and implementers with sufficient information to understand how the model was designed, developed, and tested, including the model's purpose, known limitations, and intended use(s). Correspondingly, the proposals for intervention risk management would provide users, implementers, and the wider public, including patients, with information to understand how developers of certified health IT with Health IT Modules that enable or interface with predictive DSIs analyze, mitigate, and govern risks throughout the technology's life cycle. We anticipate that these actions would dramatically increase the likelihood that a predictive DSI, enabled by or interfaced with a certified Health IT Module, is FAVES by providing information transparency

regarding how risks to individuals, groups, communities, organizations, and society would be managed more effectively, consistent with best practices.[203]

Together, our proposals for predictive DSI-specific source attributes and IRM practices information are intended to help guide medical decisions at the time and place of care, consistent with 42 U.S.C. § 300jj–11(b)(4). Beyond the application of predictive DSI-specific source attributes and IRM practices information to an episode of care, for example, we believe such transparency would also foster confidence and trust among interested parties that the technical and organization processes used in designing and developing the predictive DSI were FAVES and high-quality. Finally, we anticipate these proposed requirements would help developers of certified health IT, themselves, know if a predictive DSI that their certified Health IT Module enables or interfaces with is FAVES, and then show to their customers and the wider public that they support high-quality predictive DSIs, thus improving user and public trust in the technology.

Proposals in § 170.315(b)(11)(vii)(A)

In § 170.315(b)(11)(vii)(A), we propose that developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) employ or engage in "risk analysis," "risk mitigation," and "governance," IRM practices for all predictive DSIs, as proposed to be defined in § 170.102, that the certified Health IT Module enables or interfaces with.

For purposes of proposed § 170.315(b)(11)(vii), we define "risk" as a measure of the extent to which an entity is negatively influenced by a potential circumstance or event. Typically, risk is a function of: (1) the negative impacts, or magnitude of harm, that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.[204] Entities can be individuals, groups, communities, and society. These risks sometimes are referred to as model harms.

---

[203] NIST, AI RMF, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[204] NIST, AI RMF, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

We believe that many such developers of certified health IT already employ or engage in IRM practices, thus, the proposed requirement to provide information on these practices in (b)(11)(vi)(B) and (C) represent a low-level of burden. However, we propose to make explicit our expectations that to provide the proposed information, such developers of certified health IT must "employ or engage" in IRM practices in § 170.315(b)(11)(vi)(A). We view the proposal in § 170.315(b)(11)(vii)(A) as similar to existing Program requirements in § 170.315(g)(3) safety-enhanced design (SED) and § 170.315(g)(4) Quality management systems (QMS), and we propose the requirements in § 170.315(b)(11)(vii) for similar reasons that we adopted the SED and QMS criteria (77 FR 13843). First, all developers of certified health IT that seek certification to § 170.315(b)(11) and have certified Health IT Modules that enable or interface with predictive DSIs would become familiar with foundational IRM practices if not already familiar; second, the public disclosure of the summary information of IRM practices employed or engaged by the developer of certified health IT, as described further below, would provide transparency to purchasers (potential users), users, and other interested parties, and contribute to appropriate information to help guide medical decisions; and lastly, our proposals in § 170.315(b)(11)(vii)(A) would encourage development of healthcare-specific, consensus and industry-based best practices for risk management.

Proposals in § 170.315(b)(11)(vii)(A)(1) – Risk Analysis

In § 170.315(b)(11)(vii)(A)(*1*), we propose to require developers of certified health IT to analyze potential risks and adverse impacts associated with a predictive DSI that their certified Health IT Modules enable or interface with. NIST's AI RMF describes seven characteristics of trustworthy AI, and in § 170.315(b)(11)(vii)(A)(*1*) we propose to adapt these concepts and require that developers of health IT with certified Health IT Modules that enable or interface with predictive DSIs employ or engage in risk management practices related to the following characteristics: (1) validity; (2) reliability; (3) robustness; (4) fairness; (5) intelligibility; (6) safety; (7) security; and (8) privacy.

We have adapted these emphasis areas, and we propose that such developers of certified health IT analyze risks related to the lack or failure of validity, reliability, robustness, fairness, intelligibility, safety, security, and privacy. Consistent with the NIST AI RMF, we encourage developers of certified health IT to include the following in their analysis: (1) estimates of the likelihood and magnitude of the negative impact (harm), or consequences, of each risk; (2) to whom each risk applies (including, for example, individual, group, and societal harm); and (3) the source of each risk. In addition to assessing and measuring the magnitude of the risk, we encourage developers of certified health IT to identify who is accountable for any negative impact potentially resulting from the outcome of the risk if it is realized.[205] We are aware that many risks are affected by the extent, quality, source, and representativeness of the data used in development of the predictive DSI as well as the management, storage, and governance of that data. We strongly encourage developers to consider how issues related to data practices may contribute to risks related to the eight, interrelated characteristics proposed in § 170.315(b)(11)(vii)(A)(*1*). See section III.C.5.c.xi of this proposed rule for the discussion about data collection and use in "Data Practices and Governance: Ethical, Legal, and Social Implications of Data Collection and Use" and data quality "Technical Data Standards and Data Management Source or Input Data and Data Collection or Capture" under "Request for Comment."

It is likely that some of the information used to identify risk would be substantially similar or identical to the information provided as source attributes proposed in § 170.315(b)(11)(vi). As examples, analysis of validity, fairness, and safety may be important processes in development of source attributes and risk analysis such that the two proposals are closely aligned. Developers of certified health IT should consider risk from individual predictive DSIs and in the aggregate. Aggregate risk is affected by interaction and dependencies among

[205] For a discussion about "accountability," see NIST, AI RMF, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

models; reliance on common assumptions, data, or methodologies; and any other factors that could adversely affect several DSIs and their outputs at the same time.[206] These risks must be assessed prospectively, in a timely manner to inform the summary information of IRM practices, as proposed in § 170.315(b)(11)(vii)(C).

Analyzing risk is a continual process that should begin in the initial concept and design phase of the predictive DSI and continue through its development, deployment and full period of use, as the technology should be responsive to new risks as they occur. Health IT developers may use model risk assessments to help determine the types, frequency, and extent of evaluation activities necessary to assess risk. Information on these evaluation activities may be useful in presenting proposed source attributes information describing the "process used to ensure fairness in development of the intervention" in § 170.315(b)(11)(vi)(C)(*2*)(*ii*), the "external validation process" in § 170.315(b)(11)(vi)(C)(*2*)(*iii*) (if available), and in particular the "update and continued validation or fairness assessment schedule" in § 170.315(b)(11)(vi)(C)(*4*)(*i*).

We do not propose or describe risk tolerance associated with the eight characteristics, as we believe these should be decisions made by those involved with the design, development, deployment, and use of the technology. We propose that developers of certified health IT must analyze the potential risks and adverse impacts, associated with a predictive DSI that their certified Health IT Modules enable or interface with, related to lack or failure in the following characteristics:

- "Validity," as discussed earlier in section III.C.5.b of this proposed rule in the proposal for source attributes in § 170.315(b)(11)(vi)(C), of models used as sources for predictive DSIs can be assessed using technical characteristics. "Validity" for deployed predictive DSIs is often assessed with ongoing testing or monitoring that confirms a system is performing as intended (similar to the description of the source attributes related to "Ongoing Maintenance of Intervention Implementation and Use," in section III.C.5.b of

[206] See https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm.

this proposed rule).[207] Accuracy and robustness are interdependent factors contributing to the validity and trustworthiness of AI systems. Deployment of AI systems which are inaccurate, unreliable, or non-generalizable to data beyond their training data (i.e., not robust) creates and increases AI risks and reduces trustworthiness.[208] Assessment of risk related to validity should include and consider the following areas:

- Validation of the accuracy and completeness of data used in development and testing of the predictive DSI;[209]
- Evaluation plans and results for validation in testing environments and ongoing evaluation in deployment;[210]
- Both technical validity and clinical validity, which is closely related to measurement of effectiveness such as those discussed in the proposed source attribute "References to evaluation of use of the model on outcomes" in § 170.315(b)(11)(vi)(C)(*3*)(*v*).[211]

- "Reliability" indicates whether a model used in a predictive DSI consistently performs as required, without failure, for a given time interval, under given conditions.[212] Techniques designed to mitigate overfitting (e.g., regularization) and to adequately conduct model selection in the face of the bias-variance tradeoff can increase model reliability. Assessment of reliability should include defining what range of behaviors is considered

---

[207] For discussion of the definition of the terms or characteristics, see NIST, AI RMF, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[208] *Id.*
[209] *See, e.g.*, ANSI/CTA-2090 The Use of Artificial Intelligence in Health Care: Trustworthiness.
[210] *See, e.g.,* Microsoft Responsible AI Standard, v2: General Requirements (June 2022), https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf; Google Responsible AI with TensorFlow (June 2020), https://blog.tensorflow.org/2020/06/responsible-ai-with-tensorflow.html.
[211] As described in the FDA's *Software as a Medical Device (SAMD): Clinical Evaluation.* Issued on December 8, 2017, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/software-medical-device-samd-clinical-evaluation.
[212] See NIST, AI RMF, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

reliable for a model, the error rate considered acceptable, and the results of evaluations that demonstrate reliability in both testing and deployed environments.[213]

- "Robustness" or generalizability is the ability of a model used in a predictive DSI to maintain its level of performance under a variety of circumstances.[214] Robustness not only means that the model performs exactly as it does under expected uses, but also that it performs in ways that minimize potential harms to people if it is operating in an unexpected setting or environment. Measurement of validity, accuracy, robustness, and reliability contribute to trustworthiness, and developers of certified health IT should consider that certain types of failures can cause greater harm – and risks should be managed to minimize the negative impact of those failures.[215] Assessment of robustness should evaluate limitations of the model based on the source of the training and testing data used and how features of that data and its source might relate to performance outside of the training and testing environment, which are likely to relate to information discussed in the proposed source attribute "input features of the intervention including description of training and test data" in § 170.315(b)(11)(vi)(C)(*2*)(*i*) discussed earlier in this preamble. In analyzing robustness, developers of certified health IT should also include the variety of sources, settings, or environments in which the model has been tested and its performance in those environments.
- "Fairness," as noted above in this section, is defined by a lack of bias against certain groups, and fairness enhancing (or bias managing) processes seek to ensure that models are fair. This includes addressing concerns for equality and equity by addressing issues such as bias and unlawful discrimination. NIST has identified three major categories of AI bias that should be addressed and managed to enhance fairness of models: systemic,

---

[213] *See, e.g.*, Microsoft Responsible AI Standard, v2: General Requirements (June 2022), https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf.
[214]. See NIST, AI RMF, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf (Source ISO/IEC TS 5723:2022).
[215] *Id.*

computational and statistical, and human-cognitive. In the analysis of potential risks, an approach should consider all three categories of bias and report results of evaluations of those categories in both testing and deployed environments.[216] It is likely that some of the information used to identify risk associated with fairness would be substantially similar or identical to the information provided as source attributes related to fairness proposed in § 170.315(b)(11)(vi)(vii)(C).

- "Intelligibility" refers to the extent to which the predictive DSI can be understood, often through a representation of the mechanisms underlying an algorithm's operation and through the meaning of AI systems' output in the context of its designed functional purpose. Generally, perceptions of risk related to intelligibility stem from concerns that unintelligible models, which produce output that is difficult to make sense of or contextualize, may lead to inappropriate interpretation or use of the decision support. Risks from ambiguity on the mechanisms underlying operation can be managed by clear descriptions of how models work. Risks from an ambiguity in output in the context of functional purpose can often be addressed by communicating a description of why the predictive DSI or other systems made a particular prediction or recommendation.[217] In assessing intelligibility, developers of certified health IT should delineate the expected and acceptable context of use, including the intended users and operational setting. Developers should assess whether the predictive DSI provides intelligible information as an output that will allow for its intended users to make effective interpretation of relevant predictive DSI behavior when applied or used in the expected operational setting.[218]
- "Safety" as a concept is highly correlated with risk and generally denotes that the product is free from any unacceptable risks and the probable benefits outweigh any probable

[216] See NIST, AI RMF, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[217] See NIST, AI AI RMF, January 2023, https://www.nist.gov/itl/ai-risk-management-framework.
[218] GAO-21-519SP: *AI Accountability Framework for Federal Agencies & Other Entities*, https://www.gao.gov/assets/gao-21-519sp.pdf.

risk.[219] Safety-related risks may overlap with privacy, security, and fairness. Predictive DSIs and the models used in predictive DSIs should not, under defined conditions, cause physical or psychological injury or lead to a state in which human life, health, property, or the environment is endangered.[220] Developers should assess who could be injured, when injury could arise and how injury could arise, engaging external parties in this assessment when such risks are not obvious. Because assessment is a continuous process, developers should also implement procedures for regularly evaluating safety.

- "Security" (and relatedly resilience) is a predictive DSI's and model's ability to withstand adversarial attacks, or more generally, unexpected changes in its environment or use, including not only those related to the provenance of the data, but also, encompassing unexpected or adversarial use of the model or data. In assessing security, developers should consider common IT security concerns related to the exfiltration of models, training data, or other intellectual property through the technology's endpoints as well as any potential weaknesses in the controls for the access, transmission, and storage of sensitive information.[221]
- "Privacy" refers generally to the norms and practices that help to safeguard human autonomy, identity, and dignity,[222] as well as data autonomy and intrusions on information about an individual.[223] Privacy-related risks may overlap with safety, security, and fairness. Analysis of privacy should consider the NIST Privacy Framework and application of NIST Privacy Risk Assessment Tools.[224] Privacy values such as anonymity, confidentiality, and control generally should guide choices for AI or ML-

---

[219] Cf. ISO 14971, which considers safety to be "free from unacceptable risks." If the product is a device as defined in section 201(h) of the FD&C Act, there may be different or additional requirements that apply.
[220] See *supra* note, 218.
[221] *Id.*
[222] *Id.*
[223] See The HIPAA Privacy Rule, 65 Fed. Reg. 82461, 82464 (Dec. 28, 2000) (noting that "privacy is a fundamental right," and "many people believe that individuals should have some right to control personal and sensitive information about themselves," including health information).
[224] See https://www.nist.gov/privacy-framework; https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/focus-areas/risk-assessment/tools.

enabled technology design, development, and deployment.[225] Like safety and security, specific technical features of AI or ML-enabled technologies may promote or reduce privacy, and assessors can identify how the processing of data could create privacy-related problems.[226] We invite readers to review section III.C.5.c.xi of this proposed rule for the discussion about ethical, legal, and social implications of data collection and use in "Data Practices and Governance: Ethical, Legal, and Social Implications of Data Collection and Use."

Consistent with our proposed requirement in § 170.315(b)(11)(vii), summary information of the risk analysis IRM practices, as proposed in § 170.315(b)(11)(vii)(C), must be made available by December 31, 2024.

We seek comments on these proposals and on related tools and frameworks to support this area in healthcare, including those tools that help identify observable indicators of risks.

Proposals in § 170.315(b)(11)(vii)(A)(2) – Risk Mitigation

We propose in § 170.315(b)(11)(vii)(A)(*2*) "Risk Mitigation" to require implementation of practices to mitigate risks associated with predictive DSIs, as proposed in § 170.315(b)(11)(vii)(A)(*1*). Risk mitigation practices should seek to address adverse impacts or minimize anticipated negative impacts of predictive DSIs on patients and populations. Model risk mitigation should include disciplined and knowledgeable development and implementation practices that are consistent with the real world context of the model's use, intended specific application of the model, and goals of the model user.[227]

Risk mitigation practices implemented by developers of certified health IT should cover the following:

- *Practices to prioritize (establish different levels of) risks based on their impact and likelihood*. Developers should prioritize risks based on the magnitude of negative impact,

[225] See NIST, AI RMF, January 2023, https://www.nist.gov/itl/ai-risk-management-framework.
[226] *Id.*
[227] *Id.*

the likelihood of risk, and the categorization of the predictive DSI.[228] We encourage developers to consider these dimensions of risks as they apply to their users or customers, patients, and other individuals served by customers who the predictive DSI may be applied to, as well as consideration of how risks could impact multiple parties. Prioritization of risk should guide the implementation of mitigation practices.

- *Practices to mitigate or minimize identified potential risks*. Numerous approaches exist to minimize predictive DSIs risks.[229] We encourage developers to consider selection of an alternative label or output for the predictive model, to evaluate how information is presented to users through the predictive DSI, or to add additional context to the display of the predictive DSI. We are aware that many risks are impacted by the extent, quality, source, and representativeness of the data used to develop predictive DSIs, as well as data management, governance, and storage practices. We encourage developers to closely evaluate the adequacy of the data used to develop a predictive DSI and consider selection of alternative or additional data. We further encourage developers to monitor and mitigate any privacy or security risk introduced by acquisition and curation of data for use by a predictive DSI, the storage and management of that data, the data's use in developing the predictive DSI, and the application of the predictive DSI to individuals in a deployed setting. Human factors such as participatory design techniques and multi-

[228] For example, according to existing taxonomy, the role of the CDS, and the situation, such as IMDRF | Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations: https://www.imdrf.org/documents/software-medical-device-possible-framework-risk-categorization-and-corresponding-considerations.

[229] For example, practices described in NIST AI RMF 1.0, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf; Off. Comptroller Currency, Comptroller's Handbook: Model Risk Management (Aug. 2021), https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management /index-model-risk-management.html; See generally The Association of Food and Drug Officials (AFDO)/Regulatory Affairs Professionals Society (RAPS) Healthcare Products Collaborative, *Bias in Artificial Intelligence in Healthcare Deliverables,* White Paper (2022), https://www.healthcareproducts.org/wp-content/uploads/2023/02/Final-Bias-in-Artificial-Intelligence-11.27.22.pdf.

stakeholder approaches, and a human-in-the-loop are also important for mitigating risks related to AI bias.[230]

- *Change control plans, including schedule of validation and updating processes*. We encourage developers to create plans for monitoring the performance, fairness, calibration, and other aspects of predictive DSIs and associated models. Developers should include anticipated modifications related to retraining models, recalibrating models, updating models, and associated methodology.[231] The plan should also include information on how those changes will be implemented in a controlled manner that manages risks to patients.
- *Processes to supersede, disengage, or deactivate an existing predictive decision support intervention that demonstrate performance or outcomes that are inconsistent with their intended use.* We encourage developers to consider how variation in performance across customer sites is monitored and addressed and to implement processes by which performance inconsistent with intended use is defined and measured. Developers should implement practices to notify customers in a timely manner to disengage or otherwise alter use of predictive DSIs.
- *Approaches to including subject matter experts in measuring and validating whether the system is performing consistently with their intended use and as expected in the specific deployment setting*. We encourage developers to include diverse participants with diverse expertise relevant to a predictive DSI in risk mitigation processes. To maximize value from these participants, developers should consider not only who to include but how to include diverse voices in the development process.

---

[230] For more information about Human Factors and AI risks such as bias, see Section 3.3 of NIST Special Publication 1270, "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence", https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf and See NIST AI RMF 1.0, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[231] See, e.g., FDA, Proposed Regulatory Framework for Modifications to AI/ML-based Software as a Medical Device (SaMD), Discussion Paper and Request for Feedback, https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf.

We seek comments on these proposals.

Proposals in § 170.315(b)(11)(vii)(A)(3) - Governance

We propose in § 170.315(b)(11)(vii)(A)(*3*) "Governance" to require that health IT developers of certified health IT establish policies and implement controls for predictive DSIs. We propose that a health IT developer of a certified Health IT Module that enables or interfaces with a predictive DSI must establish policies and implement controls for how data are acquired, managed, and used for said predictive DSI. We note that the term "establish" is intended to describe the process of analysis, identification, and application of appropriate processes and protocols related to data governance for the use of DSI. "Establish" does not mean that health IT developers are unable to leverage or apply policies designed or developed by other organizations, such as guidance established by federal agencies or consensus-based standards organizations, in order to comply with § § 170.315(b)(11)(vii)(A)(*3*). Governance should encompass models, software and data developed or provided by other parties as well as internally developed interventions.[232]

We believe that governance sets an effective framework for risk management, with defined roles and responsibilities for clear communication of a predictive DSI's limitations and assumptions.[233] Effective governance should inform each phase of the technology development process.[234] Governance cultivates and implements a culture of risk management within organizations developing, acquiring, or implementing interventions. Clear documentation of policies and controls is an essential component of governance, which can help to systematically implement policies and controls and standardize how an organization's risk management practices are implemented and recorded at each step in the software development life cycle.[235] A strong governance framework provides explicit support and structure to risk management

---

[232] See NIST AI RMF 1.0, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[233] See Bd. Governors Fed. Rsrv. Sys., Supervisory Guidance on Model Risk Management, SR 11-7 (Apr. 4, 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm.
[234] See NIST Special Publication 1270, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.
[235] *Id.*

practices through policies defining relevant risk management activities, controls, or procedures that implement those policies.

Our use of the term "policies" means statements of management intent regarding the objectives and required components of intervention risk management. Our use of the term "controls" means a system of internal controls that the developer has in place to implement the associated risk management policies, including those at the organizational and technology level (e.g., processes for controlling the quality of the data inputs; internal and external audits; process to escalate conflicting views between the model development and validation groups). In model risk management, this sometimes is referred to as the "lines of defense."[236]

Developers of certified health IT would have the flexibility to choose an approach to meeting this proposed requirement that addresses their own unique circumstances for their predictive DSIs. However, we encourage developers to implement policies and controls to evaluate whether risk analysis and risk mitigation practices are being carried out as specified; to consider how policies and controls are monitored and updated; and to plan a schedule for updating those policies and controls. Policies and controls should include details on roles, responsibilities, staff expertise, authority, reporting lines, and continuity. We further encourage developers to have accountability and escalation policies and controls related to how management oversees the development, deployment, and management of predictive DSIs. These policies should describe the developer of certified health IT's decision-making parameters and include how management is held accountable for the impact of predictive DSIs.[237] We encourage developers to identify staff that are responsible for predictive DSIs and related models and to develop policies to hold those staff accountable to the developer's established policies and procedures.[238] We believe that developers should plan escalation processes that permit

---

[236] Off. Comptroller Currency, Comptroller's Handbook: Model Risk Management (Aug. 2021), https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management /index-model-risk-management.html.
[237] *Id.*
[238] *Id.*

significant issues with predictive DSI development, integration or use to reach appropriate levels of management and describe standards for timely resolution of issues with predictive DSIs and related models.[239] If the developer uses a third-party to assess risk, the developer should describe processes for determining whether assessments performed by a third party meet the standards and controls set forth in the developer's governance framework.

We propose to require that the governance policies and controls developers of certified health IT implement relate to how they acquire, manage, and use data in predictive DSIs.[240] This includes setting and enforcing priorities for managing and using data as a strategic asset, which is a concept that identifies key activities of data governance as data identification, data management policy, data issues management, data assessment, data oversight, and data communications.[241] We expect developers of health IT to consider how the policies and controls they implement for data governance ensure the responsible acquisition, management, and use of data, including how the developer of certified health IT factors in and addresses ethical, legal, and social implications (ELSI) underlying data collection (acquisition) and use,[242] including any frameworks for data practices to address consumer protection and data stewardship concerns that are beyond traditional privacy and confidentiality practices.[243] As part of how a developer of

---

[239] *Id.*

[240] See, e.g., OECD, *Recommendation of the Council on Health Data Governance*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433; General Accountability Office (GAO), AI: *An Accountability Framework for Federal Agencies and Other Entities* (June 2021), https://www.gao.gov/assets/gao-21-519sp.pdf; See generally GAO, *Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care*, (Nov. 2020), https://www.gao.gov/products/gao-21-7sp.

[241] See for example Federal Data Strategy, Data Governance Playbook, https://resources.data.gov/assets/documents/fds-data-governance-playbook.pdf.

[242] See, e.g., https://www.healthit.gov/sites/default/files/facas/HITPC_Health_Big_Data_Report_FINAL.pdf.

[243] See, e.g., The Department of Veterans Affairs (VA), including the Veterans Health Administration (VHA), and its partners are governed by the *Principle-Based Ethics Framework for Access to and Use of Veteran Data*. 87 FR 40451 (July 7, 2022) (to be codified at 38 CFR 0 (noting that the "data ethics framework is intended to be applied by all parties who oversee the access to, sharing of, or the use of veteran data, or how access or use veteran data themselves in the context of all other specific clinical, technical, fiscal, regulatory, professional, industry, and other standards"); VA, *Artificial Intelligence (AI) Strategy*, (July 2021), https://www.research.va.gov/naii/VA_AI%20Strategy_V2-508.pdf (providing a vision to improve outcomes and experiences for Veterans by developing trustworthy AI capabilities); *Principles of Artificial Intelligence Ethics for Intelligence Community*, https://www.intelligence.gov/principles-of-artificial-intelligence-ethics-for-the-intelligence-community; *AI Ethics Framework for the Intelligence Community*, Version 1.0, June 2020, https://www.intelligence.gov/artificial-intelligence-ethics-framework-for-the-intelligence-community (assisting with the Principles of AI Ethics for the Intelligence Community); See generally National Committee on Vital and Health

certified health IT establishes policies and implements controls for data governance, we suggest developing a model that establishes authority, management and decision-making parameters related to the acquisition, management, and use of data related to predictive DSIs. We invite readers to review section III.C.5.c.xi of this proposed rule for a discussion about "Data Practices and Governance: Ethical, Legal, and Social Implications of Data Collection and Use" and "Technical Data Standards and Data Management: Source or Input Data and Data Collection or Capture." We invite readers to also review section III.C.1.c for a discussion about other proposals aimed at helping to address priorities such as public health and health equity or disparities in health outcomes.

We strive to create systemic improvements in health and care through access, exchange, and use of data to have better health enabled by data. There are risks associated with data use across the predictive DSI life cycle. Our use of the terms "acquired," "managed," and "used" are intended to describe the stages of data governance. As data is acquired, there should be rigorous assessment of data quality and relevance, and appropriate documentation. Developers of certified health IT should be able to demonstrate that such data and information are suitable for the predictive DSI, and that they are consistent with the theory behind the approach and with the chosen methodology. As part of data management, the use of data proxies should be carefully identified, justified, and documented. If data and information are not representative of the developer's customer base or other characteristics, or if assumptions are made to adjust the data and information, these factors should be properly tracked and analyzed. This is particularly important for external data and information (from a vendor or outside party), especially as they relate to new products or activities.[244]

Statistics (NCVHS), *Health data stewardship: what, why, who, how An NCVHS primer*, https://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/090930lt.pdf; NCVHS, Toolkit for Communities Using Health Data, (May 2015), https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/Toolkit-for-Communities.pdf.

[244] See NIST AI 100-1, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

Developers of certified health IT have the flexibility to choose an approach to meeting this proposed requirement that addresses their own unique circumstances and risks for their predictive DSIs but may wish to examine industry data governance, data management, data stewardship, data ethics, or responsible use of data resources to determine if they are relevant and useful in their own implementation efforts.[245] We invite comments on this proposal, and we seek comment on whether this requirement should include more specificity. We are aware that there are instances in which predictive DSIs are developed by other parties, such that the proposed intervention risk management practices might reasonably be shared between those other parties and the developer of certified health IT or reside primarily with or be performed by those other parties. For instance, risk analysis related to the quality and representativeness of training data would likely be performed by the party that engaged in initially developing the predictive DSI or model used by the DSI.

In such circumstances, the proposed requirement for developers of certified health IT to employ or engage in intervention risk management practices in § 170.315(b)(11)(vii) includes determining whether or not the other party has engaged in risk management practices, such as through review of risk analysis, risk mitigation, and governance information from the other party. Consistent with previous discussions in this proposed rule regarding the availability of source attribute information for predictive DSIs developed by other parties, we expect those other parties to also provide the developer of certified health IT with relevant intervention risk management information so that such information may be available for both detailed and summary documentation in § 170.315(b)(11)(vii)(B) and § 170.315(b)(11)(vii)(C), respectively. We invite comments on this proposal and ways in which developers of certified health IT can best determine that intervention risk management practices have been conducted for all

[245] See e.g., Federal Data Strategy, Data Governance Playbook, https://resources.data.gov/assets/documents/fds-data-governance-playbook.pdf; Federal Data Strategy, Data Ethics Framework, https://resources.data.gov/assets/documents/fds-data-ethics-framework.pdf; *Health data stewardship: what, why, who, how An NCVHS primer*, https://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/090930lt.pdf. See also NIST AI RMF 1.0, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

predictive DSIs that their Health IT Module enables or interfaces with, including those predictive DSIs developed by other parties.

We believe requiring the proposed IRM practices in § 170.315(b)(11)(vii) are necessary to enhance the transparency of predictive DSIs, and thus improve their capacity to be evaluated and their utility to healthcare professionals and patients. We have sought a balance between limited prescriptiveness and sufficient detail to enable robust and broadly applicable reporting of information on risk management practices to users. We request comment on whether there are items contained within the proposals described above that we should explicitly require as elements of the overall IRM practices in these proposals. We invite comments on this proposal, and we seek comment on whether these proposed requirements should include more specificity, and what actions developers of certified health IT should take to mitigate potential discriminatory outcomes of predictive DSIs.

Proposals in § 170.315(b)(11)(vii)(B) – Compile detailed IRM practice documentation

In § 170.315(b)(11)(vii)(B), we propose that a health IT developer that attests "yes" in § 170.315(b)(11)(v)(A) must compile detailed documentation regarding IRM practices listed in § 170.315(b)(11)(vii)(A) and upon request from ONC make available such detailed documentation to ONC for any predictive decision support intervention, as defined in § 170.102, that the certified Health IT Module enables or interfaces with. We believe that a developer of certified health IT subject to this proposed requirement should be able to provide detailed documentation of their IRM practices, if ONC requests such information, without much effort because this information should be a byproduct of employing or engaging in IRM practices in § 170.315(b)(11)(vii)(A). While ONC has the authority to conduct Direct Review consistent with § 170.580(a)(2), for any known non-conformity or where it has a reasonable belief that a non-conformity exists, this proposal would enable ONC to have oversight of the requirements in § 170.315(b)(11)(vii)(A) without necessarily initiating Direct Review. Further, this proposal would enable ONC to gain insights on the IRM practices employed or engaged in by developers of

certified health IT with Health IT Modules that enable or interface with predictive DSIs to inform potential future policymaking.

We clarify that "detailed documentation" is documentation that is specific to an individual predictive DSI enabled by or interfaced with a developer of certified health IT's Health IT Module, and we clarify that this documentation should be sufficiently detailed so that we are able to review, minimally, the IRM practices enumerated in § 170.315(b)(11)(vii)(A)(*1*) through (*3*). In a scenario where a Health IT Module enables or interfaces with a predictive DSI developed by other parties, some or all of the detailed documentation on IRM practices may be provided to the developer of certified health IT by that other party. This would include other parties that the developer of certified health IT may or may not have a formal contract or directly engaged with.

As discussed below, our proposals in § 170.315(b)(vii)(C) describe what summary information we would require a health IT developer that attests "yes" in § 170.315(b)(11)(v)(A) must make publicly accessible. With respect to the detailed documentation regarding IRM practices that we propose to require be submitted to ONC upon request in § 170.315(b)(11)(vii)(B), we understand that health IT developers may have concerns regarding the disclosure of proprietary, trade secret, competitively sensitive, or other confidential information. ONC would implement appropriate safeguards to ensure, to the extent permitted by federal law, that any proprietary business information or trade secrets ONC may encounter by accessing the health IT developer's detailed documentation, other information, or technology, would be kept confidential by ONC or any third parties working on behalf of ONC in its performance of oversight responsibilities to determine compliance under the Program. However, a health IT developer would not be able to avoid providing ONC access to relevant, detailed documentation by asserting that such access would require it to disclose trade secrets or other proprietary or confidential information. Therefore, similar to our statements in the ONC Cures Act Proposed Rule (84 FR 7504), ONC Cures Act Final Rule (85 FR 25785), and the EOA Final

Rule (81 FR 72431), we recommend health IT developers clearly mark, as described in HHS Freedom of Information Act regulations at 45 CFR part 5, subparts C and D, any information they regard as trade secret or confidential prior to disclosing the information to ONC. We solicit comment on this proposal.

Further, we solicit comment on whether existing Program requirements as part of the Communications condition and maintenance of certification requirements in § 170.403 are sufficient to enable open and transparent discussion, including between developers of certified health IT and users (customers) regarding IRM practices related to predictive DSIs.

Proposals in § 170.315(b)(11)(vii)(C) and corresponding proposals for ONC-ACBs in § 170.523(f)(1)(xxi)

We propose in § 170.315(b)(11)(vii)(C) that a health IT developer that attests "yes" in § 170.315(b)(11)(v)(A) must submit summary information of the IRM practices listed in § 170.315(b)(11)(vii)(A)(*1*) through (*3*) to its ONC-ACB via publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. We also propose a new Principle of Proper Conduct for the ONC-ACBs in § 170.523(f)(1)(xxi) to require ONC-ACBs to report the proposed summary information in § 170.315(b)(11)(vii)(C), that they received from developers of certified health IT, on the Certified Health IT Product List (CHPL) for the applicable Health IT Modules. We believe this new Principle of Proper Conduct is consistent with existing public disclosure requirements (e.g., 45 CFR 170.523(f)(1)(xii) and § 170.523(f)(1)(xx)) under the Program and will help ensure accountability for the public availability of information in § 170.315(b)(11)(vii)(C).

We reiterate our proposal in § 170.315(b)(11)(vii) which would require that this summary information be made available to ONC-ACBs via publicly accessible hyperlink prior to the deadline of December 31, 2024, if finalized as proposed.

We believe that multiple interested parties, including clinicians, health systems, patients, academia, policymakers, the public, and the health IT industry would benefit from having

generalized information regarding how developers of certified health IT manage risk related to the predictive DSIs that are enabled by or interfaced with their certified Health IT Modules. Clinicians, patients, health systems, and the public could use this information to bolster their trust in the developers of certified health IT and those certified Health IT Modules that enable or interface with predictive DSIs.

"Summary information" should describe risk management practices, enumerated in § 170.315(b)(11)(vii)(A)(*1*) through (*3*), for the predictive DSIs with which a certified Health IT Module enables or interfaces within general terms.

We note that "summary information," is not specific to any single predictive DSI, like the availability of detailed documentation proposed in § 170.315(b)(11)(vii)(B). Rather, the information would pertain to the suite or portfolio of predictive DSIs enabled by or interfaced with the certified Health IT Module. We note that the summary information would likely encompass variation in risk management practices for different kinds of predictive DSIs. For instance, we expect that some risk management practices would be different for predictive DSIs developed by the developer of certified health IT; predictive DSIs developed by other parties with whom the developer of certified health IT has contracted or otherwise formally engaged with to provide predictive DSIs that are enabled by or interfaced with the Health IT Module; and for predictive DSIs developed or created by the developer of certified health IT's customers and interfaced with the Health IT Module, potentially without the developer of certified health IT's formal involvement. Summary information must encompass this variation, to the extent it is present.

We clarify that summary information should be easily understood by interested parties. By easily understandable, we mean the following. The information describes, in general terms, how the developer of certified health IT manages various kinds of risk related to predictive DSIs that their Health IT Module enables or interfaces with. In deciding on the level of detail to include in the summary information, developers of certified health IT should include plain

language descriptions of the developer's IRM practices that are sufficient for potential customers or users of the predictive DSIs to understand the goals of the health IT developer's risk management practices as proposed in § 170.315(b)(11)(vii)(A)(*1*) through (*3*). Developers of certified health IT would have the flexibility to choose an approach to meeting this proposed requirement that addresses the developer's own unique circumstances and risks for predictive DSIs, but such developers may wish to examine industry model or AI risk management frameworks or resources to determine if they are relevant and useful in their own implementation efforts.[246] In a scenario where a Health IT Module enables or interfaces with a predictive DSI developed by other parties, summary information on IRM practices should include any relevant information provided to the developer of certified health IT by that other party. We invite comment on this proposal.

Similar to our policy associated with the API-focused certification criteria in § 170.315(g)(10)(viii)(B), we propose that all IRM documentation in § 170.315(b)(11)(vii)(C) be available via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. For example, the developer of certified health IT may not impose any access requirements, including, without limitation, any form of registration, account creation, "click-through" agreements, or requirements to provide contact details or other information prior to accessing the documentation. We clarify that for the proposed IRM documentation in § 170.315(b)(11)(vii)(C), summary information would need to be submitted to the developer of certified health IT's ONC-ACB for review prior to issuing a certification. The availability of documentation as part of the certification process is also consistent with existing requirements for API documentation in § 170.315(g)(10)(viii)(B) (84 FR 7484).

---

[246] See, e.g., NIST, AI RMF, https://www.nist.gov/itl/ai-risk-management-framework; Microsoft Responsible AI Standard, v2: General Requirements, (June 2022), https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf; Off. Comptroller Currency, Comptroller's Handbook: Model Risk Management (Aug. 2021), https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management /index-model-risk-management.html.

To support submission of documentation, and consistent with other Principles of Proper Conduct in § 170.523(f)(1), we propose a new Principle of Proper Conduct for documentation in § 170.315(b)(11)(vii)(C). We propose in § 170.523(f)(1)(xxi) that ONC-ACBs report the information required in § 170.315(b)(11)(vii)(C) on the CHPL for the applicable certified Health IT Modules._We believe this new Principle of Proper Conduct will assist in promoting greater transparency for the Program and will strengthen ONC-ACB oversight regarding IRM documentation.

We invite comments on this proposal, and we seek comment on whether the requirement for summary information should include more specificity and detail.

Proposals in § 170.315(b)(11)(vii)(D) Annual Review

Finally, we propose in § 170.315(b)(11)(vi)(D) to require developers of certified health IT that attest "yes" in § 170.315(b)(11)(v)(A) to review annually and, as necessary, update the documentation described in § 170.315(b)(11)(vii)(B) and § 170.315(b)(11)(vii)(C). This provision would apply to both detailed documentation compiled as part of proposed § 170.315(b)(11)(vii)(B) and summary information submitted to ONC-ACBs via publicly accessible hyperlink as part of proposed § 170.315(b)(11)(vii)(C). As stated previously, we view the detailed documentation required in § 170.315(b)(11)(vii)(B) as being a by-product of the proposed requirement for the developer of certified health IT to engage or employ in IRM practices. Thus, we expect that developers of certified health IT subject to this proposed requirement would review documentation associated with their IRM practices annually and, as necessary, update their documentation. Further, we believe that developers of certified health IT that attest "yes" in § 170.315(b)(11)(v)(A) should consider risk as part of ongoing development cycles, and these risks should be assessed in a timely manner so that risk analysis documentation

is up to date. Similar to the HIPAA Security Rule,[247] which requires ongoing risk analysis,[248] we propose that developers of certified health IT with Health IT Modules that enable or interface with predictive DSIs review their IRM practices and update their documentation as necessary.

We believe an annual review establishes a minimum expectation for updating IRM documentation, and we believe it is good practice that predictive DSIs undergo a full validation process at some fixed interval, including updated documentation of all related activities. While we are not proposing more frequent reviews, those may be appropriate for developers of certified health IT that have Health IT Modules that enable or interface with numerous or complex predictive DSIs. We invite comment on this proposal.

Request for Comment

- Users of Certified Health IT and Predictive Decision Support Intervention Management

We are aware that, in addition to developers of certified health IT, users, such as healthcare organizations and clinicians, have responsibilities related to FAVES DSIs, including intervention or model risk management during implementation and use, as well as model validation. For example, we believe it is important that users maintain strong governance and controls to help manage model risk and how they will use outputs from interventions in decision-making, including monitoring any potential impacts of model use. Users of a predictive DSI are also best able to report on how the predictive DSI performs in real-world and local settings (which can differ from their performance during testing). We have observed emerging frameworks for the oversight of predictive DSIs.[249] We understand there are many different terms used when referring to, addressing, or describing the desire for responsible, ethical, transparent,

---

[247] 45 CFR part 160 and subparts A and C of part 164.
[248] 45 CFR. 164.306(e) and 164.316(b)(2)(iii); see also OCR Guidance on Risk Analysis, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (noting that "in order for an entity to update and document its security measures 'as needed,' which the HIPAA Security Rule requires, it should conduct continuous risk analysis to identity when updates are needed").
[249] Bedoya, Armando D., et al. "A framework for the oversight and local deployment of safe and high-quality prediction models." *Journal of the American Medical Informatics Association* (2022).

trustworthy, and accountable algorithms in healthcare, including those involving AI and ML (e.g., algorithm and AI assurance). For purposes of our proposals, we use terminology consistent with the Program structure.

We seek input on any information that the Department can use or action the Department should consider taking to ensure that implementation and use of FAVES DSIs are seen as a shared responsibility across developers of certified health IT and their customers. By shared responsibility, we mean that determination that a predictive DSI is FAVES requires an ongoing process beginning during initial model development and continuing through deployment, active use of the predictive DSI in practice and continued monitoring throughout that use.[250] As emphasized in this proposal, developers of predictive DSI are responsible for ensuring that their risk management practices and information about predictive DSI are available to their customers and presented in plain language to enable their customers to use that information. Customers of developers of certified health IT—for example, healthcare organizations and clinicians— in turn are likely to be essential to the overall process of ensuring predictive DSIs are FAVES and for determining how these predictive DSIs can be best used in their settings and for their patients.

We also seek input on any information the Department should consider or action the Department should consider taking to facilitate healthcare organizations and clinicians having the necessary competencies or expertise to assess whether a predictive DSI is trustworthy, in that the model is FAVES. This would be in addition to the information transparency (disclosures) that the proposed requirements would provide users, should those proposals be finalized. We seek input on any information commenters can offer on these topics. We understand that some aspects of predictive DSI should be familiar to clinicians and healthcare organizations because they parallel diagnostic tests and long-used risk calculators, but that other competencies may be novel and challenging. We seek input on activities, such as support for, establishment of, and

[250] See AI actors, life cycle, and activities, as detailed in Figure 3 and 4 of the NIST AI RMF: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

dissemination of learning collaboratives, best practices, 'playbooks,' or other approaches that the Department might pursue to facilitate users of certified health IT being well-equipped to determine whether predictive DSIs applied in their settings and to their patients are trustworthy.

- Data Practices and Governance: Ethical, Legal, and Social Implications of Data Collection and Use

We are aware of concerns about ELSI considerations regarding the initial or underlying data collection (sharing), data use (processing, analysis), and future (downstream) use or reuse of data,[251] including PHI,[252] in health and healthcare.[253] These considerations include those related to and impacting individuals during the design, development, implementation, and use of emerging technologies, including AI/ML-driven predictive models (data analytics tools or software), as well as the application of big data in healthcare and how these technologies may be perceived by different communities.[254] For example, we understand the public concern about AI/ML-enabled technologies, including the potential for these technologies to lead to widening health disparities, perpetuating historical human or data bias or inequity, introducing bias or disparities, and reinforcing existing ones. We also understand that there are concerns about negative, adverse, or harmful consequences that may result from the use (including data analytics) of digital data or information about individuals' health, including historically, their use in computerized decision making.[255] These concerns include, but are not limited to, those pertaining to bias or unlawful discrimination (equity), ethics, information privacy,

---

[251] See, e.g., National Telecommunications Information Administration (NTIA), U.S. Department of Commerce, Privacy, Equity, and Civil Rights, Request for Comment, January 18, 2023, https://www.ntia.gov/sites/default/files/publications/ntia_pecr_rfc_final_signed.pdf.
[252] See 45 CFR 160.103.
[253] See, e.g., Gerke S, Minssen T, Cohen G. Ethical and legal challenges of artificial intelligence-driven healthcare. Artificial Intelligence in Healthcare. 2020:295–336, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7332220/ (discussing ethical and legal challenges of AI-driven healthcare and potential strategies in the US and Europe).
[254] See generally University of California Health Data Governance Task Force, *Got Health Data? Moving Toward a Justice-Based Model of Data Use*, https://www.ucop.edu/uc-health/functions/got-health-data-moving-toward-a-justice-based-model-of-data-use-conference-april-2022.html ONC Health IT Policy Committee, Privacy and Security Workgroup, *Recommendations on Health Big Data* (August 2015), https://www.healthit.gov/sites/default/files/facas/HITPC_Health_Big_Data_Report_FINAL.pdf.
[255] See, e.g., the Department of Health, Education, & Welfare (HEW) *Report, Records, Computers, & Rights of Citizens*, 1973, https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

confidentiality, and security (safety), data misuse, data reuse (secondary use), data re-identification, and the ability to link data or records to individuals.[256] Existing federal laws and regulations address data protection, governance, and stewardship by providing federal protections for civil rights, health information privacy, human subjects, veteran data, and consumers' data privacy. For example, the HIPAA Privacy,[257] Security,[258] and Breach Notification[259] Rules ("HIPAA Rules") provide for the privacy and security of PHI used and disclosed by covered entities and their business associates. Generally, the HIPAA Privacy Rule establishes national standards for the use and disclosure of PHI,[260] including when and for what purposes HIPAA covered entities and business associates may create, receive, maintain, or transmit PHI.

The HIPAA Privacy Rule identifies the purposes for which PHI may be used and disclosed by covered entities and their business associates without an individual's authorization, including for treatment, payment, health care operations, research, and public health activities.[261] Business associates include persons who, on behalf of the HIPAA covered entity, create, receive, maintain, or transmit PHI for a function or activity regulated under the HIPAA Rules including, among other things, claims processing or administration, data analysis, data aggregation, quality assurance, patient safety activities, and practice management.[262] Persons who provide cloud computing services to covered entities, including those that may have AI/ML, algorithms, and predictive technologies that are enabled by or interface with certified Health IT Modules, may also be business associates.[263] Those persons or entities that provide AI/ML, algorithms, and

---

[256] See, e.g., Andrews, Edmund, Stanford University Human-Centered Artificial Intelligence, June 2022, https://hai.stanford.edu/news/rob-reich-ai-developers-need-code-responsible-conduct.
[257] See 45 CFR part 160 and subparts A and E of part 164.
[258] See 45 CFR part 160 and subparts A and C of part 164.
[259] See 45 CFR part 160 and subparts A and D of part 164.
[260] See 45 CFR 164.502(b), 164.514(d); 45 CFR 164.501, 164.508(a)(3), 45 CFR 164.514.
[261] See 45 CFR part 164.
[262] See the definition of "business associate" at 45 CFR 160.103.
[263] See also OCR's Guidance on HIPAA and Cloud Computing, https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html (noting that cloud computing services range "from mere data storage to complete software solutions (e.g., an electronic medical records system)").

predictive technologies that do not meet the definition of a covered entity or business associate are not regulated by the HIPAA Rules.

We are aware the use of data related to a person's health raises consumer privacy concerns with these emerging technologies,[264] not only because those persons or entities that provide these technologies may not be subject to the requirements of the HIPAA Rules.[265] For example, there are concerns that the development or use such technologies could lead to the disclosure of more PHI than is necessary to accomplish the requester's purpose in certain circumstances; concerns regarding the use or disclosure of PHI for marketing purposes;[266] concerns regarding the commercialization, monetization, licensure, or sale of PHI;[267] and concerns regarding compliance with de-identification requirements when necessary.[268] These concerns also include those related to record linkage for biomedical research[269] and the transfer of health information about individuals in ways that patients might not expect or want, or that do not reflect a patient's reasonable expectation, knowledge, or consent.

We are also aware of the increased interest within the healthcare community in using data and AI-and ML-driven technologies for population-based activities related to improving health or reducing healthcare costs, as well as for continuity of care purposes and overall case

---

[264] See, e.g., Murdoch, B. Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Med Ethics 22, 122 (2021). https://doi.org/10.1186/s12910-021-00687-3; Na L, Yang C, Lo C, Zhao F, Fukuoka Y, Aswani A. Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use of Machine Learning. JAMA Netw Open. 2018;1(8):e186040. doi:10.1001/jamanetworkopen.2018.6040; McKeon, Jill, Security, Privacy Risks of Artificial Intelligence in Healthcare, (Dec. 1, 2021), https://healthitsecurity.com/features/security-privacy-risks-of-artificial-intelligence-in-healthcare.

[265] See generally HHS Office of the Chief Technology Officer and Open Data Enterprise, *Sharing and Utilizing Health Data for AI Applications*, Roundtable Report, 2019, https://www.hhs.gov/sites/default/files/sharing-and-utilizing-health-data-for-ai-applications.pdf.

[266] 45 CFR 164.501 for definition of "marketing," 164.508(a)(3).

[267] 45 CFR 164.502(a)(i), 164.508(a)(4). A covered entity nor a business associate may not sell PHI without an authorization from the patient. A covered entity must obtain an authorization for any disclosure of PHI which is a sale of PHI.

[268] 45 CFR 164.514. See also OCR's Guide Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

[269] See, e.g., The National Institutes of Health (NIH) Office of Data Science Strategy (ODSS) and the National Library of Medicine (NLM), NIH Workshop on the Policy and Ethics of Record Linkage, June 29-30, 2021, https://datascience.nih.gov/nih-policy-and-ethics-of-record-linkage-workshop-summary. See also, NIH Common Fund's Bridge to Artificial Intelligence (Bridge2AI), https://commonfund.nih.gov/bridge2ai.

management, care planning, and care coordination, both within and outside of the health care setting, including with community-based organizations.[270]

HIPAA covered entities, such as health care providers, are generally among the customers of health IT developers, and in many cases, health IT developers serve as HIPAA business associates to their covered entity customers. Additionally, as discussed above, persons who provide cloud computing services to covered entities may also be business associates.[271] If a cloud computing service is a business associate, the uses and disclosures of PHI by such cloud computing service provider will be limited by the limitations imposed by the HIPAA Privacy Rule and those outlined in their signed Business Associate Agreements (BAAs), which may address many of the public's concerns.

However, not all entities that collect, share, and use health data are regulated by the HIPAA Rules.[272] Thus, the HIPAA Rules do not apply or protect the privacy or security of all data related to an individual's health regardless of where the data originated or is used (data source). However, there are other federal and state laws that may impose obligations upon organizations to protect consumer health data.[273] For instance, the FTC Act applies to both HIPAA covered entities and those entities not covered under HIPAA, and prohibits deceptive or unfair business practices, including in the context of health data. The FTC also enforces the Health Breach Notification Rule, which applies to certain entities not covered under HIPAA.[274]

We are aware of potential intersections with the application and use of privacy engineering or privacy by design approaches and techniques (e.g., data minimization) to help address some of the concerns discussed in this section. For example, the use of privacy-

---

[270] See generally ONC AI Showcase, January 2022, https://www.healthit.gov/news/events/onc-artificial-intelligence-showcase-seizing-opportunities-and-managing-risks-use-ai.
[271] See OCR's Guidance on HIPAA and Cloud Computing, https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html (noting that cloud computing services range "from mere data storage to complete software solutions (e.g., an electronic medical records system)").
[272] See HHS, *Examining Oversight of the Privacy and Security of Health Data Collected by Entities Not Regulated by HIPAA*, Report to Congress, (2016) https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.
[273]. See *supra* note 291 describing applicable federal consumer protection laws; See *supra* note 102 describing applicable federal civil rights laws.
[274] 15 U.S.C. § 45(a) (Section 5 of the FTC Act) and Health Breach Notification Rule in 16 CFR part 318.

preserving data sharing and analytics (PPDSA) techniques or tools, through the application of privacy enhancing technologies (PET),[275] could potentially enable collective data sharing and analysis while maintaining disassociability and confidentiality.[276] In addition, we understand that the use of technology and technical functionality or capabilities to enable electronic consent regarding data sharing and confidentiality, including how and when data about an individual can be collected and used as well as capturing, maintaining, and communicating patient's consent decision, continues to evolve.[277] We also understand that collaboration and use of an interdisciplinary or cross-functional approach across one or more parts of the development life cycle of these technologies, involving interested parties or representative actors from various disciplines (e.g., clinicians, data scientists, attorneys, social scientists, programmers, computer engineers or scientists, bioethicists, informaticians, compliance officers, patients) as part of a multi-disciplinary process,[278] could help address some of the privacy and equity concerns around data practices.

We seek comment on issues the public believes the Department should consider addressing: health equity, information privacy, information security, patient safety, and data stewardship concerns while enabling trusted development and uses of health data to advance individuals' well-being and overall technology innovation, including AI, ML, and algorithms in

---

[275] See generally OECD Report, Emerging privacy-enhancing technologies, (March 2023), https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm; The Royal Society, From privacy to partnership: The role of privacy enhancing technologies in data governance and collaborative analysis, (January 2023), https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf.

[276] See White House, Office of Science and Technology Policy (OSTP), on behalf of the Fast Track Action Committee on Advancing (FTAC) Privacy-Preserving Data Sharing and Analytics, "Request for Information on Advancing Privacy-Enhancing Technologies," FRN 87 FR 35250, June 9, 2022, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies; https://www.nitrd.gov/fast-track-action-committee-on-advancing-privacy-preserving-data-sharing-and-analytics-roundtable-series/; White House, Press Release, U.S. *U.K. Launch Innovation Privacy Challenges for Privacy-Enhancing Technologies to Tackle Financial Crime and Public Health Emergencies*, July 20, 2022, https://www.whitehouse.gov/ostp/news-updates/2022/07/20/u-s-and-u-k-launch-innovation-prize-challenges-in-privacy-enhancing-technologies-to-tackle-financial-crime-and-public-health-emergencies/. See also *Selecting Privacy-Enhancing Technologies for Managing Health Data Use,* (March 2022), https://doi.org/10.3389/fpubh.2022.814163.

[277] See also section III.C.10 of this preamble "patients right to request restrictions."

[278] See generally Figure 3 of NIST AI RMF 1.0, https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook.

healthcare. In particular, there are concerns pertaining to appropriate data de-identification (including managing re-identification risk), data use (processing and application), and data governance in healthcare. We seek comment on the desirability of federal guidance or education materials to help the public better understand and navigate the implications of existing federal protections with respect to the development and application of AI and ML-driven technologies to healthcare. We also welcome comment on how ONC can help developers of certified health IT further support users or provide additional technical capabilities to enhance and support health equity, data privacy and security with the use of algorithmic-based technology in healthcare. This request for comment relates to ONC's authorities under the HITECH Act and the Cures Act with respect to adopting standards, implementation specifications, and certification criteria as part of the Program, overseeing developers of certified health IT through Conditions and Maintenance of Certification requirements, and serving in a coordinating role with respect to health IT. Comments will help inform ONC's activities in these areas and strategic objectives, including advancing the development and use of health IT capabilities and establishing expectations for data sharing.

Request for Comment

- Technical Data Standards and Data Management: Electronic Data Source, Capture, and Use

As we discuss in our proposals related to risk management above, we understand and are aware of concerns about historical, systemic issues in source (or input) data collection, capture and use of routinely collected data, including data quality (e.g., data fit for purpose),[279] fidelity, utility, access, de-biasing or standardizing the way data is collected, and data provenance or

[279] Rajan NS, Gouripeddi R, Mo P, Madsen RK, Facelli JC. Towards a content agnostic computable knowledge repository for data quality assessment. Comput Methods Programs Biomed. 2019 Aug;177:193-201. doi: 10.1016/j.cmpb.2019.05.017. Epub 2019 May 24. PMID: 31319948.Rajan NS, Gouripeddi R, Mo P, Madsen RK, Facelli JC. Towards a content agnostic computable knowledge repository for data quality assessment. Comput Methods Programs Biomed. 2019 Aug;177:193-201. doi: 10.1016/j.cmpb.2019.05.017. Epub 2019 May 24. PMID: 31319948.

lineage (origin of data).[280] We are aware of the need regarding the development and advancement of alignment or harmonization of technical standards and support for driving adoption of USCDI data elements for representation of REL, SDOH, sexual orientation, gender identity, and various patient demographic and health status assessment data, as this data may serve as inputs to algorithmic or model "outputs." We also understand that there are technical data standard gaps for key groups and populations that could impact the fairness of DSIs that Health IT Modules enable or interface with. For example, we are aware there is limited use of consistent technical standards for coding patient disability, impairments, and other functional limitations. In addition, we support data representation fairness with an understanding that incomplete or underrepresented data that goes into a DSI could impact the output and overall use and application of the DSI. Fairness in representativeness of data includes how and whether populations are represented in training and test data for the design and development of DSI. We understand having knowledge of and focusing on addressing health disparities during model development is another important consideration related to fairness. We also are aware of the Findability, Accessibility, Interoperability, and Reuse (FAIR) Data Principles for scientific data management and stewardship that support enhancing the reusability of data with an emphasis on machine-actionability for scientific data and datasets used for data models, given the increased reliance on computational systems.[281]

---

[280] See generally https://www.sciencedirect.com/science/article/pii/S1064748121003614; https://www.jmir.org/2018/5/e185; https://doi.org/10.1016/j.jclinepi.2020.03.028; See e.g., Weikel, B. W., Klawetter, S., Bourque, S. L., Hannan, K. E., Roybal, K., Soondarotok, M., St Pierre, M., Fraiman, Y. S., & Hwang, S. S. (2023). *Defining an Infant's Race and Ethnicity: A Systematic Review. Pediatrics*, 151(1), e2022058756. https://doi.org/10.1542/peds.2022-058756; Gagliardi J. P. (2021). *What Are the Data Really Telling Us About Systemic Racism?,* American Association for Geriatric Psychiatry, 29(10), 1074–1076. https://doi.org/10.1016/j.jagp.2021.06.007; Dullabh, P., Hovey, L., Heaney-Huls, K., Rajendran, N., Wright, A., & Sittig, D. F. (2020). *Application Programming Interfaces in Health Care: Findings from a Current-State Sociotechnical Assessment*. Applied clinical informatics, 11(1), 59–69. https://www.sciencedirect.com/science/article/pii/S0895435619307668.

[281] FAIR principles, https://www.go-fair.org/fair-principles/ (noting the principles emphasize "the capacity of computational systems to FAIR data with no or minimal human intervention, given that humans increasingly rely on computational support to deal with data as a result of the increase in volume, complexity, and creation speed of data"). See Wilkinson, M., Dumontier, M., Aalbersberg, I. *et al.* The FAIR Guiding Principles for scientific data management and stewardship. *Sci Data* 3, 160018 (2016), https://www.nature.com/articles/sdata201618.

We understand the importance of appropriate electronic collection, standardized capture, and use of standardized data in healthcare, including when that data serves as inputs to algorithms, DSIs, and other advanced technologies in healthcare. ONC supports the use of technology to improve the standardized capture of a set of health data classes to support the healthcare industry's need to electronically capture the underlying data they collect for treatment, payment, health care operations, research, and public health purposes.[282] We seek comment on how ONC can further support standardization and harmonization in these areas.

xii. Proposed Update from Clinical Decision Support to Decision Support Intervention Criterion

We propose modifications to the "Base EHR" definition in § 170.102 to identify that a Health IT Module can be certified to either § 170.315(a)(9) or § 170.315(b)(11) to satisfy the definition for the period up to and including December 31, 2024. We also propose that § 170.315(a)(9) would no longer be included as part of the Base EHR definition after December 31, 2024. Rather, only § 170.315(b)(11) and not § 170.315(a)(9) would be available as a certification criterion to satisfy the definition of "Base EHR" beginning January 1, 2025.

Additionally, in § 170.315(a)(9)(vi) we propose that the adoption of § 170.315(a)(9) would expire on January 1, 2025, for purposes of the Program. Together, these proposals identify the dates when § 170.315(b)(11) replaces § 170.315(a)(9) in the Base EHR definition, and they indicate when Health IT Modules certified to § 170.315(a)(9) would need to be certified to § 170.315(b)(11) to maintain compliance with the Base EHR definition.

d. Proposed Updates to Real World Testing Condition for CDS Criterion

We propose to revise § 170.405(a) to include § 170.315(a)(9) within the list of certification criteria for which a developer of certified health IT with Health IT Module(s) certified to such criteria must successfully test the real world use of those Health IT Module(s)

[282] See 45 CFR 164.501 for complete definitions of "treatment", "payment", "health care operations", and "research"; 45 CFR 164.512(b) for discussion of "public health" activities.

for interoperability in the type of setting in which such Health IT Module(s) would be or are marketed. This would mean that a developer of certified health IT with a Health IT Module certified to § 170.315(a)(9) would be subject to the requirements set forth in § 170.405(a). This proposal would require developers of certified health IT with Health IT Modules certified to § 170.315(a)(9) to submit real world test plans and results, among other requirements, as part of the real world testing Condition and Maintenance of Certification requirements. Further, in proposing the new "Decision Support Interventions" certification criterion in § 170.315(b)(11), we recognize and intend that the developers of Health IT Modules certified to § 170.315(b)(11) would be required to conduct real world testing consistent with the existing requirements in § 170.405(a). We note this is because all criteria in § 170.315(b) are already subject to those real world testing requirements.

We believe that requiring developers of certified health IT with Health IT Modules certified to § 170.315(a)(9) to participate in real world testing is consistent with our existing approach to implementing the real world testing Condition and Maintenance of Certification requirements by focusing on interoperability-related criteria. The capabilities included within the certification criterion in § 170.315(a)(9) are interoperability focused, and § 170.315(a)(9) is unlike other certification criteria currently adopted in the "clinical" section in § 170.315(a). The functionality expressed in § 170.315(a)(9) does not result in enabling a user to "record," "change," and "access" specific data types; rather, the functionality in § 170.315(a)(9) is more complex and multi-faceted. The primary functionality of both § 170.315(a)(9) and the proposed § 170.315(b)(11) is to ensure that multiple decision support intervention types are (1) supported through interaction with certified health IT and (2) configurable based on a specified set of data types (including data listed in the § 170.315(a)(5) demographics criterion). Additionally, the existing criterion in § 170.315(a)(9) specifies, and proposed criterion in § 170.315(b)(11) would specify, that certified Health IT Modules must support the availability of an intervention's source attributes for users to review. In this regard, ONC's existing CDS criterion and the proposed

criterion in § 170.315(b)(11) are more like the care coordination criteria in § 170.315(b)(1) "Transitions of Care" and § 170.315(b)(2) "Clinical Information Reconciliation and Incorporation." Further, to be enabled, interventions in § 170.315(a)(9) must rely on a wide array of problems, medications, demographics, laboratory tests and vital signs – both generated in the source system and received through a transition of care or referral. In this regard, the functionality required by § 170.315(a)(9) represents an important culmination of ONC's interoperability efforts, fitting appropriately in with other criteria listed in § 170.405(a).

We believe there are other important reasons to include § 170.315(a)(9) in § 170.405(a). First, this requirement will provide developers with an opportunity to demonstrate how their support of evidence-based CDS and linked referential CDS positively impacts patient care through real world testing plans and results. We know that developers of certified health IT support numerous kinds of CDS, many of which are foundational to improving patient care or support other important outcomes in healthcare. Second, requiring Health IT Modules certified to § 170.315(a)(9) to be subject to real world testing will provide the public at large with information on how different certified Health IT Modules are implementing and supporting the CDS certification criterion. For example, we would expect developers to establish a range of measures as part of their real world testing plans, described in § 170.405(b)(1), because developers have flexibility to craft real world testing measures specific to their products and customers. We would also expect developers of certified health IT with Health IT Modules certified to § 170.315(a)(9) to report on those measures as part of real world testing results, per requirements in § 170.405(b)(2), which would have the potential to provide the public with new insights on the market for CDS. Finally, we believe that requiring developers with Health IT Modules certified to § 170.315(a)(9) to participate in real world testing will be a helpful bridge to compliance for similar requirements proposed for the Decision Support Interventions certification criterion.

We note that the effect of proposing to include Health IT Modules certified to § 170.315(a)(9) in § 170.405(a) and the effect of proposing a revised version of the CDS criterion in § 170.315(b)(11), would require developers of certified health IT certified to § 170.315(a)(9) and § 170.315(b)(11) to follow the testing plans, methods, and results reporting; submission dates; and August 31 deployment deadline requirements in § 170.405(b) similar to the requirements of other applicable certification criteria listed in § 170.405(a). We anticipate that if finalized as proposed this would mean that Health IT Modules certified to § 170.315(a)(9) would be subject to the real world testing Condition and Maintenance of Certification requirements beginning with the 2023 real world testing cycle. This means that Health IT Modules certified to § 170.315(a)(9) prior to August 31, 2023, would need to, among other requirements, address each of the elements in § 170.405(b)(1)(iii)(A) through (G) in their real world testing plans by December 15, 2023, and submit results based on those plans no later than March 15, 2025. We invite comment on this proposal.

Relationship to Other Federal Agencies' Relevant Activities, Interests, and Regulatory Authority

There is broad interest across the Department in the development, implementation, and use of algorithms and AI in healthcare.[283] AHRQ is exploring the impact of existing healthcare

---

[283] See, e.g., The NIH recently established the Artificial Intelligence Machine Learning Consortium to Advance Health Equity and Researcher Diversity (AIM-AHEAD) to identify priority research aims in health equity and AI/ML, as well as the training and infrastructure needed to support these, https://datascience.nih.gov/artificial-intelligence/aim-ahead. The 2022 Centers for Medicare & Medicaid Servicers (CMS) Strategic Plan includes a pillar to advance health equity, including incorporating equity in model design, https://www.cms.gov/sites/default/files/2022-04/Health%20Equity%20Pillar%20Fact%20Sheet_1.pdf; NIH NCATS, *Bias Detection Tools in Health Care Challenge*, (October 2022): https://www.challenge.gov/?challenge=minimizing-bias-and-maximizing-long-term-accuracy-of-predictive-algorithms-in-healthcare; The Secretary's Advisory Committee on Human Research Protections (SACHRP) Recommendations, Considerations for the Institutional Review Board (IRB) Review Involving AI, (July 2022), https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-e-july-25-2022-letter/index.html; Zuckerman, Brian L., James M. Karabin, Rachel A. Parker, William E. J. Doane, and Sharon R. Williams (2022). *Options and Opportunities to Address and Mitigate the Existing and Potential Risks, as well as Promote Benefits, Associated with AI and Other Advanced Analytic Methods,* OPRE Report #2022-253, Washington, DC: Office of Planning, Research, and Evaluation, Administration for Children and Families, U.S. Department of Health and Human Services, https://www.acf.hhs.gov/opre/report/options-opportunities-address-mitigate-existing-potential-risks-promote-benefits; See HHS. Trustworthy AI (TAI) Playbook. September 2021, https://www.hhs.gov/sites/default/files/hhs-trustworthy-ai-playbook.pdf.

algorithms on racial and ethnic disparities in health and healthcare.[284] The FDA recently discussed the development of sophisticated algorithms that incorporate AI/ML and the role they play in health, as part of the FDA's strategic priority to advance health equity[285] as well as provided clarity around which CDS functionalities they consider to be a medical device.[286] The HHS Office for Civil Rights (OCR) is proposing to clarify through regulation that Section 1557 of the Affordable Care Act prohibits a covered entity from discriminating on the basis of race, color, national origin, sex, age, or disability in its health programs and activities through the use of clinical algorithms in its decision-making.[287] Also, CMS recently requested information on how Medicare policy can encourage software developers to prevent and mitigate bias in algorithms and predictive modeling as well as how to accurately evaluate that necessary steps have been taken to prevent and mitigate bias in software algorithms.[288]

Outside of the Department, multiple federal agencies are also exploring policies to prevent and mitigate bias in AI and ML and the intersection with privacy, equity, and civil

---

[284] See AHRQ, *Impact on Healthcare Algorithms on Racial and Ethnic Disparities in Health and Healthcare*, Systematic Review Protocol, https://effectivehealthcare.ahrq.gov/products/racial-disparities-health-healthcare/protocol; AHRQ, Draft Comparative Effectiveness Review, February 2023, https://effectivehealthcare.ahrq.gov/products/racial-disparities-health-healthcare/draft-report; AHRQ, *Meetings Examine Impact of Healthcare Algorithms on Racial and Ethnic Disparities in Health and Healthcare*, (March 2023), https://effectivehealthcare.ahrq.gov/news/meetings.

[285] See FDA, Center for Devices and Radiological Health, 2022-2025 Strategic Priorities, https://www.fda.gov/media/155888/download. The FDA also has an action plan to advance regulatory concepts for AI/ML-based devices and has identified guiding principles for the development of good machine learning practices related to AI/ML-based medical devices. See https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device; U.S. Food & Drug Admin., *Good Machine Learning Practice for Medical Device Development: Guiding Principles* (Oct. 2021), https://www.fda.gov/medical-devices/software-medical-device-samd/good-machine-learning-practice-medical-device-development-guiding-principles.

[286] For information about the scope of decision support software functions as a medical device, see FDA, *Clinical Decision Support Software Final Guidance* (September 2022), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software?utm_medium=email&utm_source=govdelivery; FDA's Digital Health Policy Navigator, https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-policy-navigator?utm_medium=email&utm_source=govdelivery.

[287] See 87 FR 47824.

[288] CMS, Medicare Program: Hospital Outpatient Prospective Payment Systems (OPPS) NPRM, 87 FR 44502, July 2022, https://www.federalregister.gov/documents/2022/07/26/2022-15372/medicare-program-hospital-outpatient-prospective-payment-and-ambulatory-surgical-center-payment#p-1338 (noting that "bias in software algorithms has the potential to disparately affect the health of certain populations.") In 2020, CMS hosted an AI Health Outcomes Challenge for innovators to demonstrate how AI tools can be used to accelerate development of AI solutions for predicting patient health outcomes for Medicare beneficiaries for potential use in CMS Innovation Center innovative payment and service delivery models and solicited public feedback to better understand the resource costs for services involving the use of innovative technologies, including but not limited to software algorithms and AI. See https://innovation.cms.gov/innovation-models/artificial-intelligence-health-outcomes-challenge#:~:text=The%20CMS%20Artificial%20Intelligence%20(AI,for%20potential%20use%20in%20CMS.

rights.[289] For example, the Federal Trade Commission (FTC) has addressed AI repeatedly in its work through a combination of law enforcement and policy initiatives,[290] and recently sought

---

[289] See, e.g., The U.S. Department of Commerce, including the National Telecommunications and Information Administration (NTIA) is exploring the intersection of privacy, equity, and civil rights, exploring ways in which commercial data flows of personal information can lead to disparate impact and outcomes for marginalized or disadvantaged communities. See https://hai.stanford.edu/events/artificial-intelligence-and-economy-charting-path-responsible-and-inclusive-ai and https://www.federalregister.gov/documents/2021/11/30/2021-25999/privacy-equity-and-civil-rights-listening-sessions; The U.S. Department of Justice, *Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring* (2022), https://beta.ada.gov/ai-guidance/; EEOC: The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees, EEOC-NVTA-2022-2 (2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence; U.S. Equal Employment Opportunity Commission (EEOC), *Launches Initiative on Artificial Intelligence and Algorithmic Fairness* (Oct. 28, 2021), https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness; The U.S. Department of Veterans Affairs, AI Strategy, (July 2021), https://www.research.va.gov/naii/VA_AI%20Strategy_V2-508.pdf; Bd. of Governors of the Fed. Reserve System, Bureau of Consumer Fin. Protection, Fed. Deposit Ins. Corp., Nat'l Credit Union Admin., & Office of the Comptroller of the Currency, 86 FR 16837 (Mar. 31, 2021) (Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, Identifying Unlawful Discrimination as a Potential Risk of Using Artificial Intelligence); Bureau of Consumer Fin. Protection, Circular 2022-03, Adverse Action Notification Requirements in Connection with Credit Decisions Based on Complex Algorithms (May 26, 2022), https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/. See also, the National AI Advisory Committee (NAIAC), https://www.ai.gov/naiac/.

[290] See, e.g., The FTC and U.S. Department of Justice settled a lawsuit against a weight loss app, requiring it to delete data and its novel algorithms, and pay a fine for illegally collecting personal data from children under 13. https://www.justice.gov/opa/pr/weight-management-companies-kurbo-inc-and-ww-international-inc-agree-15-million-civil-penalty. See also, "Everalbum" case, https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3172-everalbum-inc-matter (settling allegations that the company deceived consumers about the use of facial recognition to analyze users' private images, including in connection with training FRT models); the "Mole Detective" case: https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3210-new-consumer-solutions-llc-mole-detective (alleging deceptive conduct, where app developers claimed in advertisements that their consumer-facing app could determine based on photographs whether a mole was cancerous). See FTC Report to Congress on Privacy and Security, September 2021, https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf; *Aiming for truth, fairness, and equity in your company's use of AI*, FTC Blog, (April 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai (discussing FTC's activities in this area); https://www.ftc.gov/system/files/documents/public_statements/1587283/fpf_opening_remarks_210_.pdf; *Keep your AI claims in check*, FTC Blog, (February 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check For information on best practices to reduce bias and discrimination in clinical algorithms, *see generally* Fed. Trade Comm'n, Using Artificial Intelligence and Algorithms (Apr. 8, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms; Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; Rebecca Kelly Slaughter, Algorithms and Economic Justice, Yale J. L. & Tech. (Aug. 2021), https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pd The agency has also held several public events focused on AI issues, including workshops on dark patterns and voice cloning, sessions on AI and algorithmic bias at PrivacyCon 2020 and 2021, a hearing on competition and consumer protection issues with algorithms and AI, a FinTech Forum on AI and blockchain, and an early forum on facial recognition technology (resulting in a 2012 staff report). See https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop; https://www.ftc.gov/news-events/events-calendar/you-dont-say-ftc-workshop-voice-cloning-technologies; https://www.ftc.gov/news-events/events-calendar/privacycon-2021; https://www.ftc.gov/news-events/eventscalendar/privacycon-2020; https://www.ftc.gov/news-events/events-calendar/ftc-hearing-7-competition-consumerprotection-21st-century; https://www.ftc.gov/news-events/events-calendar/2017/03/fintech-forum-blockchainartificial-intelligence; and https://www.ftc.gov/news-events/events-calendar/2011/12/face-facts-forum-facialrecognition-technology.

comment on harms from businesses of collecting, analyzing, and monetizing information about people.[291] In addition, NIST is actively working to move toward standardizing ways to identify and manage the harmful effects of bias in AI technology,[292] and developing a standard risk management framework for AI.[293]

We note that ONC regulates developers of certified health IT and their Health IT Modules, ensuring that both conform to technical standards, certification criteria, implementation specifications, and adhere to Conditions and Maintenance of Certification requirements. As it relates to the current CDS criterion in § 170.315(a)(9), ONC's regulatory oversight of developers of certified health IT includes requirements that their Health IT Modules certified to that criterion can enable two types of decision support interventions, evidence-based and linked referential, which must be (1) configurable based on data specified in § 170.315(a)(9)(ii) and (2) include source attributes in § 170.315(a)(9)(v) relevant to the individual decision support intervention enabled by the certified Health IT Module. We note that our authority to regulate developers of certified health IT under the Program is separate and distinct from other federal agencies' regulatory authorities focused on the same or similar entities and technology. For example, the safety and effectiveness of a software function, including clinical decision support or other kinds of decision support interventions, is within the purview of Food and Drug Administration (FDA) regulatory oversight, if such software functionality meets the definition of a "device."[294] In the area of predictive technology, ONC and FDA support a harmonized and

---

[291] *See also* Press Release, FTC, California Company Settles FTC Allegations It Deceived Consumers about use of Facial Recognition in Photo Storage App (Jan. 11, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers-about-use-facial-recognition-photo (announcing settlement of allegations that company deceived consumers about the use of facial recognition to analyze users' private images, including in connection with training FRT models); Press Release, FTC, FTC Cracks Down on Marketers of "Melanoma Detection" Apps (Feb. 23, 2015) https://www.ftc.gov/news-events/news/press-releases/2015/02/ftc-cracks-down-marketers-melanoma-detection-apps (announcing settlements of allegations that operators of mobile applications engaged in unlawful deception by claiming that their applications could detect a mole's melanoma risk based on a photograph taken with a smart phone).

[292] NIST, SP 1270, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

[293] NIST, AI 100-1, https://www.nist.gov/itl/ai-risk-management-framework.

[294] See *supra* 87. For more information about determining whether a software function is potentially the focus of the FDA's oversight, please visit the FDA's Digital Health Policy Navigator Tool: https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-policy-navigator.

complementing approach, independent of the platform that the technology exists on, in accordance with our existing intersecting regulatory oversight.

We note that the questions of whether DSIs enabled by or interfaced with certified health IT are subject to FDA regulations, under the Federal Food, Drug, & Cosmetic Act, or are used by entities subject to the HIPAA Rules,[295] federal nondiscrimination laws,[296] federal consumer protection laws[297] or other federal regulations,[298] are separate and distinct from the question of whether a developer or such technology is subject to regulatory oversight by ONC's Health IT Certification Program, to which our proposals pertain.

Given the intersecting nature and interest across the Department to address the use of AI for purposes of health, we consulted extensively with our HHS partners. Specifically, we worked with counterparts at AHRQ, FDA, and OCR in developing proposals to advance our shared goals of promoting predictive DSIs in healthcare that are valid, fair, appropriate, effective, and safe to deliver patient care. We plan to continue to coordinate with these and other federal agencies so that to the extent practicable, federal requirements that may apply to certified health IT and developers of certified health IT are aligned and not duplicative.

In this proposal, we are taking an approach that is both reflective of our authorities and aligned with others in the Department and Federal Government. We are not establishing requirements for technology not certified under the Program.[299] We are also not establishing new requirements for FDA regulation of software as a device or expectations for software functions

---

[295] For more information about entities subject to the HIPAA Rules, please visit: https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html. See also definitions of "covered entity" and "business associate" at 45 CFR 160.103.

[296] For more information about covered entities that must comply with federal nondiscrimination laws enforced by OCR, please visit: https://www.hhs.gov/civil-rights/for-providers/index.html.

[297] See FTC, *Report to Congress on Privacy and Security*, September 2021, https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

[298] See, e.g., SACHRP, *Considerations for IRB Review of Research Involving AI* (discussing the Common Rule), (July 2022) https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-e-july-25-2022-letter/index.html.

[299] See the ONC Health IT Certification Program, https://www.healthit.gov/topic/certification-ehrs/about-onc-health-it-certification-program.

that meet the definition of a device,[300] including "Device CDS" software functions that are regulated by FDA as devices.

We anticipate that our collaboration with our federal partners on these proposed requirements would assist AHRQ, CMS, FDA, FTC, NIST, OCR, Veterans Health Administration, and other federal partners as they work within the bounds of their respective legal authorities with the goal of having greater consistency across federal agencies and the entire health IT ecosystem.

6. Synchronized Clocks Standard

We propose to remove from 45 CFR 170.210(g) the current named specification for clock synchronization, which is Network Time Protocol (NTP v4 of RFC 5905). However, we propose to amend 45 CFR 170.210(g) so that Health IT Modules certified to applicable certification criteria continue to utilize any network time protocol (NTP) standard that can ensure a system clock has been synchronized and meets time accuracy requirements. The applicable certification criteria that either reference our proposed, revised in § 170.210(g), or cross-reference a provision that references § 170.210(g), include § 170.315(d)(2), § 170.315(d)(3), § 170.315(d)(10), and § 170.315(e)(1).

a. Background

In the 2014 Edition Proposed Rule, we noted that having correctly synchronized clocks is an information security best practice and the NTP has been widely used and implemented since its publication in 1992 (77 FR 13840). We proposed to finalize a requirement for Health IT Modules to use a "synchronized clocks" standard, and we proposed to permit either NTPv3 or NTPv4. In response to the 2014 Edition Proposed Rule, commenters expressed support for our proposed "synchronized clocks" standard and our proposal to permit either NTPv3 or NTPv4. Commenters noted that the use of these synchronization technologies is very common and supported in all major operating systems (77 FR 54184). They stated that it was unclear why this

[300] Section 201(h) of the FD&C Act.

would be a requirement for EHR technology certification because it is unlikely that the EHR technology itself will be directly implementing this type of synchronization and more likely that it will be relying on the lower-level systems' clock functionality (e.g., the operating system within which the EHR technology runs). One commenter stated that it is important to avoid a requirement that would make the operating system (that provides the standard clock) part of what is needed for EHR certification as this would impose artificial limits on what operating systems can be used without certifying multiple permutations. This commenter contended that because the ability to use an operating system clock is common, it was unnecessary for this standard to be required for certification.

In response to this comment, we reiterated our expectation that EHR technology will likely obtain a system time from a system clock that has been synchronized following the NTPv3 or NTPv4 standard (77 FR 54184). We expressly worded the standard to acknowledge this likely scenario by stating "[t]he date and time recorded *utilize* a system clock that has been synchronized * * *." (Emphasis added.) We do not intend for this specific capability to create a binding relationship between EHR technology and a particular operating system. For certification, EHR technology must be able to demonstrate, as the standard states, that it can utilize a system clock that has been synchronized following NTPv3 or NTPv4. Accordingly, we finalized that a Health IT Module certified to § 170.315(d)(2), § 170.315(d)(3), § 170.315(d)(10), or § 170.315(e)(1) would be required to adhere to (RFC 5905) Network Time Protocol Version 4 or Network Time Protocol Version 3 for the synchronized clock requirement.

Feedback from industry has indicated that some developers rely on Microsoft-based operating systems to synchronize network time, which is a different standard than NTP v4. Subsequent to this feedback, we provided sub-regulatory flexibility to health IT developers to

permit the use of Microsoft's "[MS-SNTP]: Network Time Protocol (NTP) Authentication Extensions" (MS-SNTP) in their Health IT Modules.[301]

b. Justification

We propose to remove from § 170.210(g) a named standard to which a system clock has been synchronized when date and time are recorded. This would have the effect of modifying the requirement that Health IT Modules certified to § 170.315(d)(2), § 170.315(d)(3), § 170.315(d)(10), or § 170.315(e)(1) record date and time utilizing a system clock synchronized to a particular named standard. However, we propose to modify § 170.210(g) such that Health IT Modules certified to any of the certification criteria listed above would still be required to utilize a network time protocol standard that can ensure a system clock has been synchronized and meets the time accuracy requirements as defined in the applicable certification criteria.

We understand that beyond NTP and MS-SNTP, there are other network time protocol standards, some of which are more appropriate than others in specific contexts. We also understand that various operating and server systems, such as systems developed and published by Microsoft, employ a Simple Network Time Protocol (SNTP) extension to NTP. We considered proposing to add only the use of MS-SNTP as an alternative to Network Time Protocol Version 4 (NTP v4) of RFC 5905 (currently specified in § 170.210(g)), but decided against proposing this addition given the various standards that exist. We believe that requiring Health IT Modules to support a network time protocol standard of their choosing allows maximum flexibility for both health IT developers of certified health IT and end users of certified Health IT Modules while still ensuring that the time accuracy requirements in the above-listed certification criteria will be fully supported. We welcome comment on these proposals.

7. Standardized API for Patient and Population Services

---

[301] *See* § 170.315(e)(1) paragraph (ii) Certification Companion Guide available here: https://www.healthit.gov/test-method/view-download-and-transmit-3rd-party.

In the ONC Cures Act Final Rule, we adopted multiple standards and implementation specifications in § 170.215 to support the certification criterion in § 170.315(g)(10). At that time, CMS included references to these standards and implementation specifications for the purposes of aligning standards requirements across HHS in the Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers Final Rule (CMS Interoperability and Patient Access Final Rule (85 FR 25510-25640)). Subsequently, we have identified a need to improve the descriptions and categorization of these standards and implementation specifications based on public input. The healthcare and health IT communities have indicated that as HHS continues to advance standards alignment for different use cases, greater clarity in the purpose of each standard and the associated IG may support ease of understanding for organizations with less prior experience with certification criteria and the Program. In addition, public input suggested ONC should provide more clarity to differentiate distinct update timelines for each type of standard or implementation specification, for example when related standards may include different version identifiers (e.g., FHIR Release 4.0.1 as compared to US Core Implementation Guide STU 3.1.1). We are therefore, in conjunction with the proposals described in this section, proposing to reorganize § 170.215 to delineate the purpose and scope more clearly for each type of standard or implementation specification. We propose to revise the structure of § 170.215, to support the proposals described in this section, as follows:

<u>Application Programming Interface Standards.</u>

(a) *API base standard.*

(b) *API constraints and profiles.*

(c) *Application access and launch.*

(d) *Bulk export and data transfer standards*.

(e) *API authentication, security, and privacy.*

We believe this approach will help to provide greater clarity and more specific identification of a standard or implementation specification for a precise purpose or as applicable for a given point in time.

a. Native Applications and Refresh Tokens

In the ONC Cures Act Final Rule, we required Health IT Modules certified to § 170.315(g)(10) to issue refresh tokens to "confidential applications" that could securely receive and store refresh tokens. Specifically, we established in § 170.315(g)(10)(v)(A)(*1*)(*ii*) a requirement for Health IT Modules to issue refresh tokens to applications that are "capable of storing a client secret" (85 FR 25945).

After the publication of the ONC Cures Act Final Rule, health IT developers preparing for testing and certification to the § 170.315(g)(10) certification criterion, as well as third-party application developers, requested that we clarify this requirement. Health IT developers identified that we had not fully explained how our policy would apply to "native applications," which, according to Internet Engineering Task Force (IETF) RFC 6749, are "clients installed and executed on the device used by the resource owner (i.e., desktop application, native mobile application)" and their interactions with OAuth 2.0 authorization servers (85 FR 70076). These health IT developers noted that a strict interpretation of the final rule could exclude native applications. This includes native applications that use or are capable of using additional technology that make them "capable of storing a client secret," as well as native applications that are capable of securely handling a refresh token without needing a client secret. Consequently, health IT developers indicated that the technical ambiguity around native applications would negatively impact testing and certification. Further, health IT developers contended that without timely and explicit clarifications, health IT developers' support for native applications would vary widely (85 FR 70076).

We agreed with these concerns and determined that timely additional clarification was necessary. On November 4, 2020, we published an interim final rule (IFR) with request for comment that corrected this ambiguity and provided clarification (85 FR 70064). In the IFR, we clarified and made the regulation text consistent by adding a new paragraph in § 170.315(g)(10)(v)(A)(*1*)(*iii*) and revising paragraphs § 170.315(g)(10)(v)(A)(*1*)(*ii*) and § 170.315(g)(10)(v)(A)(*2*)(*ii*). In the new paragraph in § 170.315(g)(10)(v)(A)(*1*)(*iii*), we specified that a Health IT Module's authorization server must issue a refresh token to native applications that are capable of securing a refresh token. In § 170.315(g)(10)(v)(A)(*1*)(*ii*) and § 170.315(g)(10)(v)(A)(*2*)(*ii*), we updated the regulation text to be consistent with the paragraph we added in § 170.315(g)(10)(v)(A)(*1*)(*iii*) by specifying that a "Health IT Module's authorization server" must issue a refresh token to applications capable of storing a client secret. And in § 170.315(g)(10)(v)(A)(*2*)(*ii*) we updated the regulation text by removing the word "new" preceding "refresh token" (85 FR 70077). We noted that these updates make the certification criterion clear and consistent and disambiguate the implications for native applications.

We clarified in the IFR preamble that health IT developers must publish the method(s) by which their Health IT Module(s) support the secure issuance of an initial refresh token to "native applications" according to the API technical documentation and transparency requirements in § 170.404. In addition, we clarified that application developer attestations to health IT developers regarding the ability of their applications to secure a refresh token, a client secret, or both, must be treated in a good faith manner consistent with the provisions established in the API openness and pro-competitive conditions in § 170.404(a)(4) (85 FR 70077). Finally, we clarified in the IFR that health IT developers can determine the method(s) they use to support interactions with "native applications" and that health IT developers are not required to support all methods that third-party application developers seek to use (85 FR 70077).

In response to the IFR, we received comments expressing concern that the ability to "secure a refresh token" rather than meet a "confidential app profile" makes the refresh token a

single point of failure and is a major security risk, and that it undermines the control patients exercise when they reauthenticate an app. Commenters suggested that ONC should only require long-term EHR access for native apps that meet the SMART App Launch Guide definition of "confidential app profile." Other commenters argued that ONC's policy creates confusion by creating disparate rules around different application architectures and is not being based in established security standards. They argued that this would result in limiting patient choice without improving security, while also potentially introducing more security concerns. They suggested that ONC should require long-term EHR access to any patient selected application.

In response to public feedback in the IFR, and subsequent interaction with industry, we propose to remove mention of "applications capable of storing a client secret," in § 170.315(g)(10)(v)(A)(*1*)(*ii*) and § 170.315(g)(10)(v)(A)(*2*)(*ii*). We propose to revise § 170.315(g)(10)(v)(A)(*1*)(*ii*) to state, "A Health IT Module's authorization server must issue a refresh token valid for a period of no less than three months to applications using the 'confidential app' profile according to an implementation specification adopted in § 170.215(c)." We also propose to revise § 170.315(g)(10)(v)(A)(*2*)(*ii*) to state, "A Health IT Module's authorization server must issue a refresh token valid for a new period of no less than three months to applications using the 'confidential app' profile according to an implementation specification adopted in § 170.215(c)." These proposed revisions will better reflect a Health IT Module's obligation for first time and subsequent connection refresh tokens using concepts familiar to industry and according to the HL7 FHIR SMART Application Launch Framework. We note that existing requirements for Health IT Modules to issue a refresh token to native applications, consistent with § 170.315(g)(10)(v)(A)(*1*)(*iii*), remains unchanged.

We will continue to monitor implementation of § 170.315(g)(10), engage with the standards development community, and provide information through existing ONC Certification Companion Guides (CCGs), the ONC API Resource Guide, and other educational materials. We invite comment on these proposals.

b. FHIR United States Core Implementation Guide Version 5.0.1

In the ONC Cures Act Final Rule, ONC adopted the FHIR US Core Implementation Guide (IG) STU3 version 3.1.0 implementation specification in § 170.215(a)(2) (85 FR 25740). At the time of the ONC Cures Act Final Rule's publication, the US Core IG STU 3.1.0 was the latest version available. ONC later adopted the FHIR US Core IG v3.1.1 in an interim final rule with comment period published by ONC on November 4, 2020, and titled "Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency" (85 FR 70073-74). The US Core v3.1.1 resolved several technical issues, editorial copy/paste errors, omissions, and places in need of minor clarification in v3.1.0. Both versions define the minimum conformance requirements for accessing patient data using FHIR Release 4 and included profiled resources, operations, and search parameters for the Data Elements required in the USCDI standard (adopted in § 170.213).

Since the publication of the ONC Cures Act Final Rule, the US Core IG has evolved. Yearly US Core IG updates reflect changes to USCDI versions and requests from the HL7 US Realm FHIR community. Notable updates to the US Core IG include v4.0.0, which supports USCDI v1 and clarifies the definition of "must support" elements, and v5.0.1, which supports USCDI v2. As of publication of this NPRM, the National Coordinator has approved both USCDI v2 and the US Core IG v5.0.1 under the Standards Version Adoption Process (SVAP). Health IT developers taking advantage of SVAP flexibility can incorporate these standards into their Health IT Modules as permitted by 45 CFR 170.405(b)(9).

The US Core IG v6.0.0 is anticipated to include support for the data elements and classes added to USCDI v3. At the time of publication of this NPRM, the US Core IG v6.0.0 has not been finalized. Based on the annual US Core release cycle, we believe US Core IG v6.0.0 will be published before ONC issues a final rule.[302] Therefore, it is our intent to consider adopting the

[302] http://hl7.org/fhir/us/core/history.html.

updated US Core IG v6.0.0 that supports the data elements and data classes in USCDI v3 since we propose to adopt USCDI v3 in this rule. Each US Core IG update builds on previous releases to improve the efficacy of the specification by addressing feedback from the HL7 FHIR community. Likewise, as USCDI evolves to address critical healthcare needs such as health equity and public health, the US Core IG provides a foundational standard for accessing and exchanging this data. Health IT systems that adopt the latest version of US Core can therefore provide the latest consensus-based capabilities for providing access to USCDI data classes and elements using FHIR APIs. We propose to adopt the FHIR US Core IG v5.0.1 in § 170.215(b)(1)(ii) and incorporate it by reference in § 170.299. Additionally, because the FHIR US Core IG v3.1.1 is currently referenced (via cross-references to § 170.215(a)(2)) in § 170.315(g)(10)(i)(A) and (B), (ii)(A) and (iv)(A), we propose to revise each of those sections to instead cross-reference § 170.215(b)(1). We note that we propose to restructure the standards in § 170.215 to better categorize API standards and to enable simultaneous use of different versions of IGs for a set period of time. For example, we propose to categorize the US Core IGs v3.1.1 in § 170.215(b)(1)(i) as part of a group of standards for constraining and profiling data elements, and we propose that the adoption of this standard expires on January 1, 2025. We propose to include the US Core IG v5.0.1 in this same group in § 170.215(b)(1)(ii). Together, this recategorization and establishment of an adoption expiration date would give health IT developers of certified health IT the option to use either IG for a period of time and establish a concrete date for when they would need to implement and support the newer version in their Health IT Modules. We propose similar changes to other standards listed in § 170.215 and address those proposals in subsequent sections of this preamble.

c. FHIR Endpoint for Service Base URLs

The ONC Cures Act Final Rule established the API Conditions and Maintenance of Certification requirements in 45 CFR 170.404(b)(2), which contain a specific provision that, for Health IT Modules certified to the certification criterion in § 170.315(g)(10), certain “service

base URLs"— otherwise known as "endpoints"— must be publicly published for all customers in a machine-readable format at no charge (85 FR 25764 – 25765). These electronic endpoints are the specific locations on the internet that make it possible for apps to access EHI at the patient's request.

In the ONC Cures Act Proposed Rule, we indicated that we "strongly encourage API Technology Suppliers, health care providers, HINs and patient advocacy organizations to coalesce around the development of a public resource or service from which all stakeholders could benefit" (84 FR 7494). However, we decided against naming specific standards in the ONC Cures Act Final Rule and did not establish requirements for the content or format of the endpoint lists to provide industry an opportunity to coalesce on specifications. We finalized § 170.404(b)(2) to require that Certified API Developers must make their service base URLs freely accessible and in a machine-readable format at no charge.

Since the ONC Cures Act Final Rule was published, we have found that developers with publicly discoverable endpoint lists have defined their own, bespoke publication approaches and unique formats. There is variability across developers of certified health IT in the format they are using to publish their service base URLs, indicating that the industry has not coalesced around a common framework or approach. Research conducted through ONC's Lantern Project confirms that this variability among developers of certified health IT is hindering maturation of a vibrant app ecosystem for patients and the healthcare community, which is a primary goal of ONC policy and regulations in this area.[303]

The inconsistent implementation of this requirement has rendered important data meant to facilitate connections to endpoints difficult to access.[304] Specifically, the organization(s) associated with an endpoint is not always available, and even where available, is not always available in a format that can be readily used. Patient-facing apps require access to these

---

[303] https://www.healthit.gov/buzz-blog/healthit-certification/shining-a-light-on-fhir-implementation-progress-toward-publishing-fhir-endpoints.
[304] https://www.healthit.gov/news/events/onc-lantern-workshop.

endpoints to provide patients access to information maintained by specific provider organizations; without standardized formats and an ability to search for endpoints, patients are unable to find which endpoint(s) refer to their provider. Similar barriers exist for others involved in healthcare seeking to leverage apps for interoperability.

Additionally, it is difficult to map multiple, unique organizations to endpoints. Experience to-date indicates that the name of the organization associated is typically formatted as free text (i.e., String), with no unique identifier to know which organization is being supported by the service base URL. For example, the organization name given by the endpoint, "Acme Children's Hospital," could be mapped to six possible organization names, including "Acme's Children's Hospital Anesthesiology," "Acme's Children's Hospital - Urgent Care," and "Acme Children's Hospital – Ambulatory Care Center Pharmacy," among others. This endpoint might map to any one of these organizations, making a definite match difficult to determine.

Even more complicated is the possibility of a single endpoint representing all six of the "Acme Children's Hospital" organizations in the example above. A single String is unable to represent the complexity of healthcare systems, where a system can contain many subsystems, or where a FHIR API URL can support a set of systems. Including all organizations that are serviced by an endpoint is important for discovery of which endpoint serves a particular health care provider, which in turn would allow the user to access the relevant EHI through that endpoint. Having all healthcare organizations serviced by the endpoint accessible and in a standardized format would help app developers easily fetch information to enable patients and other users to access, exchange, and use information.

We propose to revise the requirement in § 170.404(b)(2) to include new data format requirements. We anticipate that these new specifications would establish standards for industry adoption and better facilitate patient access to their health information. In the revised § 170.404(b)(2), we also propose to incorporate the following existing requirements in § 170.404(b)(2)(i) and (ii): a Certified API Developer must publish service base URLs "For all of

its customers regardless of whether the Health IT Modules certified to § 170.315(g)(10) are centrally managed by the Certified API Developer or locally deployed by an API Information Source;" and publish these service base URLs "at no charge" as part of proposed § 170.404(b)(2).

In the "Service base URL publication" requirements in § 170.404(b)(2)(i), we propose to require that service base URLs must be formatted in FHIR "Endpoint" resource format according to the standard adopted in § 170.215(a). Additionally, in § 170.404(b)(2)(ii), we propose to require that organization details such as name, location, and provider identifiers (e.g., National Provider Identifier (NPI), CMS Certification Number (CCN), or health system ID) for each service base URL must be published in US Core "Organization" resource format according to the implementation specifications adopted in § 170.215(b)(1) (we note that elsewhere in this proposed rule in section III.C.7.b we propose to move US Core IGs to § 170.215(b)(1)), with the "Organization.endpoint" element referencing the service base URLs managed by this organization.

We propose these formats because they are based on the FHIR Release 4 and US Core IG industry standards that are already adopted for use in the Program in § 170.315(g)(10). We are specifically proposing the FHIR "Endpoint" resource because it is used for representing technical endpoint details and contains a required "address" element that, according to the FHIR R4 standard, contains "the technical base address for connecting to this endpoint." Certified API Developers would be able to populate this element, in each of their published "Endpoint" resources, with a service base URL that can be used by patients to access their electronic health information.

We additionally propose the US Core "Organization" resource because it can be used to represent important contextual information around a service base URL. The US Core "Organization" resource contains an optional "endpoint" element that can be used to reference

"technical endpoints providing access to services operated for the organization."[305] To standardize a link between published "Endpoint" resources and organizational details relating to the organization that services these endpoints, we propose to require, in § 170.404(b)(2)(ii)(A), that this optional "endpoint" element be populated on publicly published "Organization" resources and that they reference the "Endpoints" managed by the organization. We note that "publicly published" means that the information is made publicly available and note that ONC will host a link to developers' service base URL list on the Certified Health IT Product List (CHPL) or another website hosted by ONC. This information would give the public a standard way of knowing how published "Endpoint" and published "Organization" resources are linked and which organizational details apply to which service base URLs.

Additionally, the US Core "Organization" resource contains a "mandatory" element called "name" that contains a "name used for the organization." In addition to this required element, we propose in § 170.404(b)(2)(ii)(B) to require Certified API Developers to make available "must support" elements of organization location and provider identifier(s) using the US Core "Organization" resource. An organization's location could be an address that is populated in the "address" element of the US Core "Organization" resource; and a provider identifier could be a National Provider Identifier (NPI), Clinical Laboratory Improvement Amendments (CLIA) number, or other health system ID populated in the "identifier" element. Altogether, this information helps contextualize service base URLs and enables application developers to more easily and consistently provide patient access to their electronic health information. We welcome comment on this proposal and whether additional data should be required as part of organizational details.

Finally, we propose, in § 170.404(b)(2)(iii)(A), to require that these resources be collected in a FHIR "Bundle" resource that the Certified API Developer would publicly publish. According to the FHIR specification, a "Bundle" acts as "a container for a collection of

[305] https://www.hl7.org/fhir/organization.html.

resources" and is widely used in use cases like returning search results and grouping resources as part of a message exchange.[306] Given the broad use of the "Bundle" resource throughout the FHIR specification (e.g., FHIR search), we expect that most FHIR clients and FHIR application developers would be familiar with the "Bundle" resource and be able to parse "Bundle" resources electronically and extract relevant information from them for use in their application. Alternatively, we are considering a different format for requiring that the Endpoint and Organization resources be collected for publication. We are also considering the Newline Delimited JSON (ndjson) format. According to the ndjson specification, this format is convenient for publishing "structured data that may be processed one record at a time."[307] The ndjson format is an efficient way for machines to parse large amounts of data given that the entire file does not need to be read into memory before parsing. We expect that these "Endpoint" and "Organization" JSON resource lists may be large, depending on the developer of certified health IT's client base. We expect that most Certified API Developers will be familiar with this format because it is included as an underlying standard in the FHIR Bulk Data Access IG required for certification to § 170.315(g)(10). Given the simplicity of the ndjson standard, we also expect that most FHIR clients and FHIR application developers would easily be able to parse ndjson files electronically and extract relevant information from them for use in their application. We invite comment on whether we should finalize our proposal to adopt a requirement for Endpoint and Organization resources to be made publicly available according to the FHIR Bundle or if we should finalize the requirement to use a ndjson format.

We also propose, in § 170.404(b)(2)(iii)(B), that Certified API Developers ensure Endpoint and Organization resources remain current by reviewing this information quarterly and, as necessary, update the information. We recognize that as customers upgrade and install new health IT, data provided in the Endpoint and Organization resources will change. To serve its

[306] http://hl7.org/fhir/R4/bundle.html.
[307] http://ndjson.org/.

intended purpose, we believe this information should be updated regularly. We believe these resources must remain up to date to ensure application developers can easily and consistently provide patients access to their EHI. We note that a one-time publication of the developer's current list of endpoints for active customers upon certification to the § 170.315(g)(10) criterion will only meet initial certification requirements, and we propose to establish in § 170.404(b)(2)(iii)(B) a requirement that Certified API Developers maintain this information over time. We also note that failure to maintain the service base URLs and ensure the associated organization information remains up to date and free of errors or defects on a quarterly basis would be considered a violation of this Condition and Maintenance of Certification requirement and may result in corrective action. We clarify that any endpoint or organization information that is out of date, incomplete, or otherwise unusable for more than 90-days would be considered in violation of this proposed requirement. However, we request comment whether we should shorten this period of time to 60 or 30 days.

We believe that further standardization will better enable individuals to connect to their EHI, and we believe that this requirement will also support other industry efforts to leverage and scale endpoint directories. For example, the FHIR community, through the Argonaut Project, recently developed the "Patient-access Brands" conceptual model that specifies standardized formats for publishing endpoints and related organizational information.[308] Specifically, this model includes FHIR "Endpoint" and "Organization" resource profiles for FHIR formatting of endpoint and organization details. The model also specifies how these "Endpoint" and "Organization" resources can be related to each other in a way that allows app developers to fetch organization details related to an endpoint such as organization name, logo, location, aliases, and other brand details that would be recognizable to the patient. We invite comment on these proposals.

[308] https://hackmd.io/@argonaut/patient-access-brands.

d. Access Token Revocation

In the ONC Cures Act Final Rule, we established a requirement in § 170.315(g)(10)(vi) for Health IT Modules certified to § 170.315(g)(10) to be able to revoke an authorized application's access at a patient's direction (85 FR 25945). This required capability is intended to enable patients to "definitively revoke an application's authorization to receive their EHI until reauthorized, if ever, by the patient" (85 FR 25747). We noted in the ONC Cures Act Final Rule that we finalized § 170.315(g)(10)(vi) as a functional requirement to allow health IT developers the ability to implement it in a way that best suits their existing infrastructure and allows for innovative models for authorization revocation to develop (85 FR 25747). We understand that a lack of specificity in the current requirement has led to some confusion among health IT developers and application developers.

As part of health IT developers' implementation of these requirements, we have received feedback regarding the implementation of authorization revocation, specifically around the revocation of access tokens. Health IT developers have requested clarification regarding letting access tokens expire in lieu of immediate access token revocation for the purposes of certification testing. The OAuth 2.0 Token Revocation specification, RFC 7009, describes expiration of short-lived access tokens as a design option for authorization servers to revoke an application's access. This design option conforms with industry standard practice and may reduce health IT developer burden as the Health IT Module would not have to perform token introspection for each resource request nor maintain a database of valid access tokens.

We propose to revise the requirement in § 170.315(g)(10)(vi) to specify that a Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a patient's direction within 1 hour of the request. This requirement aligns with industry standard practice of short-lived access tokens as specified in Internet Engineering Task Force

(IETF) Request for Comments (RFC) 6819,[309] IETF RFC 7009,[310] and Section 7.1.3 of the SMART Application Launch Framework version 1.0.0, which states that "Access tokens SHOULD have a valid lifetime no greater than one hour. Confidential clients may be issued longer-lived tokens than public clients." This proposal would provide clarity and create a consistent expectation that developers revoke access within 1 hour of a request, regardless of their internal approach to fulfilling a patient's request to revoke access. This proposal would also assure patients that once requested, an application's access to their data would be revoked within 1 hour. This would also support situations where a patient may have an unexpected change in their privacy concerns and seek to curtail access to their information in as short a time as possible, especially regarding access by entities not regulated by the HIPAA Rules.

We considered a shorter timeframe, but we concluded that 1 hour would be both an appropriate expectation for developers to meet and would be consistent with industry standards for revocation of an application's access. We also expect that many or most developers would institute a process that results in revocation of access in a timeframe much less than 1 hour. Investigation into industry best practice leads ONC to believe that a 1-hour requirement to revoke an authorized application's access at a patient's direction is an appropriate baseline requirement. We invite comment on this proposal.

e. SMART App Launch 2.0

In the ONC Cures Act Final Rule, we adopted the HL7 FHIR SMART Application Launch Framework (SMART v1) Implementation Guide Release 1.0.0 implementation specification, a profile of the OAuth 2.0 specification, in § 170.215(a)(3) (85 FR 25741). SMART v1 provides reliable, secure authorization for a variety of app architectures through the use of the OAuth 2.0 standard. This Implementation Guide (IG) supports both required and optional requirements, known as the "SMART on FHIR Core Capabilities" (85 FR 25741). This

[309] Available at: https://www.rfc-editor.org/pdfrfc/rfc6819.txt.pdf.
[310] Available at: https://www.rfc-editor.org/pdfrfc/rfc7009.txt.pdf.

profile includes required support for "refresh tokens," "Standalone Launch," and "EHR Launch" capabilities from the SMART IG. Additionally, as part of adopting the implementation specification in § 170.215(a)(3), the ONC Cures Act Final Rule required support for optional capabilities including, "launch-ehr," "launch-standalone," "client-public," "client-confidentialsymmetric," "sso-openid-connect," "context-banner," "context-style," "context-ehr-patient," "context-ehr-encounter," "context-standalone-patient," "context-standalone-encounter," "permission-offline," "permission-patient," and "permission-user."

As part of the adopted implementation specification, we explicitly required mandatory support of the "SMART on FHIR Core Capabilities" for Program testing and certification, and we stated that by requiring the "permission-patient" "SMART on FHIR Core Capability" in § 170.215(a)(3), Health IT Modules presented for testing and certification to § 170.315(g)(10), via cross-references to § 170.215(a)(3), must include the ability for patients to authorize an application to receive their electronic health information (EHI) based on FHIR resource-level scopes (85 FR 25741, 25746). Practically, this means that patients would need to have the ability to authorize access to their EHI at the individual FHIR resource-level, from one specific FHIR resource (*e.g.,* "Immunization") up to all FHIR resources necessary to implement the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2). This capability gives patients increased control over how much EHI they authorize applications of their choice to receive. For example, if a patient downloaded a medication management application, they would be able to use these authorization scopes to limit the EHI accessible by the application to only information contained in FHIR "MedicationRequest" and "Medication" profile.

The SMART Application Launch Framework Implementation Guide Release 2.0.0 (SMART v2) Guide is the next major release of the SMART Application Launch Framework

IG.[311] The SMART v2 Guide iterates on the features of the SMART v1 Guide by including revisions aligning with industry consensus to provide technical improvements and reflect security best practices. The SMART v2 Guide technical enhancements improve the authentication and authorization security layer provided by the SMART v1 Guide and enables increased capabilities and functionality for individual control of EHI. Therefore, we propose to adopt the SMART v2 Guide in § 170.215(c)(2), and we propose that the adoption of the SMART v1 Guide in § 170.215(c)(1) would expire as of January 1, 2025. We clarify that both SMART v1 and SMART v2 will be available for purposes of certification where certification criteria reference § 170.215(c) until the expiration date of January 1, 2025, after which time only SMART v2 will be available for certification if we finalize our rule as proposed.

As part of this proposal, we propose to adopt several sections specified as "optional" in the SMART v2 Guide as "required" for purposes of the Program for certification criteria that reference § 170.215(c). Specifically, we propose to adopt all Capabilities as defined in "8.1.2 Capabilities," which include but are not limited to (1) backward compatibility mapping for SMART v1 scopes as defined in "3.0.2 Scopes for requesting clinical data;" (2) asymmetric client authentication as defined in "5 Client Authentication: Asymmetric (public key);" and granular scopes as defined in (3) "3.0.2.3 Finer-grained resource constraints using search parameters." Additionally, we propose to require support for the "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch" Capability Sets from "8.1.1 Capability Sets." Also, we propose to adopt token introspection as defined in "7 Token Introspection." Again, we clarify that for the period before January 1, 2025, Health IT Modules certified to certification criteria that reference § 170.215(c) may use either SMART v1 or SMART v2 for certification.

Further, we note that the SMART v2 Guide includes section 3.0.2.3 "Finer-grained resource constraints using search parameters," and associated "3.0.2.4 requirement for support"

[311] https://hl7.org/fhir/smart-app-launch/STU2/index.html.

and "3.0.2.5 experimental features," which present concepts for further development within the SMART v2 Guide. Together, these optional functionalities will enable more granular control for individuals, clinicians, and other users to share information with apps of their choice in more explicit ways. The granular scope functionality would empower patients and providers to share health data in a more granular fashion, which will improve confidence in the use of third-party apps by allowing app users to decide which specific type of EHI they share with the app. These functionalities would help address privacy and security concerns of third-party app access to health data and further patient empowerment by providing the ability to limit an app's access to a granular, minimum set of health data, as determined by the app user. We propose these sections for adoption as part of SMART v2 Guide with the understanding that either the SMART v2 Guide or another implementation guide such as the US Core Implementation Guide will define more specific requirements for finer-grained resource constraints using search parameters.

i. SMART v2 Guide New and Revised Features Proposed for Adoption

The SMART v2 Guide introduces new or revised requirements to the previous version of the implementation guide, SMART Guide v1. Major requirements new to the SMART v2 Guide include support for the OAuth 2.0 security extension Proof Key for Code Exchange (PKCE), as well as a revision of the scope syntax. The SMART v2 Guide includes requirements that both the EHR and all apps support the OAuth 2.0 security extension PKCE. PKCE is an industry standard security extension for OAuth 2.0 to mitigate the known security vulnerability of authorization code interception attacks.[312] The requirement of PKCE especially improves the security of native apps, or apps that operate from an individual's phone or tablet, which were particularly vulnerable to authorization code interception attacks.

Another major change included in the SMART v2 Guide is revision of the syntax of scopes provided to apps. To align with the FHIR interactions of "Create", "Read", "Update",

[312] https://www.oauth.com/oauth2-servers/pkce/.

“Delete”, “Search”, collectively known as “CRUDS,” scopes are constructed to consist of combinations of five types of permissions corresponding to the CRUDS interactions. The use of this CRUDS scope syntax permits improved patient choice for persistent access as more specific combinations of permissions can be granted to apps as opposed to the scope syntax used in the SMART v1 Guide, which only used two permission types of “read” and “write.”

New feature: PKCE

One of the major security improvements in the SMART v2 Guide is the requirement that all apps support the OAuth 2.0 security extension Proof Key for Code Exchange (PKCE). PKCE is designed to mitigate the known security vulnerability of authorization code interception attacks, with native apps especially targeted. According to IETF RFC 7636, the request for comment which defines the PKCE extension, this attack can be used to illegitimately obtain an access token from the authorization server and thus obtain server data in an unauthorized manner. PKCE mitigates this vulnerability by creating cryptographically random keys for every authorization request. The authorization server performs proof of possession of the secret key by the client. This mitigates the vulnerability as an attacker who intercepts the authorization code cannot redeem it for an access token as they do not possess the secret key associated with the authorization request.

Support for PKCE is important because PKCE makes health app access of patient health information more secure in a standardized manner. ONC recognizes healthcare participants and patients are interested in the secure use of health apps, including native apps, to access health information. PKCE support makes the granting of access to health information via health apps more secure by mitigating the known vulnerability of authorization code interception attacks. We believe the support of PKCE would further our goal of secure access of health information without special effort by further securing health app access, especially for native apps. Therefore, we propose to require the support of PKCE as specified in the SMART v2 Guide. We invite comment on this proposal.

New Feature: CRUDS scope syntax

Another major update in the SMART v2 Guide is the revision of the scope syntax to align with the FHIR REST API interactions for FHIR resources. Previously in the SMART v1 Guide, scope syntax for FHIR resources was delineated in terms of combinations of "read" and "write" permissions. The SMART v2 Guide revises this scope syntax by splitting "read" permissions into two types of permissions which correspond to FHIR REST API interactions, "Read" and "Search." Similarly, the "write" permissions from the SMART v1 Guide are split into "Create," "Update," and "Delete." This alignment of scope syntax to the FHIR REST API interactions permits Health IT Module authorization servers to provide greater specificity regarding which permissions are granted in scopes to apps and has the benefit of improved technical clarity to health IT and application developers. This additional specificity for scopes also improves a patient's control over how an app accesses their health data by clarifying for the patient what specific type of API interactions are permitted to the app. For example, under this new syntax the patient could specifically permit an app "read" access to a FHIR resource but deny "search" access for the same FHIR resource.

Currently, as stated in 85 FR 25742, the § 170.315(g)(10) certification criterion only requires health IT developers to support "read" capabilities according to the standard and implementation specifications adopted in § 170.215(a) and in § 170.215(b)(1), including the mandatory capabilities described in "US Core Server CapabilityStatement." We will continue this policy for § 170.315(g)(10), as specified in the SMART v2 Guide, which would include "Read" and "Search" permissions to be supported for certification to the § 170.315(g)(10) criterion. We welcome comment on these scopes and are interested in the public's experience with other aspects of CRUDS.

ii. SMART v2 Optional Features Proposed as Required by ONC

We propose to require all Capabilities as defined in "8.1.2 Capabilities" and the "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch" Capability Sets from

"8.1.1 Capability Sets." The following section identifies optional component pieces of 8.1.2 Capabilities and optional profiles of the implementation guide that we propose to be required.

First, the SMART v2 Guide introduces functionality specified as optional in the implementation guide. We propose to make several of these optional functionalities required as part of the proposed implementation specification, and therefore required for certification criteria that reference proposed § 170.215(c)(2). First, one such optional functionality is the mapping between SMART v1 Guide and SMART v2 Guide scopes for the purpose of backward compatibility. We propose to require support of this mapping for the purposes of interoperability between implementations of the SMART v1 Guide and the SMART v2 Guide. As part of the current "Authentication and authorization" requirements in § 170.315(g)(10)(v) for the certification criterion in § 170.315(g)(10), Health IT Modules must support authentication and authorization during the process of granting access to patient data. Part of the authorization process involves an application requesting permission to access patient data in the form of OAuth 2.0 scopes as specified in the SMART v1 Guide. The SMART v2 Guide changes the format of these scopes, making SMART v2 scopes not directly compatible with SMART v1 scopes. The SMART v2 Guide provides a mapping of SMART v1 scopes to SMART v2 scopes for the purposes of backward compatibility. For the purposes of interoperability with existing API deployments implementing the SMART v1 Guide, we propose to require that servers advertise the "permission-v1" capability in their "well-known/smart-configuration" discovery document, return SMART v1 scopes when SMART v1 scopes are requested and granted, and process SMART v1 scopes according to the backward compatibility mapping specified in SMART v2 Guide "3.0.2 Scopes for requesting clinical data."

Second, the SMART v2 Guide introduces an optional profile for authorization servers to support asymmetric client authentication for confidential clients. We propose to require Health IT Modules support asymmetric client authentication as an option for confidential clients during the process of authentication and authorization when granting access to patient data. This

proposed requirement would align with the security practices of industry as evidenced by the SMART v2 Guide's recommendation that asymmetric client authentication be used when available and improves interoperability for clients by making this API security feature consistently available across § 170.315(g)(10)-certified APIs. Client authentication is the process by which the authorization server verifies the identity of the client requesting authorization. The SMART v1 Guide specifies client authentication in terms of symmetric client authentication, in which authentication is based on a secret key shared by both the authorization server and the client. The SMART v2 Guide introduces a new profile for client authentication, asymmetric client authentication. Asymmetric client authentication relies upon public key cryptography for authentication, with the client having public and private keys. The SMART v2 Guide specifies asymmetric client authentication as an optional profile but recommends clients use asymmetric client authentication when available. Given this recommendation of the SMART v2 Guide, we believe there would be a security benefit for servers to provide clients the option to use asymmetric client authentication over symmetric client authentication. Additionally, clients would benefit from having asymmetric client authentication supported by authorization servers consistently in a standardized way. Therefore, we propose to require Health IT Modules support asymmetric client authentication as defined in "5 Client Authentication: Asymmetric (public key)" as an option for confidential clients during the process of authentication and authorization when granting access to patient data. We also propose to require Health IT Modules advertise the "client-confidential-asymmetric" capability in their "well-known/smart-configuration" discovery document.

Third, the SMART v2 Guide also introduces a new optional feature of granular scope constraints using search parameters. This feature uses the FHIR REST API search parameter syntax to specify permissions more granular than the FHIR resource level, which was the maximum granularity of scopes in the SMART v1 Guide. By using search parameters associated with a FHIR resource, a scope can be made to apply only to a specific subset of a FHIR resource

and therefore the permissions granted to the client via such a scope would be limited to this subset. For example, the SMART v2 Guide mentions how an authorization server can provide a scope for laboratory Observations using the "category" search parameter instead of all Observation resources. This granular scope functionality would empower patients with greater control over what types of information applications of their choice receive from a Health IT Module. This would also improve patients' ability to select granular permissions to grant persistent access to applications. However, the SMART v2 Guide leaves this new functionality as optional and does not specify specific search parameter requirements for finer-grained scope constraints. We propose to require "3.0.2.3 Finer-grained resource constraints using search parameters" with the clarification that Health IT Modules certified to § 170.315(g)(10) must minimally be capable of handling finer-grained scopes using the "category" parameter for (1) the Condition resource with Condition sub-resources Encounter Diagnosis, Problem List, and Health Concern and (2) the Observation resource with Observation sub-resources Clinical Test, Laboratory, Social History, SDOH, Survey, and Vital Signs. We anticipate that the US Core IG will provide guidance for developers to support a minimum number of search parameters and this minimum list will be consistent with the optional scopes described in section "3.8 Future of US Core" of the US Core IG v6.0.0. We invite comment on this proposal, and we seek comment on whether we should expand the minimum search parameters for Health IT Modules certified to § 170.315(g)(10).

Fourth, the SMART v2 Guide revises how capabilities are categorized. The "SMART Core Capabilities" in the SMART v1 Guide define capabilities supported by the server and are made available to inform clients of supported functionality. "Capabilities" are grouped into "Capability Sets" to define the functionalities required for a specific use case. The SMART v2 guide restructures how "Capabilities" are organized, and no longer includes "SMART Core Capabilities." Instead, the SMART v2 Guide includes a list of "Capabilities" and "Capability Sets." To align with the capabilities proposed for adoption and the current § 170.315(g)(10)

requirement, via cross-reference to the existing § 170.215(a)(3), for Health IT Modules to support "SMART Core Capabilities" as specified in the SMART v1 Guide, we propose to require the following "Capability Sets" from the SMART v2 Guide of "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch" in addition to the "8.1.2 Capabilities," enumerated in the SMART v2 Guide, including the capabilities of: "launch-ehr," "launch-standalone," "authorize post," "client-public," "client-confidential-symmetric," "client-confidential-asymmetric," "sso-openid-connect," "context-banner," "context-style," "context-ehr-patient," "context-ehr-encounter," "context-standalone-patient," "context-standalone-encounter," "permission-offline," "permission-online," "permission-patient," "permission-user," "permission-v1," and "permission-v2." We note that "context-banner," and "context-style," which are capabilities for supporting user interface integration with the application, are respectively optional and "experimental" features in the SMART v2 Guide; however, we propose to maintain them as required based on the previously adopted requirements for the criterion in § 170.315(g)(10). We seek comment on whether these should be maintained as required or if we should instead modify this requirement to designate "context-banner," and "context-style," as optional, in alignment with the SMART v2 Guide. We propose to require the "permission-offline" and "permission-online" capabilities as this functionality would empower individuals, clinicians, and other users to deny authorization for online or offline access. Additionally, we request specific comment on the inclusion of all of the aforementioned aspects of the SMART v2 Guide and any related benefits or challenges of finalizing as proposed.

Additionally, the SMART v2 Guide introduces a new requirement to support POST-based authorization for the client authorization request. This new requirement in the SMART v2 Guide is adapted from the OpenID Connect Core specification and is related to the requirement in § 170.315(g)(10)(v)(A)(*1*)(*i*), which requires a Health IT Module to support authentication and authorization during the process of granting access to patient data according to the OpenID Connect Core standard. The SMART v2 Guide includes the "authorize-post" capability under

"Capabilities" for servers to indicate support for this requirement. To align with this new technical requirement in SMART v2 and the authorization and authentication requirement in § 170.315(g)(10)(v)(A)(*1*)(*i*), we propose to require the "authorize-post" capability.

We propose to require the following optional capabilities as required: "permission-v1"; "permission-v2"; "client-confidential-asymmetric;" and "authorize-post" from section "8.1.2 Capabilities" to support new technical requirement for backward compatibility with SMART v1 Guide scopes, SMART v2 Guide granular scopes, asymmetric client authentication, and support for authorization via HTTP POST respectively. In sum, we propose to require all Capabilities as defined in "8.1.2 Capabilities" and the "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch" Capability Sets from "8.1.1 Capability Sets."

The SMART v2 Guide also defines a profile for OAuth 2.0 token introspection. As described in the ONC Cures Act Final Rule (85 FR 25748), commenters on the ONC Cures Act Proposed Rule requested a requirement in the § 170.315(g)(10) criterion for token introspection, a process which defines how an authorization server can be queried for information about a token. In response to this feedback, ONC subsequently finalized a token introspection requirement in § 170.315(g)(10)(vii) but did not specify a standard and encouraged industry to coalesce around a common standard, such as OAuth 2.0 Token Introspection (RFC 7662). The SMART v2 Guide introduces a profile for OAuth 2.0 Token Introspection in "7 Token Introspection." We believe a standardized process for token introspection would improve interoperability for FHIR clients and resource servers by defining specific expectations around what information a Health IT Module's authorization server returns about a token when queried by a client or resource server. To facilitate such interoperability, we propose to revise the token introspection requirement in § 170.315(g)(10)(vii) to state, "A Health IT Module's authorization server must be able to receive and validate tokens it has issued in accordance with an implementation specification in § 170.215(c)." This requirement would ensure that a Health IT

Module's authorization server must be able to receive and validate tokens it has issued in accordance with SMART v2 Guide "7 Token Introspection."

Finally, we again note that we propose to restructure the standards listed in § 170.215 to better categorize API standards and to enable simultaneous use of different versions of IGs for a set period of time. We propose to categorize the SMART v1 Guide in § 170.215(c)(1) as part of a group of standards that enable client applications to access and integrate with data systems, and we propose that the adoption of this standard expires on January 1, 2025. In so doing, we propose to move the implementation specification currently found in § 170.215(a)(3) to § 170.215(c)(1). We propose the SMART v2 Guide in this same group in § 170.215(c)(2). Together, this recategorization and establishment of an expiration date for § 170.215(c)(1) would give health IT developers of certified health IT the option to use either SMART Guide version for a period of time, and it would establish a concrete date for when they would need to implement and support the newer version in their Health IT Modules certified to certification criteria that reference § 170.215(c).

8. Patient Demographics and Observations Certification Criterion in § 170.315(a)(5)

Background

In the 2015 Edition Final Rule (80 FR 62601), ONC required the recording, capture, and access to a patient's sex, sexual orientation, and gender identity for Health IT Modules certified to the "Demographics" certification criterion (§ 170.315(a)(5)) (80 FR 62747). This rule also defined a required set of standardized terminology to represent each of these data elements (80 FR 62618-62620). Since then, ONC has received recommendations through the Health Information Technology Advisory Committee (HITAC) and public feedback that the current terms and terminologies used to represent sex, gender identity, and sexual orientation are limited and need to be updated.

Meanwhile, the healthcare industry had similarly taken note of the need for precision for ideas encompassed in terms such as "sex" and "gender" and launched the Gender Harmony

Project[313] to capture these concepts consistently within healthcare. The Gender Harmony Project introduced for the health IT context the concepts "Sex for Clinical Use" (SFCU), "Recorded Sex or Gender," (RSG), "Name to Use," and "Pronouns." The Gender Harmony Project defines Sex for Clinical Use as a category that is based on clinical observations typically associated with the designation of male and female; Name to Use provides the name that should be used when addressing or referencing the patient; Recorded Sex or Gender is the documentation of a specific instance of sex and/or gender information; and Pronouns are determined by a patient and used when referring to the patient in speech, clinical notes and in written instructions to caregivers (e.g., she/her/hers or they/them.) Sex for Clinical Use, Name to Use, Recorded Sex or Gender, and Pronouns are new concepts currently not present in the certification criteria.

Proposals

In this section, we outline our proposals to modify the "Demographics" certification criterion (§ 170.315(a)(5)). We propose to rename § 170.315(a)(5) from "Demographics" to "Patient Demographics and Observations," to acknowledge that the data elements being proposed are broader than demographics information, as we look to promote a more inclusive healthcare system.

We propose to add the data elements "Sex for Clinical Use" in § 170.315(a)(5)(i)(F), "Name to Use" in § 170.315(a)(5)(i)(G), and "Pronouns" in § 170.315(a)(5)(i)(H) to the "Patient Demographics and Observations" certification criterion (§ 170.315(a)(5)). This addition reflects concepts developed by the HL7 Gender Harmony Project and help promote inclusivity in care delivery.

We propose to revise the terminology standards specified for "Sex" in § 170.315(a)(5)(i)(C). ONC has received significant feedback reflecting the need to be more inclusive in the terminology representing the data element. As such, ONC proposes to revise the

[313] https://confluence.hl7.org/display/VOC/The+Gender+Harmony+Project.

fixed list of terms for "Sex" in § 170.315(a)(5)(i)(C), which are represented by HL7® Value Sets for AdministrativeGender and NullFlavor in § 170.207(n)(1). We propose to ultimately replace § 170.207(n)(1) with the SNOMED CT code set proposed in § 170.207(n)(2). We refer the readers to section III.C.1 of the rule for additional information about the proposed change to the terminology standard. In order to be less disruptive to developers of certified health IT, we propose to provide flexibility and allow recording the element using the specific codes represented in § 170.207(n)(1) for the time period up to and including December 31, 2025, to provide enough time to transition their health IT systems to SNOMED CT® by January 1, 2026. By having § 170.207(n)(1) expire at the end of 2025 and adding (n)(2) as a requirement for Health IT Modules certified to § 170.315(a)(5) beginning January 1, 2026, we propose to enable health IT developers to specify any appropriate value from the SNOMED CT® code set with the standard specified in § 170.207(n)(2).

Additionally, we propose to replace the terminology standards specified for Sexual Orientation in § 170.315(a)(5)(i)(D), and Gender Identity in § 170.315(a)(5)(i)(E). ONC has received significant feedback reflecting the need to be more inclusive in the terminology representing each of these data elements. As such, ONC proposes to revise the fixed list of terms for Sexual Orientation in § 170.315(a)(5)(i)(D), and Gender Identity in § 170.315(a)(5)(i)(E), which are represented by SNOMED CT and HL7® Value Set for NullFlavor in § 170.207(o)(1) and (2), and ultimately replace it with the SNOMED CT code set specified in § 170.207(o)(3). We refer the readers to section III.C.1 (USCDI) of the rule for additional information about the proposed change to the terminology standard.

We further propose to set an expiration date of January 1, 2026, for the adoption of the values sets referenced in § 170.207(o)(1) and (o)(2). This will allow the use of either the value sets in § 170.207(o)(1) and (o)(2) or the standard proposed in § 170.207(o)(3) beginning on the effective date of a final rule and transitioning to allow only the use of the proposed standard in § 170.207(o)(3) after December 31, 2025. Consistent with our proposals in sections III.A and

III.C.11, developers of certified health IT with Health IT Modules certified to criteria that reference § 170.207(o)(1) or (o)(2) would have to update those Health IT Modules to § 170.207(o)(3) and provide them to customers by January 1, 2026.

We also propose to add Sex for Clinical Use (SFCU) as a new data element in § 170.315(a)(5)(i)(F). SFCU is a category based upon clinical observations typically associated with the designation of male and female. It supports context specificity, is derived from observable information, and is preferably directly linked to the information this element summarizes. SFCU represents a patient's sex relevant to a specific clinical setting. This is valuable when providing care for a patient whose condition or treatment is dependent on their sex as determined by observing and evaluating, for example, a patient's hormonal values, organ inventory, genetic observations, or external genital morphology. SFCU may differ from a patient's sex as recorded on a birth certificate or driver's license. We further clarify, that while there may be multiple values of Sex for Clinical Use tied to different events, such as requesting a laboratory test or imaging study, we propose to require health IT developer be able to record at least one value of SFCU. Additionally, in order to align with current industry practice and to provide flexibility to health IT developers, we propose that health IT be capable of recording SFCU using the LOINC® terminology code set standard specified in proposed § 170.207(n)(3).

We propose to add new data elements Name to Use in § 170.315(a)(5)(i)(G) and Pronouns in § 170.315(a)(5)(i)(H), respectively, to advance the culturally competent care for lesbian, gay, bisexual, transgender, queer, intersex, asexual, and all sexual and gender minority (LGBTQIA+) people. Multiple values for a given patient may be valid over time. For the purposes of this proposal, we require at least one value for Pronouns and Name to Use be recorded. Additionally, in order to align with current industry practice and to provide flexibility to health IT developers, we propose that health IT be capable of recording Pronouns using the LOINC® terminology code set standard specified in proposed § 170.207(o)(4).

In addition to the other data elements proposed in this section, the HL7 Gender Harmony Project created an element named Recorded Sex or Gender (RSG). RSG documents a specific instance of sex and/or gender information. RSG is considered a complex data element that includes provision for a sex or gender value, as well as reference to the source document where the value was found, whereas Sex is a simple data element. RSG provides an opportunity for health IT developers to differentiate between sex or gender information that exists in a document or record, from Sex for Clinical Use (SFCU) which is designed to be used for clinical decision-making.

Given the work undertaken by the Gender Harmony Project to develop an implementation guide that would work with all HL7 product families, we request comment on the following options we could pursue for a final rule.

Option 1 (proposed in regulation text): Require health IT developers to record Sex as proposed in § 170.315(a)(5)(i)(C). This would enable Sex to be recorded in accordance with the SNOMED CT standard, specified in § 170.207(n)(2), as well as the standard specified in § 170.207(n)(1) for the time period up to and including December 31, 2025. It would mean, however, that health IT developers would not be required to differentiate between sex and/or gender information when recording the information.

Option 2: Replace Sex with Recorded Sex or Gender in § 170.315(a)(5)(i)(C). Adopt the data element Recorded Sex or Gender as specified in the HL7 Gender Harmony Project. This would require health IT developers to capture the source documents while recording sex and/or gender information. Recorded Sex or Gender would further provide an opportunity for health IT developers to differentiate between sex or gender information that exists in a document or record, from Sex for Clinical Use (SFCU), which is designed to be used for clinical decision-making.

In preparing comments, we encourage commenters to fully review our proposed certification criterion in § 170.315(a)(5) and USCDI v3. Notably, if we were to adopt RSoG in a

final rule as an alternative to Sex for the proposed certification criterion in § 170.315(a)(5), then health IT developers would be required to ensure that they perform the necessary transformations to meet the requirements associated with USCDI v3 and associated certification criteria. We highly encourage commenters to express their perspectives and explicitly note their preferred option in comments.

Base EHR Definition

We propose to revise and update the "demographics" certification criterion (§ 170.315(a)(5)), which we propose to rename "patient demographics and observations," and which is included in the Base EHR definition in § 170.102. This means Health IT Modules would need to be updated to accommodate the additional requirements in the "Patient Demographics and Observations" certification criterion in order to meet the Base EHR definition.

In addition, because December 31, 2022, has passed, we propose to revise the Base EHR definition by removing the reference to § 170.315(g)(8) in § 170.102(3)(ii) and replacing the references to § 170.315(g)(10) in § 170.102(3)(ii) and (iii) with a single reference to § 170.315(g)(10) in § 170.102(3)(i).

9. Updates to Transitions of Care Certification Criterion in § 170.315(b)(1)

In this section, we outline our proposals to update the Transitions of Care certification criterion (§ 170.315(b)(1)) to align it with changes made in USCDI v3, which we propose to adopt in § 170.213(b).

We propose to replace the fixed value set for the USCDI data element "Sex" and instead enable health IT developers to specify any appropriate value from the SNOMED CT code set with the standard specified in § 170.207(n)(2). Health IT developers can continue using the specific codes for Sex represented in § 170.207(n)(1) for the time period up to and including December 31, 2025. We note that these dates are proposed for the adoption of the associated standards in § 170.207(n), including the expiration of the adoption of the standard in

§ 170.207(n)(1) on January 1, 2026. Consistent with our proposals in sections III.A and III.C.11, developers of certified health IT with Health IT Modules certified to criteria that reference § 170.207(n)(1) would have to update those Health IT Modules to § 170.207(n)(2) and provide them to customers by January 1, 2026.

Finally, we propose a conforming update to § 170.315(b)(1) to update the listed minimum standard code sets for Problems in § 170.315(b)(1)(iii)(B)(*2*). We propose that Health IT Modules certified to § 170.315(b)(1) use, at a minimum, the version of the standard specified in § 170.207(a)(1). We invite comment on these proposals.

10. Patient Requested Restrictions Certification Criterion

Through our efforts to advance interoperability across a nationwide health IT infrastructure, ONC has specifically focused on how health IT can support efforts to reduce healthcare disparities and provide both insights and tools for the purposes of measuring and advancing health equity. This includes specific steps to expand the capabilities of health IT to capture and exchange data that is essential to supporting patient-centered clinical care that is targeted to supporting a patient's unique needs. However, as ONC pursues policies intended to improve the interoperability and sharing of data through adoption of standards-based certification criteria and implementation specifications, we are aware of the imperative to protect health data privacy. This need is compounded by the inclusion of new data elements in the USCDI that are intended to support advancement in health equity, but which also may increase data sensitivity because of the potential for bias or stigmatized care. We believe the need to protect sensitive health information is foundational to a health equity by design principle not only to protect patient privacy, but also to mitigate the risk of any unintended negative impact on an individual resulting from the disclosure of sensitive health information.

We are also cognizant that identifying which health data are defined as "sensitive" may vary across federal or state laws, and may further vary based on an individual patient's perspective. Thus, the concept of "sensitive data" is dynamic and specific to the individual.

Patient populations that have historically been subject to discrimination may identify a wide range of demographic information as sensitive, including race, ethnicity, preferred language, sex, sexual orientation, gender identity, and disability status. Efforts to support whole patient care and expand the capture of social, psychological, and behavioral health information have led to advancements in standards for representation of social determinants of health (SDOH). We must also keep in mind that the capture and exchange of SDOH data includes the potential risk for discrimination or misuse.

Advances in genetic testing and genomic research offer opportunities for early intervention and preventative care, but again, they represent a potential risk that may not be fully addressed by current privacy laws. Finally, there are types of clinical information that could impact the patient if disclosed, such as reproductive health, behavioral health, and substance abuse information.

The HIPAA Privacy Rule provides individuals with several rights intended to empower them to be more active participants in managing their health information. These include the right to access certain health information maintained about the individual; the right to have certain health information amended; the right to receive an accounting of certain disclosures; the right to receive adequate notice of a covered entity's privacy practices; the right to agree or object to, or authorize, certain disclosures; the right to request restrictions of certain uses and disclosures; and provisions allowing a covered entity to obtain consent for certain uses and disclosures.[314]

Under the HIPAA Privacy Rule, covered entities as defined in 45 CFR § 164.530(i) are required to allow individuals to request a restriction on the use or disclosure of their PHI for treatment, payment, or health care operations and to have policies in place by which to accept or deny such requests (See 45 CFR § 164.522(a)(1)(i)(A)). The HIPAA Privacy Rule does not specify a particular process to be used by individuals to make such requests or for the entity to accept or deny the request. However, we believe that certified health IT should—to the extent

[314] See 45 CFR. §§ 164.524, 164.526, 164.528, 164.520, 164.510, 164.508, 164.522, and 164.506(b), respectively.

feasible——support covered entities so they can execute these processes to protect individuals' privacy and to provide patients an opportunity to exercise this right.

Patient-directed privacy of data the patient deems sensitive requires attention to specific challenges from both a technology and a policy perspective, which we recognize cannot be easily solved. However, as we intended with the ONC Cures Act Final Rule, we believe there may be approaches that could, at a minimum, support the advancement of health IT tools to support discrete parts of these privacy workflows.

We are therefore proposing a new certification criterion, an addition to ONC's Privacy and Security Framework under the Program, and a revision to an existing certification criterion to support additional tools for implementing patient requested privacy restrictions.

a. Patient Right to Request a Restriction New Criterion – Primary Proposal

We propose to adopt a new certification criterion specifically in support of the HIPAA Privacy Rule's "right to request a restriction" on certain uses and disclosures (See also 45 CFR 164.522(a)). We propose to add the new certification criterion "patient requested restrictions" in § 170.315(d)(14) to enable a user to implement a process to restrict uses or disclosures of data in response to a patient request when such restriction is agreed to by the covered entity. We propose that this new criterion in § 170.315(d)(14) would be standards-agnostic, allowing health IT developers seeking to certify a Health IT Module to the criterion flexibility in how they design these capabilities so long as they meet the functional requirements described for certification. We specifically intend the proposed § 170.315(d)(14) to advance the technological means to support clinicians and other covered entities when honoring patient requests for the restriction of uses or disclosure of PHI through certified health IT.

We propose to add the following in § 170.315(d)(14) for this new criterion "patient requested restrictions":

- For any data expressed in the standards in § 170.213, enable a user to flag whether such data needs to be restricted from being subsequently used or disclosed; as set forth in 45 CFR § 164.522; and
- prevent any data flagged pursuant to paragraph (d)(14)(i) of this section from being included in a subsequent use or disclosure for the restricted purpose.

We propose that "enabl[ing] a user to flag" means enabling the user of the Health IT Module to indicate that a request for restriction was made by the patient and that the user intends to honor the request. In the case of integration with a Health IT Module certified to the revised criterion in § 170.315(e)(1) discussed in this section, that request made by the patient could be in part automated for requests made through an internet-based method. However, the functionality under the proposed new criterion in § 170.315(d)(14) must include the ability for the user to indicate a request made via other means. We note that such "flags" may leverage use of security labels like those included in the HL7 data segmentation for privacy (DS4P) implementation guides discussed in section III.C.10.b, or other data standards such as provenance or digital signature specifications[315]. The use of such standards or specifications would be at the discretion of the health IT developer. The health IT developer would have the flexibility to implement the "enable a user to flag" functionality in the manner that works best for their users and systems integration expectations.

We propose that the developer of a certified Health IT Module, under this standards-agnostic approach, would have the flexibility to implement the restriction on the inclusion in a subsequent use or disclosure via a wide range of potential means dependent on their specific development and implementation constraints (e.g., flagged data would not be included as part of a summary care record, not be displayed in a patient portal, or not be shared via an API).

---

[315] For example, the USCDI v3 includes a provenance data class (https://www.healthit.gov/isa/uscdi-data-class/provenance#uscdi-v3) and submissions in ISA include digital signature as a potential addition to provenance within the USCDI: https://www.healthit.gov/isa/uscdi-data/signature. Further specifications for provenance data and digital signatures in the context of FHIR-based transactions are also referenced in ISA: https://www.healthit.gov/isa/representing-data-provenance.

We welcome public comment on this proposal. We also direct readers to section III.C.10.b of this section in which we propose and seek comment on an alternative to leverage security label standards as a source taxonomy for the "flag" applied to the data for the new criterion in § 170.315(d)(14).

We also propose to modify the Privacy and Security Framework in § 170.550(h) to add the proposed new criterion. Specifically, we propose to modify § 170.550(h)(iii) in reference to the certain of "care coordination" certification criteria in § 170.315(b); § 170.550(h)(v) in reference to the "view, download, and transmit to 3rd party" certification criterion in § 170.315(e)(1); and to § 170.550(h)(viii) in reference to the § "application access" certification criteria at § 170.315(g)(7) through (g)(9) and the "standardized API for patient and population services" certification criterion at § 170.315(g)(10).

We propose that the new "patient requested restrictions" certification criterion in § 170.315(d)(14) would be required for the Privacy and Security Framework by January 1, 2026.

We welcome public comment on this proposal.

Finally, we propose a modification to the "view, download, and transmit to 3rd party" certification criterion in § 170.315(e)(1) in order to support patients' ability to leverage technology to exercise their right to request a restriction under the HIPAA Privacy Rule. We propose that a Health IT Module certified to the criterion in § 170.315(e)(1) must also enable an internet-based approach for patients to request a restriction of use or disclosure of their EHI for any data expressed in the USCDI standards in § 170.213. Specifically, we propose to modify § 170.315(e)(1) to add a paragraph (iii) stating patients (and their authorized representatives) must be able to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213.

The current version of the § 170.315(e)(1) "view, download, and transmit to 3rd party" certification criterion uses the concept of "internet-based" to convey, at § 170.315(e)(1)(i), that "[p]atients (and their authorized representatives) must be able to use *internet-based technology* to

view, download, and transmit. . . .” (emphasis added). In the ONC Cures Act Final Rule (85 FR 25886), we described how we chose to use the term “internet-based method” in lieu of other options such as “web-based delivery” because it more technically aligns with the concept we were attempting to support. Such methods would be accessed via an API, patient portal, or other internet-based means. We believe a similar approach is appropriate for the additional functionality supporting a patient request.

We propose that conformance with this update to the “view, download, and transmit to 3rd party” certification criterion in § 170.315(e)(1)(iii) would be required by January 1, 2026, for Health IT Modules certified to § 170.315(e)(1). Consistent with our proposals in sections III.A and III.C.11, developers of certified health IT with Health IT Modules certified to § 170.315(e)(1) would have to update those Health IT Modules to § 170.315(e)(1)(iii) and provide them to customers by January 1, 2026.

We welcome public comment on this proposal.

We do not propose any changes to the current certification criteria for “security tags - summary of care - send “ and “security tags - summary of care – receive” in § 170.315(b)(7) and § 170.315(b)(8) respectively; however, we note that the inclusion of the proposed new certification criterion in § 170.315(d)(14) into the Privacy and Security Framework in § 170.550(h) would mean that the proposed new certification criterion would be applicable for Health IT Modules certified to the security tags—send and security tags—receive certification criteria as well. We seek comment on whether those certification criteria should also be directly modified in alignment with the proposals described in this section.

We seek comment on the capabilities we have proposed for the new criterion in relation to the HIPAA Privacy Rule right to request a restriction. We specifically seek comment on whether the proposed new criterion should include additional functions to better support compliance with the HIPAA Privacy Rule right to request a restriction. We also seek comment on whether the proposed new criterion should, for example, include capabilities to support

HIPAA Privacy Rule provisions for emergency disclosures in § 164.522(a)(1)(iii) and (iv) or termination of a restriction under § 164.522(a)(2). We direct readers to section III.C.10.c for further discussion and specific questions for consideration.

Finally, we seek public comment on each part of this proposal—the new criterion in § 170.315(d)(14), the inclusion of the request capability for patients in § 170.315(e)(1), and the requirements with the Privacy and Security Framework in § 170.550(h)—both separately and as a whole. We specifically seek comment on the feasibility of each part in terms of technical implementation and usefulness for patients and covered entities using these capabilities. We also seek comment on the health IT development burden associated with implementation of the capabilities including for the individual certification criterion referenced in the Privacy and Security Framework in § 170.550(h).

In addition, we seek comment on any unintended consequences that the new criterion in § 170.315(d)(14) or the addition to the Privacy and Security Framework in § 170.550(h) might place on patients, clinicians, or other covered entities using certified health IT. We seek comment on whether, and by how much, the use of this criterion as part of broader privacy workflows might represent a reduction in manual effort for covered entities, a positive impact on uptake by patients, or other benefits such as supporting documentation of restrictions as required under the HIPAA Privacy Rule in § 164.522(a)(3).

Finally, we seek comment on methods by which we might quantify the development burden and costs as well as the potential benefits or future cost savings for the new criterion in § 170.315(d)(14), the new functionality in the existing criterion in § 170.315(e)(1), and the addition to the Privacy and Security Framework in § 170.550(h).

b. Alignment with Adopted Standards – Alternate Proposals and Request for Information

In addition to the primary proposal above, we also propose a set of alternatives for the new certification criterion proposed in § 170.315(d)(14), and we seek comment on various

options related to the potential use of standards and the scope of both the applicable data and the use cases. Our primary proposal described in section III.C.10.a above for the new criterion in § 170.315(d)(14) does not specify any required standard or implementation specification for the criterion; rather, it describes the desired functionality absent standards.

In the alternative proposals below, we seek comment on the potential use of data segmentation for privacy standards and implementation specifications, the number and types of applicable use cases supported by the implementation specifications that should be certified, and the data elements that could be tagged with security labels that must be supported for each criterion. This set of alternatives contrasts with our primary proposal by naming specific standards and implementation specifications for the new criterion in § 170.315(d)(14) to achieve patient-requested restrictions.

In the 2015 Edition Final Rule, we adopted and incorporated by reference the HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (HL7 CDA DS4P IG) in § 170.205(o)(1) and § 170.299 respectively. In the ONC Cures Act Final Rule, we updated certification criteria supporting the application of security labels at a granular level for sending in (in § 170.315(b)(7)) and receiving (in § 170.315(b)(8)), which reference the HL7 CDA DS4P IG (85 FR 25707). The HL7 CDA DS4P IG was balloted in 2014 and reaffirmed by HL7 in 2019.[316] Subsequent to the publication of the ONC Cures Act Final Rule, HL7 balloted the HL7 FHIR Data Segmentation for Privacy Version 1.0.0 (HL7 FHIR DS4P IG),[317] which includes an API specific functionality supporting similar concepts as the document-based HL7 CDA DS4P IG. While the HL7 FHIR DS4P IG may employ different descriptive terms for the application of meta-data specifications (e.g., resource rather than document/section), it is otherwise aligned to the underlying constructs of the C-CDA IG.

[316] https://www.hl7.org/implement/standards/product_brief.cfm?product_id=354.
[317] https://build.fhir.org/ig/HL7/fhir-security-label-ds4p/index.html.

The HL7 CDA DS4P IG establishes four types of reusable and platform neutral structures referred to as "Privacy Annotation Building Blocks." These include Confidentiality Level, Purpose of Use, Obligation Policy, and Refrain Policy. In the HL7 FHIR DS4P IG, these categories are described as "Tag Sets" and expanded slightly to include a "General Purpose of Use," category and associated value set. Each of these building blocks provide metadata regarding sensitivity levels, handling instructions, and permitted uses of data, and they are represented as a security label. Both of these IGs (collectively referred to hereafter as the HL7 DS4P IGs) leverage the HL7 Privacy and Security Healthcare Classification System (HCS) Security Label Vocabulary, which provides a common syntax and semantics for interoperable security labels in health care. The HCS Security Label Vocabulary and HL7 DS4P IGs' Privacy Annotation Building Blocks and Tag Sets are meant to support several computable "actions," to segment data in different contexts. We understand that the combination of different actions in different contexts creates significant optionality and may be difficult to implement, even with the assistance of HL7 DS4P IGs. As such, we propose and seek comment on a standards agnostic approach and several alternative approaches that would reference a standard and constrain optionality of these standards in specific ways.

As described in section III.C.10.a, we propose a new criterion "patient requested restrictions" in § 170.315(d)(14) that is standards agnostic, rather than require use of a specific standard for the Security Label vocabulary or application of security labels. We believe this approach would provide flexibility for developers of certified health IT to provide this functionality in ways that are convenient for their underlying system structures and in support of existing workflows for patient requested restrictions under the HIPAA Privacy Rule. However, we seek comment on a set of alternate proposals which would instead reference the HL7 CDA DS4P IG and the HL7 FHIR DS4P IG and which consider the potential to adopt these standards with constraints.

This alternative approach — proposing that § 170.314(d)(14) reference specific standards rather than proposing it be standards agnostic — would remove ambiguities inherent in the standards agnostic proposal by establishing a basis for the "flag" on the data using consensus standards for security labeling. The use of these standards may also facilitate implementation of capabilities to support patient requested restrictions on certain uses or disclosures by providing taxonomy for the scope of such restrictions and the purpose or use to which such restrictions apply. We believe the alternative proposals, which rely on HL7 standards, may be preferrable for developers of certified health IT that seek standards-based implementation guidance over flexibility. However, we specifically seek comment on whether that assumption is correct and whether a standards agnostic approach would be more technically feasible.

Specifically, the alternative proposals are as follows:

- In section III.C.10.b.i, we seek comment on a set of alternate proposals adopting each of the HL7 DS4P IGs, the HCS Security Label Vocabulary, or both for the new criterion in § 170.315(d)(14).
- In section III.C.10.b.ii, we seek comment on alternate proposals adopting the HL7 DS4P IGs and/or the HCS Security Label Vocabularies with constraints beyond those described in the IGs, that, if finalized, would constrain the requirements within the IGs to only certain use cases.
- In section III.C.10.b.iii, we seek comment on an additional alternate proposal that, if finalized, would limit the specified scope of USCDI data that the proposed new criterion in § 170.315(d)(14) and the proposed revised criterion in § 170.315(e)(1) would be required to support.

We additionally seek comment on the technical feasibility of each alternative, including the potential development burden and any associated burden on patients, clinicians, or other covered entity using certified health IT, as well as the positive impact on uptake by patients, or

other benefits such as supporting documentation of restrictions as required under the HIPAA Privacy Rule in § 164.522(a)(3).

i. Alternate Proposals Adopting Standards in Full

We propose and seek comment on three alternatives that would adopt and apply standards and implementation specifications to the proposed new criterion in § 170.315(d)(14).

- First Alternative: In this alternative proposal, we propose and seek comment on the use of the HL7 CDA DS4P IG, which is already incorporated by reference in § 170.299, as a basis for the application of a "flag" and the terminology for instructions on use or disclosure. This alternative proposal would require the use of the HL7 CDA DS4P IG for security labels and applicable actions described by the Privacy Annotation Building Blocks for the proposed new certification criterion in § 170.315(d)(14). This alternative proposal would also modify the proposed reference within the Privacy and Security Framework in § 170.550(h)(3) so that the new criterion in § 170.315(d)(14) would only be applicable in § 170.550(h)(3)(iii) for Health IT Modules certified to the criteria in § 170.315(b)(1) and § 170.315(g)(9). The purpose of this would be that if the new criterion in § 170.315(d)(14) referenced the HL7 CDA DS4P IG, that IG would only be applicable under the Privacy and Security framework to those certification criteria that also reference the HL7 C-CDA standard in § 170.205(a)(5).
- Second Alternative: In this alternative proposal, we propose and seek comment on the use of the HL7 FHIR DS4P IG, which would be adopted and incorporated by reference in § 170.299, as a basis for the application of a "flag" and the terminology for instructions on use or disclosure. In this proposal, the HL7 FHIR

DS4P IG[318] would be adopted and incorporated by reference in § 170.299 for security labels and applicable actions described by Tag Sets for the proposed new certification criterion in § 170.315(d)(14). This alternative proposal would also modify the proposed reference within the Privacy and Security Framework in § 170.550(h)(3) so that the new criterion in § 170.315(d)(14) would only be applicable in § 170.550(h)(3)(viii) for Health IT Modules certified to the criterion in § 170.315(g)(10) The purpose of this would be that if the new criterion in § 170.315(d)(14) referenced the HL7 FHIR DS4P IG, that IG would only be applicable under the Privacy and Security framework to those certification criteria that also reference the HL7 FHIR standard in § 170.215(a).

- Third Alternative: We propose and seek comment on a third alternative that would require only the HCS Security Label Vocabulary as a basis for the application of a "flag" and the terminology for instructions on use or disclosure. The HCS Security Label Vocabulary is referenced in both the HL7 CDA and FHIR DS4P IGs. Use of the HCS Security Label Vocabulary would, in this alternative proposal, serve as the basis for a format-agnostic and transport-mechanism-agnostic standard for the application of security labels and to define the general instructions for each label. Under this third alternative, we would propose to reference the HCS Security Label Vocabulary for security labels and applicable actions for the proposed new criterion in § 170.315(d)(14) as follows: For any data expressed in the standards in § 170.213, enable a user to apply security labels based on the HCS Security Label Vocabulary to identify whether such data needs to be restricted from being subsequently used or disclosed as set forth in 45 CFR § 164.522; and for any data with such security label pursuant to

[318] The HL7 FHIR DS4P IG is proposed for incorporation by reference and further described in section v. of this proposed rule. See also https://build.fhir.org/ig/HL7/fhir-security-label-ds4p/index.html.

paragraph (d)(14)(i) enable the correlated action for subsequent use or disclosure for the restricted purpose defined in the HCS Security Label Vocabulary.

This alternative would not require full implementation of either HL7 DS4P IG. The HCS Security Label Vocabulary is a part of the HL7 CDA DS4P IG standard already adopted in § 170.205(o)(1) and incorporated by reference in § 170.299, and it could be used across Health IT Modules referenced in the Privacy and Security Framework in § 170.550(h) whether the applicable certification criterion is a C-CDA or FHIR-based functionality.

We welcome public comment on these three alternate proposals, including which approach would be most effective or feasible in terms of implementation of the standards options described for the proposed criterion in § 170.315(d)(14). We direct readers to section V of this proposed rule for more detail and request for comment on the HL7 FHIR DS4P IG proposed for incorporation by reference for the purposes of the alternate proposal for the criterion in § 170.315(d)(14).

We also specifically seek public comment on whether these alternate proposals for the proposed criterion in § 170.315(d)(14) would help to define the requirements for the criterion in a manner that would be more beneficial or more burdensome than a standards agnostic approach, and if so, which alternate proposal would be most beneficial. We seek comment on the health IT development burden and cost associated with implementation of the IGs described. We seek comment on any unintended consequences that the use of these standards might place on health IT developers, patients, clinicians, or other covered entities using certified heath IT. We seek comment on whether, and by how much, the use of these standards might represent a reduction in the burden of manual privacy workflows otherwise still necessary under a standards agnostic approach. We seek comment on the potential benefits to patients, or other benefits such as supporting documentation of restrictions as required under the HIPAA Privacy Rule in § 164.522(a)(3). Finally, we seek comment on clear methods by which we might quantify the

development burden and costs as well as the potential benefits or future cost savings that could be associated with a standards-based approach as compared to adopting only a functional requirement.

ii. Alternate Proposal Adopting Standards with Constraints

We note that the HL7 DS4P IGs specify security labels for a wide range of use cases, privacy policies, applicable actions and segmentation of data beyond the scope of the patient right to request a restriction under the HIPAA Privacy Rule. We, therefore, also propose and seek comment on an alternative that would reference these standards as described in section III.C.10.b.i, but would specify the scope of use to only require support for the privacy workflows associated with the HIPAA Privacy Rule patient right to request a restriction on disclosure or use rather than on the full range of privacy and security workflows that the standards may support. This alternative proposal for the proposed criterion in § 170.315(d)(14) would reference the HL7 DS4P IGs or the HCS Security Label Vocabulary but would not require the implementation of all applicable security labels or actions described in these specifications. We seek comment on whether, for the purposes of certification, we should adopt the HL7 DS4P IGs or reference the HCS Security Label Vocabulary as described in the alternate proposals in sub-section i. but with additional constraints to narrow the scope. We seek comment on whether we should adopt specific constraints to allow health IT developers to demonstrate the capability to filter, redact, or implement another defined action only for certain use cases supported by the security labels in the HCS Security Label Vocabulary, Privacy Annotation Building Blocks, and Tag Sets. For example:

- Should we constrain the requirements to apply the IGs for only certain general purposes or purposes of use? Specifically, should we limit requirements described in the applicable IGs for actions defined by PurposeofUse and GeneralPurposeofUse values associated with purposes allowed for patient requested restriction under the HIPAA Privacy Rule? These value sets include a range of references that could be used to limit the scope. For

example, one value describes a label based on a patient choice to participate, or not, in clinical trials (CLINTRCH). In addition, which values in the PurposeofUse and GeneralPurposeofUse value sets would be most appropriate for the purpose of the patient requested restriction under the HIPAA Privacy Rule?

- Should we constrain the requirements to apply the IGs for only certain actions described for the restrictions? Specifically, should we limit requirements described in the applicable IGs for actions described under the RefrainPolicy ValueSet to only those defined actions relating to the patient request for restriction use case? Which values would be most appropriate for that purpose? For example, should we focus on actions to support the value NOATH, NOCOLLECT, NOINTEGRATE, or NOLIST? What other values in the RefrainPolicy ValueSet define actions that would also be appropriate for the use case?
- Should we limit requirements described in the applicable IGs for actions defined under the ObligationPolicy ValueSet that are necessary to implement the patient request for restriction or individual choice use case? For example, should we focus on support for the value REDACT? What other values would also be appropriate for the use case? Would either or both of these proposed alternatives to constrain the scope of the HL7 DS4P IGs reduce complexity and support feasibility for implementation of the new criterion in § 170.315(d)(14)?
- Are there health IT development burden considerations associated with implementation of these alternatives, including for the certification criteria in § 170.315(b) and (g) referenced in the Privacy and Security Framework in § 170.550(h)(3)(iii) and (viii)? Are there unintended consequences that these constraints on the proposed criterion in § 170.315(d)(14) might place on health IT developers, patients, clinicians, or other covered entities using certified health IT? Are there clear methods by which we might quantify the development burden and costs as well as the potential benefits or future cost

savings for this proposed alternative constrained version of the proposed criterion in § 170.315(d)(14)?

iii. Alternate Proposal for Adoption of Full and Constrained Data Elements within the USCDI

We propose and seek comment on an additional alternative beyond those referenced above in sections III.C.10.b.i and III.C.10.b.ii. This additional alternative would limit the total scope of data required for certification to the proposed new criterion in § 170.315(d)(14) and the proposed revisions to the existing criterion in § 170.315(e)(1). Under this alternate proposal, instead of the full scope of data expressed in the USCDI standards in § 170.213, as referenced in proposed § 170.315(d)(14)(i) and the proposed revisions to the existing criterion in § 170.315(e)(1), certification for these criteria would apply for only the Patient Demographics/Information, Clinical Notes, Medications, and Health Status Assessments data classes within the USCDI. We additionally seek comment on whether some other scope of certain data classes or data elements would be most appropriate.

We welcome public comment on these alternate proposals both individually and in combination. We seek comment on whether these proposed constraints on the scope of the applicable data would reduce complexity and support feasibility for implementation of the new proposed criterion in § 170.315(d)(14) and the proposed revisions to the existing criterion in § 170.315(e)(1). We seek comment on the health IT development burden associated with implementation of the constrained capabilities in relation to the individual certification criteria in § 170.315(b) and (g) referenced in the Privacy and Security Framework in § 170.550(h)(3)(iii) and (viii).

We also seek comment on any unintended consequences that these constraints on the data in the new criterion in § 170.315(d)(14) and the proposed revisions to the existing criterion in § 170.315(e)(1) might place on health IT developers, patients, clinicians, or other covered entities using certified health IT.

Finally, we seek comment on clear methods by which we might quantify the development burden and costs as well as the potential benefits or future cost savings for this proposed alternative to constrain the USCDI referenced in the proposed criterion in § 170.315(d)(14) and the proposed revisions to the existing criterion in § 170.315(e)(1).

c. Alignment with Applicable Law – Request for Information

ONC certifies capabilities of Health IT Modules to perform specific functions, in many circumstances using specific standards. These are generally restricted to technical standards and capabilities. The user of the technology may also need to comply with certain requirements established by federal, state, territory, local or tribal law. Our intent for proposing a technical means for patients to request a restriction on their data is to advance tools that support privacy laws, including the HIPAA Privacy Rule right to request a restriction of certain uses and disclosures.[319] We emphasize that use of any future Health IT Module certified to these proposed requirements would not, by itself, fully discharge the obligations under the HIPAA Privacy Rule of a covered entity to allow an individual to request a restriction on the use or disclosure of their PHI for treatment, payment, or health care operations or to have policies in place by which to accept or deny such requests. Further, use of any such certified Health Module would not discharge the obligations of a covered entity to meet any other requirements under 45 CFR 164.522. In addition, there may be other applicable laws that affect the exchange of particular information, and those laws should be considered when developing individual choice policies.

We seek comment on whether there are modifications, adjustments, additions, or restrictions we should consider for our proposal to better support privacy workflows under the HIPAA Privacy Rule:

[319] HHS Office for Civil Rights. HIPAA "Right to Request a Restriction": https://www.hhs.gov/hipaa/for-professionals/faq/right-to-request-a-restriction/index.html.

- Are there modifications, adjustments, additions, or restrictions that could support the termination of a restriction request as described under § 164.522(a)(2)? Should such a capability be a requirement for the proposed new criterion in § 170.315(d)(14)?
- Are there modifications, adjustments, additions, or restrictions that could support emergency use or disclosure of otherwise restricted information as described under § 164.522(a)(1)? Should such a capability be a requirement for the proposed new criterion in § 170.315(d)(14)? In such instances, how would the original restriction request be documented and persisted to prevent redisclosure or use subsequent to emergency use or disclosure as described under § 164.522(a)(1)(iv)?
- Are there modifications that would better support the documentation of restrictions as described under § 164.522(a)(3)? Are there modifications, adjustments, additions, or restrictions we should consider for our proposal to better support privacy workflows under other HIPAA Privacy Rule provisions? For example, are there modifications that would specifically support covered entities in implementing protections based on patient preferences for the prevention of harm for patients as allowable under § 164.524(a)(3)? Are there modifications, adjustments, additions, or restrictions we should consider for our proposal to better support privacy workflows under other applicable law? For example, are there modifications that would specifically support patient preferences for the privacy of EHI under state laws restricting disclosure of health information of minors? Are there modifications, adjustments, additions, or restrictions that would specifically support patient preferences for applicable laws related to disclosure and use of EHI related behavioral health or substance abuse? Are there modifications, adjustments, additions, or restrictions that would specifically support patient preferences for restrictions on disclosure or use related to stigmatized care under other state laws?

In section IV.C.3 of this proposed rule, we outline a range of questions for public comment and request information to specifically consider the policy implications related to supporting health IT users' ability to segment and selectively display, delay, or withhold EHI consistent with patient preferences for information sharing, applicable law, and other considerations such as when a delay or other interference with particular EHI access, exchange, or use may be reasonable and necessary under the conditions of an information blocking exception. We direct readers to section IV.C.3 for discussion and questions related to an illustrative sampling of use cases for data segmentation and user/patient access management functionalities. We also welcome public comment on this proposal to support patients' right to request a restriction of disclosure in the context of information sharing requirements under the ONC Cures Act Final Rule.

11. Requirement for Health IT Developers to Update their Previously Certified Health IT

Section 3001(b) of the PHSA directs the National Coordinator to conduct the duties defined in section 3001(c), including the implementation of a certification program in section 3001(c)(5) of the PHSA, "in a manner consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information." This includes considerations for health IT to reduce costs resulting from inefficiency and incomplete information, to provide appropriate information to help guide medical decisions at the time and place of care, to improve the coordination of care, to facilitate a rapid response to public health threats and emergencies, and to promote greater efficiencies in the marketplace. As ONC administers the Program and adopts new or updated standards, implementation specifications, and certification criteria on behalf of the Secretary under section 3004 of the PHSA, we must also seek to address these requirements. When the healthcare industry and healthcare standards community update or develop new clinical guidelines, address emerging public health challenges, implement new state or local laws targeting high priority health issues, or develop new interoperability standards for enhanced care coordination, ONC

often must also adopt aligned updates to the standards, implementation specifications, and certification criteria applicable in the Program. This is essential to ensure that certified capabilities of health IT continue to support the development of a nationwide health IT infrastructure.

Previously, such updates were implemented via an entirely new "edition" of certification criteria. As described in section III.A of this proposed rule, while this approach supported clarity for Program requirements at a given time, we believe the burden and rigidity of the "edition" approach render it unsustainable over the long term. A more modular approach that can accommodate changes for specific use cases without disrupting the entirety of the marketplace through a wholesale "edition" update is more appropriate to support an interoperable health IT infrastructure across a wide range of use cases (*see* section III.A of this proposed rule for a discussion on maintaining a single set of "ONC Certification Criteria for Health IT" and discontinuing year-themed editions). When a health IT developer voluntarily participates in the Program, if they intend for their health IT to be certified and maintain its certification, then they are committing to the policies and terms of the Program as expressed through regulatory provisions, including the implementation of any updates to the criterion or standards as applicable for each criterion to which they certify a Health IT Module. Further, the process of implementing updates for certified health IT systems must include providing necessary updates for use in real world settings as required by the Real World Testing Condition of Certification at 45 CFR 170.405.

In the 2015 Edition Proposed Rule, we clarified our expectation that ONC-ACBs render a Health IT Module non-conformant to the certification criteria in instances where the developer of certified health IT does not make the capability available; substantially restricts or limits its use; or has not disclosed known material information about the implementation or use of the capability (80 FR 16878). Likewise, in the 2015 Edition Final Rule, we provided different scenarios and examples of non-conformities in the field where certified capabilities are not

functioning properly, including when due to the failure by the developer of certified health IT to support the implementation of appropriate updates (80 FR 62710).

Subsequently, the Cures Act added to section 3000 of the PHSA a definition of "interoperability" (at 42 U.S.C. 300jj(9)) with respect to health information technology (also defined in the PHSA (42 U.S.C. 300jj(5)) as such health information technology that: (1) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user; and (2) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law.[320] The Cures Act incorporated the term "interoperability" into provisions establishing the Conditions of Certification under the Program, the EHR Reporting Program, and requirements for the HITAC to recommend a policy framework and address priority target areas. The Cures Act also requires that ONC establish benchmarks for advancing the priority target areas defined and that the HITAC develop annual progress reports on advancing interoperability. The definitions of interoperability and health information technology were also codified by ONC in 45 CFR 170.102.

In this proposed rule, as we move away from the use of editions to define timeframes for updating to new and revised certification criteria (*see also* section III.A and specifically Table 1), we believe it is important to continue to provide clarity regarding the obligations of developers who are seeking to certify health IT and maintain a Health IT Module's certification, including, as applicable, certification to revised certification criteria and the timely provision of such technology to their customers. We are therefore proposing to incorporate applicable timelines and expiration dates that will apply for capabilities and standards updates within each individual criterion or standard as appropriate to the criterion and include specific requirements under the

[320] The term ''interoperability,'' with respect to health information technology, also means such health information technology that does not constitute information blocking as defined in section 300jj–52(a) (42 U.S.C. 300jj(9)(C)).

"Assurances" Condition of Certification, discussed in detail in the next section (section III.D of this proposed rule).

We propose to make explicit in the introductory text in § 170.315 that health IT developers voluntarily participating in the Program must update their certified Health IT Modules—including when new standards and functionality are adopted— and provide that updated certified health IT to customers in accordance with the timelines defined for a specific criterion or standard where included, such as via cross-reference, in § 170.315. We propose that health IT developers with health IT certified to any of the certification criteria in § 170.315 would need to update their previously certified Health IT Modules to be compliant with any revised certification criterion adopted in § 170.315 (please see section III.A of this proposed rule for the proposed definition of revised certification criterion (or criteria)), including any certification criteria to which their Health IT Modules are certified that reference new standards adopted in 45 CFR part 170 subpart B, and capabilities included in the revised certification criterion. Health IT developers would also need to provide the updated heath IT to customers of the previously certified health IT according to the timelines established for that criterion and any applicable standards. In addition to supporting the goals of the Program, we believe this approach will help to advance interoperability. Requiring health IT developers who voluntarily participate in the Program to update Health IT Modules to revised certification criteria (including new and revised standards) can help to advance capabilities for access, exchange, and use of EHI for authorized use under applicable State or Federal law. In addition, ensuring health IT developers voluntarily participating in the Program provide such updates to customers will help to enable the secure exchange of EHI with, and use of EHI from, other health information technology without special effort on the part of the user. We believe these proposed timelines also serve to support clear and transparent benchmarks for furthering interoperability throughout the health IT infrastructure.

As noted previously, the updates to criteria may include technical capabilities such as security enhancements or additional transactions not previously supported for a criterion. These updates may also include an expansion of the data supported by content, vocabulary, and format standards to increase the scope of interoperable EHI. For example, as new data elements are standardized, updates to criteria may help to incorporate these data elements into clinical systems in an interoperable manner. Such advancement could be in response to an emergent need such as a public health response, but it may also be for commonly used information that is essential to care but for which representation via standard vocabularies has lagged behind. One such example is the inclusion of functional status, disability status, and mental or cognitive status in the USCDI v3.[321] These data elements are essential for long term and post-acute care, but without consistent standards for representation of this information, they were often included in non-computable formats or excluded from health information exchange. The adoption of USCDI v3 and its incorporation into certification criteria through updates to those criteria, as proposed in this rule, means that certified health IT systems would be able to support representation of this health information in a standardized computable format, if those proposals are finalized. Updating current systems to incorporate these data elements and providing updated certified health IT to customers would allow users of certified health IT to begin to access, exchange, and use such data without special effort. Over the long term, this advancement of interoperability for certified health IT systems may also have a positive impact on the availability of this essential data and the capability to access, exchange, and use this data across a nationwide health IT infrastructure – including for purposes not yet specifically supported by certified health IT such as clinical research.

In the ONC Cures Act Final Rule, we discussed how we expected developers to make technology updates available to their customers (see, for example, 85 FR 25665) in relation to

[321] USCDI version 3 Health Status Assessments Data Class: https://www.healthit.gov/isa/uscdi-data-class/health-status-assessments#uscdi-v3.

the 2015 Edition Cures Update. We stated that health IT developers would have until the applicable deadline to make technology certified to these updated criteria available to their customers, and during this time developers may continue supporting technology certified to the prior version of certification criteria for use by their customers. We further noted that customers may continue to use the certified health IT they had available to them and can work with their developers to implement any updates in a manner that best meets their needs (85 FR 25665).

We also included a requirement to "provide" customers with updated Health IT Modules as a Maintenance of Certification requirement (e.g., § 170.405(b)(3)) for the Real World Testing Condition of Certification requirement (§ 170.405(a)) for certain criteria updated in the 2015 Edition Cure Update and the EHI Export certification criterion in the Assurances Condition of Certification (§ 170.402(b)(2)). Subsequent to the ONC Cures Act Final Rule, through correspondence and public forums, health IT developers and the healthcare community described differences of opinion regarding whether there is a meaningful difference between "make available" and "provide" in practical application and requested that ONC specify only one of these terms. In the introductory text in § 170.315 we propose in this rule, we propose to use only the term "provide" without the inclusion of "make available." We also propose that "provide" does not imply that the Health IT Module must be in production use across all customers. Instead, we propose that to "provide" the product means the developer must do more than make the product available and there must be demonstrable progress toward implementation in real world settings. We propose to maintain the prior approach where a Health IT Module may be certified to either the existing criterion or the revised certification criterion until the end of the deadline, so that during the interim period existing customers may continue to use the certified technology they have available to them and can work with their developers to implement updates in a manner that best meets their needs. Finally, as with the 2015 Edition Cures Update, in order to support effective communication of the updates, we would implement a practical approach to

facilitate transparency using the Certified Health IT Product List (CHPL),[322] which is the tool that health care providers and the general public may use to identify the specific certification status of a certified health IT product at any given time, to explore any certification actions for a product, and to obtain a CMS Certification ID for a product, which is used when participating in some CMS programs. We note that historically, CMS has included additional guidance for such program participants within CMS proposed or final rules (see, for example, 85 FR 84818-84828).

Consistent with section 3006 of the PHSA, we note that under this proposed rule, a developer of certified health IT would not be required to provide updated technology to any customer that elected to decline the update for any reason. Such reasons might include a customer choosing to discontinue use of a specific Health IT Module or product, or to no longer participate in HHS programs that require the use of certified health IT. We note that in such cases, while the Health IT Module may still operate, it would no longer be certified and may no longer meet program requirements for HHS programs requiring the use of certified health IT. Specifically, we propose that for all revised certification criteria in § 170.315, a developer of certified health IT shall update their certified health IT to such criteria and provide these updates to their customers in accordance with the dates identified for each revised certification criterion, including for standards referenced by the criteria in accordance with the dates identified for each applicable standard in 45 CFR part 170 subpart B.

As mentioned above, in section III.D of this proposed rule, we describe our proposal for Condition and Maintenance of Certification requirements under the Assurances Condition of Certification for health IT developers of certified health IT. By doing so, we propose both the technical requirements for conformance to the certification criterion and the behavioral requirements for conformance to the condition in the Program. As described in section III.D, this Condition of Certification provides specified periods of time to "update and provide" certified

[322] ONC Certified Health IT Product List: https://chpl.healthit.gov.

health IT. We note that in some cases the timelines and expiration dates for applicable capabilities and standards defined for a certification criterion in § 170.315 may be longer or shorter than the standard period of time defined in the proposed condition of certification. This difference is due to our analysis of the urgency of the use case, the readiness for the capability or standard, and the current use of such capability or standard by the healthcare industry, including consideration of dependent requirements across HHS programs.

We welcome comments on this proposal.

D. Assurances Condition and Maintenance of Certification Requirements

Section 4002(a) of the Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification under the Program, provide assurances satisfactory to the Secretary that such developer, unless for legitimate purpose(s) as specified by the Secretary, will not take any action that constitutes information blocking as defined in section 3022(a) of the PHSA or any other action that may inhibit the appropriate exchange, access, and use of EHI. In the ONC Cures Act Final Rule, we adopted specific Conditions and Maintenance of Certification requirements for health IT developers of certified health IT consistent with this authority (s*ee also* ONC's implementation approach for section 4002 as discussed in the Cures Act Final Rule at 85 FR 25718).

The Conditions of Certification that were codified focused on health IT developers providing assurances that: their health IT certified under the Program conforms to the full scope of the certification criteria; they would not take any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the full scope of the technology's certification; and, for those with a certified Health IT Module that is part of a health IT product that electronically stores EHI, they would certify to the EHI Export certification criterion. These Conditions of Certification, and in some instances accompanying Maintenance of Certification requirements, provide assurances to the Secretary, and by default to customers and users of certified health IT, that health IT developers are not taking actions that could

potentially constitute information blocking, or at the least, inhibit the appropriate exchange, access, and use of EHI.

In this proposed rule, we propose to establish a new Condition of Certification and accompanying Maintenance of Certification requirements under the Assurances Condition of Certification. These new requirements would serve to provide the assurances to the Secretary that Congress sought and further clarify Program requirements that are established under the authority provided in section 3001(c)(5) of the PHSA and discussed in detail above in section III.C.11 ("Requirement for Health IT Developers to Update their Previously Certified Health IT").

1. Condition of Certification

We propose in § 170.402(a)(5), that, as a Condition of Certification, a health IT developer must provide an assurance that it will not inhibit a customer's timely access to interoperable health IT certified under the Program. To support this assurance, we propose accompanying Maintenance of Certification requirements, which are discussed in detail below. The Maintenance of Certification requirements define the scope of this proposed Condition of Certification and provide clarity in terms of what it would mean to take the action of "inhibiting," what constitutes "timely access," and what is "interoperable health IT certified under the Program."

Interoperable health IT is an underpinning of the Program and particularly the conditions of certification found in the Cures Act and implemented in 45 CFR part 170 subpart D. Congress established support for health IT interoperability beginning with the authority provided in the HITECH Act to adopt standards (including implementation specifications and certification criteria) and establish the Program. It continued to emphasize health IT interoperability through requiring the establishment of metrics to determine the extent of "widespread interoperability" in the Medicare Access and CHIP Reauthorization Act (MACRA) (section 106(b)(1)). Ultimately, Congress went on to define interoperability with respect to health IT in the Cures Act, including

incorporating the information blocking definition within the interoperability definition. Congress further incorporated or specifically referenced the interoperability definition where it required, in 42 U.S.C. § 300jj-11(c)(5)(D), the Secretary to establish certain Conditions of Certification, including the "Communications," "Real World Testing," and "Insights" Conditions of Certification.

With this proposed rule, we propose that, for purposes of certification and the maintenance of such certification under the Program, a health IT developer would need to provide an assurance that its health IT is certified to the most recently adopted certification criteria and such certified health IT is made available to its customers in a timely manner (see below and section III.C.11). These actions are essential because certification criteria, and in particular revised certification criteria (as defined in this proposed rule), include standards, implementation specifications, and capabilities that support and improve interoperability as that term is defined by the Cures Act and incorporated in 45 CFR part 170. Since the inception of the Program, ONC has updated certification criteria to include the most recent versions of standards and implementation specifications that most appropriately support and improve interoperability at the time of adoption. This is because as standards and implementation specifications evolve, they, by their very nature, improve interoperability by allowing for more complete access, exchange, and use of all electronically accessible health information. Further, the interoperability definition also focuses, in part, on the secure exchange and use of EHI from other health IT without special effort on the part of the user. The Assurances Condition is an important piece to supporting and achieving these goals because it seeks assurances from health IT developers that they will not take any actions to inhibit the appropriate access, exchange, and use of EHI.

As a more practical and concrete implementation of the Assurances Condition and of supporting interoperability, it is important for users, particularly customers of developers of certified health IT, to have health IT certified to the most recent standards and capabilities. Otherwise, a health IT developer voluntarily participating in the Program would be undermining

interoperability and making it more difficult for customers of health IT developers of certified health IT to access, exchange, and use EHI as updated standards (e.g., USCDI, C-CDA, and FHIR) make more EHI readily accessible for electronic access, exchange, and use. Similarly, capabilities such as those found in the EHI Export and Electronic Case Reporting certification criteria improve the ability for health IT to allow complete access, exchange, and use of all electronically accessible health information.

2. Maintenance of Certification Requirements

We first propose, in § 170.402(b)(3)(i), that a health IT developer must update a Health IT Module, once certified to a certification criterion adopted in § 170.315, to all applicable revised certification criteria, including the most recently adopted capabilities and standards included in the revised certification criterion. For clarity, '*applicable* revised certification criteria' would be those certification criteria to which the Health IT Module was previously certified that meet the definition of a revised certification criterion as proposed in this rule (please see section III.A of the preamble and "revised certification criterion (criteria)" under § 170.102 of the regulation text for the proposed definition of revised certification criterion/criteria). Equally important, and, as stated above, to meet the proposed requirement, the Health IT Module would need to be updated to the most recently adopted capabilities and standards included in the revised certification criterion. For example, if the adopted revised certification criterion referenced new standards that will eventually replace the current standards referenced in the criterion, then the Health IT Module would need to be updated to the new standards before the end of the established timeframe for updating the Health IT Module. Second, we propose, in § 170.402(b)(3)(ii), that a health IT developer must provide all Health IT Modules certified to a revised certification criterion to its customers of such certified health IT. A customer, for this purpose, would be any individual or entity that has an agreement to purchase or license the developer's certified health IT. This proposed requirement would be more broadly

applicable than for "updated" Health IT Modules alone, as discussed via illustration of the proposed timeliness requirements below.

We propose separate "timely access" or "timeliness" Maintenance of Certification requirements for each of the two proposed Maintenance of Certification requirements above that would dictate by when a Health IT Module must be updated to revised certification criteria, including the most recently adopted capabilities and standards; and by when a Health IT Module certified to a revised certification criterion, including the most recently adopted capabilities and standard, must be provided to the health IT developer's customers. We propose, in § 170.402(b)(3)(iii), that unless expressly stated otherwise in 45 CFR part 170, a health IT developer must complete the proposed "update" and "provide" requirements according to the following proposals. First, we propose, in § 170.402(b)(3)(iii)(A), that a health IT developer must update and provide a Health IT Module by no later than December 31 of the calendar year that falls 24 months after the effective date of the final rule adopting the revised certification criterion or criteria. This would mean that, depending on the day when the final rule effective date fell, a health IT developer would have between two years and potentially up to almost three years (e.g., where a final rule is effective in January or February) to update a Health IT Module. Second, we propose that the "provide" requirement would need to be completed within this same timeframe for customers of the previous certified health IT that must be updated under the "update" proposal. However, we propose deviations to this timeframe because the "provide" requirement applies to all Health IT Modules that are certified to a criterion that meets the revised certification criterion definition (i.e., not just health IT previously certified to a 'prior version' of a revised certification criterion) **and** to *new* customers of health IT certified to revised certification criteria.

To illustrate when and how the "provide" and "timeliness" requirements would be applicable to a health IT developer beyond the "update" scenario recited above, we offer the following explanations. If a developer "expanded the scope" of a certified Health IT Module to

include certification to a revised certification criterion, then the "provide" condition would be applicable. In such cases, all of the health IT developer's customers would be considered "new" customers for purposes of the Health IT Module certified to the revised certification criteria criterion as the *capabilities are new to them*. If a health IT developer new to the Program, presumably with all "new" customers (again, any certified capability would be new to them), certified a Health IT Module to a revised certification criterion after the effective date of the final rule adopting the revised certification criterion, but during the period when both the "new" and "old" standards or capabilities, or both, are referenced within a revised certification criterion, the "provide" condition would be applicable. Similarly, if any health IT developer certified a Health IT Module to a revised certification criterion at a time when only the most recently adopted capabilities and standards are available for certification to the revised certification criterion, then the "provide" requirement must be met.

In all the above circumstances, we propose that health IT certified to revised certification criteria must be provided to all customers, including new customers (i.e., new to the capabilities), of health IT developers under the Program within reasonable timeframes. In this regard, we propose precisely the following timeframes:

Unless expressly stated otherwise in 45 CFR part 170, a health IT developer must complete the "update" and "provide" requirements:

- By no later than December 31 of the calendar year that falls 24 months after the effective date of the final rule adopting the revised certification criterion or criteria; or
- If the developer obtains new customers of health IT certified to the revised certification criterion after the effective date of the final rule adopting the revised certification criterion or criteria, then the health IT developer must provide the health IT certified to the revised certification criterion to such customers within whichever of the following timeframe that expires last:

- By no later than December 31 of the calendar year that falls 24 months after the effective date of the final rule adopting the revised certification criterion or criteria; or
- No later than 12 months after the purchasing or licensing relationship has been established between the health IT developer and the new customer for the health IT certified to the revised certification criterion.

The proposed above timeframes would offer health IT developers, at a minimum, no less than 12 months to provide health IT certified to revised certification criteria to new customers (i.e., customers new to the capability). Based on the proposed timeframes, a health IT developer has the ability to plan both the certification to revised certification criteria and the execution of contracts and agreements with new customers to ensure that it can meet the above timelines for new customers. However, by way of example via a proposal in this proposed rule, the "Unless expressly stated otherwise in this part" proposed in § 170.402(b)(3)(iii) would override the proposed timelines (e.g., 24 months or more in some cases) for updating and providing health IT certified to USCDI v3. We have proposed (see section III.C.1) to add the newly released USCDI v3 to the USCDI standard in § 170.213(b) and that the adoption of the current USCDI v1 standard would expire on January 1, 2025.

This USCDI v3 proposal not only would override the "24 month or more" timelines, but it also illustrates the importance of the "update and provide" proposals in this rule that support interoperability. The adoption of USCDI v3 would expand the data required to be accessible through certified health IT beyond the data elements included in USCDI v1 and thus would increase the amount of data available to be accessed, exchanged, and used for patient care. However, if a health IT developer with certified health IT inhibited its customers' timely access to health IT certified to USCDI v3 (i.e., by January 1, 2025), then the more than 40 additional data elements included in USCDI v3 would not be among the data available to be accessed,

exchanged, and used by the health IT developer's customers; and a significant amount of EHI may not be shared. We welcome comments on the proposed approach and timelines.

If a health IT developer did *not* meet the proposed update or provide requirements, including the timeliness requirements, then they would not only violate these requirements but also the proposed new condition by ***inhibiting*** a customer's timely access to interoperable health IT certified under the Program. As such, the developer would have committed non-conformities under the Program, unless the health IT developer did so for a permissible reason as described in section III.C.11 (see, for example, a developer of certified health IT would not be required to provide updated certified health IT to any customer that elected to decline the update for any reason; or a health IT developer's exercising their ability to reduce the scope of a certification while not under ONC-ACB surveillance or ONC direct review).

To note, we propose a conforming revision to the Real World Testing Maintenance of Certification requirements in § 170.405(b) in that we propose to remove most of the "update and provide" requirements currently found in this section because they are moot based on the publication date of this proposed rule and the subsequent publication of a final rule for this proposed rule (e.g., many timelines expired on December 31, 2022).

E. Real World Testing – Inherited Certified Status

In the ONC Cures Act Final Rule, we finalized requirements in § 170.405(a) that a health IT developer with Health IT Module(s) certified to § 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10), and (h) must: successfully test the real world use of the technology for interoperability in the type(s) of setting(s) in which such technology would be marketed. We established in § 170.405(b) that each developer's annual real world testing plan is required to be published by December 15 of a given year and would need to address all of the developer's Health IT Modules certified to criteria listed in § 170.405(a) as of August 31 of that year (85 FR 25769). We also finalized that this annual real world testing plan would pertain to real world testing activities to be conducted in the year following the December 15 plan publication due

date, with an annual real world testing results report to be published by March 15 (§ 170.405(b)(2)(ii) of the year following the year in which the real world testing is conducted) (85 FR 25774).

However, many health IT developers update their Health IT Module(s) on a regular basis, leveraging the flexibility provided through ONC's Inherited Certified Status (ICS).[323] Because of the way that ONC issues certification identifiers, this updating can cause an existing certified Health IT Module to be recognized as new within the Program. Regular updating, especially on a frequent basis such as quarterly or semi-annually, creates an anomaly that could result in existing certified Health IT Modules being inadvertently excluded from the real world testing reporting requirements.

In order to ensure that all developers test the real world use of their technology as required, we propose to eliminate this anomaly by requiring health IT developers to include in their real world testing results report the most recent version of those Health IT Module(s) that are updated using Inherited Certified Status after August 31 of the year in which the plan is submitted. This will ensure that health IT developers fully test all applicable Health IT Modules as part of their real world testing requirements. Please note, this proposal would prevent a developer from avoiding, or delaying conducting or reporting real world testing specifically on the updated versions of Modules certified through Inherited Certification Status after August 31 of a given year. This proposal would not change the underlying requirement that a developer with one or more Health IT Modules certified to any criterion listed in § 170.405(a) must plan, conduct, and report on real world testing of each of those Health IT Modules on an annual basis. We seek comment on this proposal.

F. Insights Condition and Maintenance of Certification

1. Background and Purpose

[323]https://www.healthit.gov/sites/default/files/policy/public_applicability_of_gap_certification_and_inherited_certified_status.pdf.

The Cures Act specified requirements in section 4002(c) to establish an Electronic Health Record (EHR) Reporting Program to provide transparent reporting on certified health IT in the categories of interoperability, usability and user-centered design, security, conformance to certification testing, and other categories, as appropriate to measure the performance of EHR technology. Data collected and reported would address information gaps in the health IT marketplace and provide insights on the use of certified health IT.

To develop the EHR Reporting Program, ONC contracted with the Urban Institute and its subcontractor, HealthTech Solutions, to engage the health IT community for the purpose of identifying measures that developers of certified health IT would be required to report on as a Condition and Maintenance of Certification under the Program. The Urban Institute published a final report in February 2022, which included a recommended set of measures for the EHR Reporting Program. ONC conducted additional research and expert consultations to refine the recommended set of measures in the Urban Institute's final report. Based on the additional research and expert consultations, we propose in this proposed rule, to modify the measures that the Urban Institute developed, consistent with section 3009A(a)(4) of the PHSA. We propose our modified versions of the measures in this proposed rule and solicit comment on both the underlying measures and our proposed modifications to them. In other words, our proposals with respect to each measure reflect how we propose to modify the set of measures in the Urban Institute's final report.

For clarity purposes, we intend to refer to the Condition and Maintenance of Certification associated with the "EHR Reporting Program" as the "Insights" Condition and Maintenance of Certification (also referred to as the "Insights Condition") throughout this proposed rule. We believe this descriptive name captures a primary policy outcome of this requirement.

2. Insights Condition – Proposed Measures

The proposed measures associated with the Insights Condition described in this proposed rule relate to and reflect the interoperability category in section 3009A(a)(3)(A)(iii) of the PHSA.

They relate to four aspects or areas of interoperability, which we refer to as “areas” throughout this proposed rule: individuals' access to EHI, public health information exchange, clinical care information exchange, and standards adoption and conformance, as discussed in further detail below. The majority of our proposed measures are data points derived from certified health IT systems. The proposed measures generally consist of numerators and denominators that will help generate metrics (e.g., percent across a population), which are further detailed in each proposed measure, but measures can also serve as standalone values. Note that in some cases ONC plans to generate multiple metrics by using different denominators for the same numerator or using different numerators with the same denominator. This approach would allow ONC to generate a variety of metrics. In one case, the measure is a simple attestation. For each measure, we have included information on the rationale for proposing the measure, proposed numerators and denominators, and key topics for comment.

As mentioned above, ONC contracted with the Urban Institute and its subcontractor, HealthTech Solutions, to engage the health IT community for the purpose of identifying measures that developers of certified health IT would be required to report on as a Condition and Maintenance of Certification under the Program. Identification of developer measures began with a broad literature and market scan, including market research discussions with subject matter experts, to identify potential measures for the categories specified in the Cures Act. The approach for identifying measures included several considerations, such as priority interoperability functions, relevance to ONC policy priorities and broader interests, measures reflecting information that ONC cannot obtain without regulation, and efforts that are not duplicative of other data collection.

The Urban Institute published draft measures for public feedback. ONC charged the HITAC to review the draft measures and provide recommendations to the National Coordinator on the draft measures. Both the HITAC and public were asked to provide feedback on topics such as frequency of reporting; data granularity; appropriateness of look-back periods; clarity of

definitions and measurement; benefit of measures relative to burden of collecting data; how to address potential interpretation challenges; potential burden on users of certified health IT; potential burden on small or start up developers of certified health IT; and value of measures to provide insights on interoperability. The HITAC transmitted recommendations to the National Coordinator on September 9, 2021. The Urban Institute's public feedback period ended on September 14, 2021.

After the public feedback period ended, the Urban Institute conducted feasibility testing with targeted respondents to assess the extent to which developers of certified health IT could produce and report on prospective measures. Specifically, the feasibility testing focused on understanding developers' ability to produce data required to calculate the measures from existing technology; understanding anticipated costs of preparing to produce data required to calculate the measures; relative burden of individual measures; and potential barriers to measure reporting.

The Urban Institute published a final report in February 2022, which included a recommended set of measures. The Urban Institute considered public feedback, HITAC recommendations, and feasibility testing with developers in determining the recommended set of measures included in the Urban Institute's final report.

ONC conducted additional research to modify the recommended set of measures in the Urban Institute's final report. The proposed measures included in this proposed rule were modified to reduce ambiguities and to address potential costs and burdens. Consistent with section 3009A(a)(3)(C) of the PHSA, we propose to modify the measures the Urban Institute developed, as well as implement minimum reporting qualifications designed to ensure that small and startup developers are not unduly disadvantaged by the proposed measures.

We note that the following proposed measures are for the initial Insights Condition requirements. In future rulemaking, we anticipate proposing additional measures for future

iterations of the Insights Conditions and Maintenance of Certification requirements under the Program.

Through this first set of proposed measures, ONC intends to provide insights on the interoperability category specified in the Cures Act (as codified at section 3009A(a)(3)(A)(iii) of the PHSA). We intend to explore the other Cures Act categories (security, usability and user-centered design, conformance to certification testing, and other categories to measure the performance of EHR technology) in future requirements.

We seek feedback on how we may further refine the proposed measures to improve feasibility, clarity, and potential insights gained. We welcome comments from the public on the proposed measures and overall Program processes related to the Insights Conditions and Maintenance of Certification. As stated above, the following describes our rationale for proposing the measure, proposed numerators and denominators, and key topics for comment.

We also have explored various pathways on how to make it easier for the public to view and comment on the detailed technical specifications supporting the proposed measures. While the substantive requirements for each measure are defined in this proposed regulation, we have determined that measure specification sheets would be a logical and accessible method for the public to also review and provide comment on the technical specifications supporting those requirements. This is consistent with the approach used by other HHS programs to solicit public feedback related to measure technical specifications (e.g., CMS Electronic Clinical Quality Measures (CMS eCQMs)). These methods allow for more effective review of the technical detail including supporting public comment on those specifications in a transparent manner. For more details and to provide comment on the technical specifications for measure calculation for the proposed measures, please consult the measure specification sheets available at www.healthIT.gov/NPRM. We welcome comments on the measure specifications sheets and note that such public comment will be used to further refine the technical specifications should

we finalize our proposals. We intend to keep these measure specification sheets up-to-date based on public feedback through a predictable and transparent process.

Insights Condition Cross-cutting Requirements

While the following proposed measures, as detailed below, require unique and specified data points, there are certain requirements that we propose to apply across multiple measures, including but not limited to: (1) data submitted by health IT developers would be provided and aggregated at the product level (across versions); (2) health IT developers would provide documentation related to the data sources and methodology used to generate these measures; and (3) health IT developers may also submit descriptive or qualitative information to provide context as applicable. The Cures Act specifies, per section 3009A(b) of the PHSA, that as a Condition of Maintenance of Certification, a health IT developer shall submit responses to the criteria developed with respect to all certified technology offered by such developer. Due to the specified requirements of the proposed measures, we believe it is reasonable to expect health IT developers, as part of their responses, to provide documentation used to generate the proposed measures for more accurate and complete data calculation. Overall, the documentation should help ensure the data is interpreted correctly. Thus, the documentation related to the data sources and methodology would include the types of data sources used, how the measure was operationalized (e.g., any specific definitions), any assumptions about the data collected, information on the providers or products that are included/excluded from the numerators and denominators, and a description about how the data was collected. ONC would use the measure data submitted by health IT developers to calculate the metrics (e.g., percentages and other related statistics). We intend that developers of certified health IT would submit this information to an independent entity, per statutory requirements in section 3009A(c) of the PHSA, as part of the implementation of the Insights Condition, which we discuss later in this section of the preamble.

For measures where patient encounters are relevant, we propose the definition of an encounter should be based on the National Committee for Quality Assurance (NCQA) outpatient value set and SNOMED CT inpatient encounter codes. For outpatient codes, developers should use NCQA's Outpatient Value Set.[324,325] For inpatient codes, developers should use SNOMED CT codes 4525004, 183452005, 32485007, 8715000, and 448951000124107.[326] Listed below is a description of each SNOMED CT code:

- Emergency department patient visit (procedure) – 4525004
- Emergency hospital admission (procedure) – 183452005
- Hospital admission (procedure) - 32485007
- Hospital admission, elective (procedure) - 8715000
- Admission to observation unit (procedure) - 448951000124107

We selected these value sets because they were recommended by HITAC[327] and were also recommended as part of Urban Institute's final report.[328] We seek comment on whether to define encounters in this manner, or include any type of visit (e.g., all encounters) in the measure denominator. Additionally, we seek comment on alternative approaches to measuring encounters.

Other shared requirements relate to similar sets of denominators across some of the measures. This should reduce burden associated with the measures. For example, the number of encounters during a reporting period is used as a denominator for the individual access to electronic health information measure, the immunization measures, and the clinical exchange measures.

---

[324] See: 2022 Quality Rating System Measure Technical Specifications. Published October 2021. https://www.cms.gov/files/document/2022-qrs-measure-technical-specifications.pdf.
[325] NCQA's Outpatient Value Set is available with a user ID and login at https://store.ncqa.org/my-2021-quality-rating-system-qrs-hedis-value-set-directory.html; or https://vsac.nlm.nih.gov/valueset/expansions?pr=all OID: 2.16.840.1.113883.3.464.1003.101.12.1087.
[326] Available for search at https://www.findacode.com/index.html.
[327] https://www.healthit.gov/sites/default/files/page/2021-10/2021-09-09_EHRRP_TF_2021__HITAC%20Recommendations_Report_signed_508.pdf.
[328] https://www.urban.org/sites/default/files/publication/105427/electronic-health-record-ehr-reporting-program-developer-reported-measures.pdf.

We refer readers to section III.F.4 of this preamble below for a discussion of the reporting period, reporting submission process, and other reporting requirements, that apply across measures associated with the Insights Condition's requirements.

Measurement Area: Individual Access to Electronic Health Information

A number of federal policies have sought to increase individuals' access to their EHI. In 2014, CMS' EHR Incentive Programs, supported by the Program, required participating hospitals and eligible health care providers to adopt certified EHR technology with capabilities that enable individuals to electronically view, download, and transmit their health information, which was largely implemented via a patient portal.[329,330] The ONC Cures Act Final Rule (85 FR 25642) set forth policies to make EHI more easily available by providing a way for certified health IT to include secure, standards-based APIs that enable individuals to access and better manage their health information using health applications (apps). Currently, individuals primarily view their EHI through a smartphone health app that is directly associated with their patient portal.[331] Patient portals and their associated apps can be offered by a health care provider (e.g., the clinician's office or a hospital) or through the developer of the certified health IT the health care provider uses. A number of studies have shown that patient engagement with EHI—such as through the use of patient portals—can help patients make informed decisions about their healthcare, facilitate communication with health care providers, improve adherence to medications, and lead to better health outcomes.[332,333,334]

---

[329] U.S. Department of Health and Human Services. Medicare and Medicaid Programs: Electronic Health Record Incentive Program – Stage 2. 2012 Sep. Available from: https://www.govinfo.gov/content/pkg/FR-2012-09-04/pdf/2012-21050.pdf.

[330] Office of the National Coordinator for Health Information Technology. Certification of Health IT. View, download, and transmit to 3rd party. Available from: https://www.healthit.gov/test-method/view-download-and-transmit-3rd-party.

[331] https://www.healthit.gov/data/data-briefs/individuals-access-and-use-patient-portals-and-smartphone-health-apps-2020.

[332] Dendere R, Slade C, Burton-Jones A, Sullivan C, Staib A, Janda M. Patient portals facilitating engagement with inpatient electronic medical records: a systematic review. Journal of Medical Internet Research. 2019 Apr 11;21(4):e12779.

[333] Shorter Hospital Stays Associated with Patient Portal Use. Epic Research. (November 17, 2021). Retrieved from: https://epicresearch.org/articles/shorter-hospital-stays-associated-with-patient-portal-use.

[334] James J. Patient engagement. Health Affairs Health Policy Brief. 2013 Feb 14;14(10.1377).

Given the national efforts made to advance the use of EHI with the goal of enhancing patient engagement and improving health outcomes, it is important to monitor the uptake and usage of EHI by individuals. ONC has largely relied on national surveys[335] to track progress in individuals' ability to access their health information using portals and apps. These surveys have provided insights into hospitals' ability to provide individuals with the capability to use portals and apps to manage their EHI, and subsequently individuals' self-reported use of these tools. However, these surveys have several limitations in the insights that they provide. Surveys of hospitals only provide insights on the capabilities to support individuals' access to EHI through portals and apps, rather than provide data on whether patients *use* those capabilities, which is critical to monitoring the success of ONC's and other efforts to increase patient engagement with EHI. Further, national surveys of physicians may not provide a complete picture of capabilities to support individuals' access to their EHI, as some physicians may not be knowledgeable about such capabilities. For example, in the 2019 National Electronic Health Records Survey,[336] a sizable percentage of office-based physicians indicated they do not know whether their health IT system enables their patients to view, download, or transmit their online medical records. These surveys also rely on self-reporting rather than using administrative data on the actual use of these functionalities. Lastly, patient surveys have largely examined the use of patient portals and apps directly associated with these portals but have had difficulty developing questions that provide insights into the access and use of third-party apps by individuals.[337]

Recently, third-party apps have emerged as an alternative method for individuals to view and manage their EHI. These apps are considered "third-party" because they are not directly associated with a health care provider or the developer of the provider's certified health IT, but instead are developed and marketed by an outside software developer. Some third-party apps

---

[335] https://www.healthit.gov/data/data-briefs/hospital-capabilities-enable-patient-electronic-access-health-information-2019.
[336] https://www.cdc.gov/nchs/data/nehrs/2019NEHRS-PUF-weighted-estimates-508.pdf.
[337] Johnson C, Richwine C, & Patel V. (September 2021). Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2020. ONC Data Brief, no.57. Office of the National Coordinator for Health Information Technology: Washington DC.

permit patients to view their EHI using certified API technology (as defined in § 170.404(c)) that integrates the app with information in the health care provider's certified health IT using the Health Level Seven (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standard, HL7 SMART Application Launch Framework and other associated standards and implementation specifications.

Given the different access methods that now exist, we propose an individuals' access to their EHI measure (as further discussed below) to require developers of certified health IT to report on the different methods individuals use to access their health information. This proposed measure would provide more detailed insights into the implementation and use of this capability by individuals, including whether and to what extent individuals are using third-party apps to access their EHI. We also seek to differentiate between individuals who access their EHI using these methods who had an encounter during the reporting period from those that did not have an encounter during the reporting period, as this differentiation would provide insights into usage for other convenience-oriented reasons (e.g., travel) that are not necessarily driven by a healthcare encounter.

Individuals' Access to Electronic Health Information Supported by Certified API Technology Measure

We propose to adopt the "Individuals' Access to Electronic Health Information Supported by Certified API Technology" measure within the "Individuals' Access to Electronic Health Information" area in § 170.407(a)(1). We propose to require that any developer of certified health IT with Health IT Modules certified to either the "view, download, and transmit to a 3rd party" certification criterion (§ 170.315(e)(1)), or the "standardized API for patient and population services" certification criterion (§ 170.315(g)(10)), report the numbers of unique patients that used each of the specified methods to access their EHI, unless eligible for subset reporting requirements discussed later in this section.

We propose two distinct numerators and three denominators as part of the measure in § 170.407(a)(1). As noted earlier in this section, we plan to generate multiple metrics from a combination of different numerators and denominators. We propose the first numerator to be the number of unique individuals who had an encounter and accessed their EHI at least once during the reporting period via at least one of three types of methods: (1) third-party app using technology certified to "standardized API for patient population services" certification criterion under § 170.315(g)(10); (2) patient portal using technology certified to the "view, download, and transmit to 3rd party" certification criterion under § 170.315(e)(1) only; or (3) app offered by the health IT developer or health care provider using technology certified to the API criterion under § 170.315(g)(10) (if applicable). We propose a second numerator to be the number of unique individuals who accessed their EHI regardless of an encounter during the reporting period using at least one of the same three types of methods identified above. Each of these numerators would be stratified or reported by type of method.

These proposed numerators differ from those developed by the Urban Institute by separating the numerators by individual encounter and EHI access status instead of by method. As explained above, this differentiation would provide insights into usage for other convenience-oriented reasons (e.g., travel) that are not necessarily driven by a healthcare encounter. In addition, we have replaced the third method proposed by the Urban Institute (Combination of third-party app desktop patient portal, and/or health care provider app) with apps offered by the health IT developer or health care provider. With both the numerators stratified by access method and the denominators separated by both encounter and access status, we believe that a combination measure is no longer needed. Our proposed third method will allow for distinction between third-party apps and those offered by health IT developers and health care providers. Overall, these proposed measures would still collect the data that the Urban Institute designed measures would obtain and give further interpretive strength, providing greater insights into how individuals are accessing their EHI.

We propose the first denominator for this measure to be the total number of unique individuals who had an encounter (as defined earlier in this preamble) during the reporting period. We propose the second denominator to be the total number of unique individuals who used at least one of the types of methods referenced above to access their EHI who had an encounter during the reporting period. We propose the third denominator to be the total number of unique individuals who used at least one of the three types of methods referenced above to access their EHI during the reporting period (regardless of whether the individual had an encounter or not).

The data collected for this specification would enable ONC to calculate the following metrics:

- Percent of individuals with an encounter who access EHI by the type of method
- Percent of individuals with an encounter who access EHI by at least one type of method
- Percent of all individuals who access EHI by at least one type of method

Our proposed measure would provide insight into the methods patients use to access their EHI through certified health IT. We believe this measure is important because as noted earlier in this section, increasing patients' access to their data can increase patient engagement and improve health outcomes.[338] The proposed measure seeks to measure patients' access to patient portals in a more refined manner than that proposed by the Urban Institute, which will provide insights on the shifts in methods used by individuals over time by differentiating apps that are directly associated with the health care provider or the developer of the provider's certified health IT from those that are not directly associated with the health care provider or health IT developer. We also seek to measure patients' access to patient portals in a manner that aligns with ONC's certification criteria regarding patient access to their EHI and differentiate between

[338] Health Affairs. (2013). Health Policy Brief: Patient Engagement. Accessed March 16, 2023, at: http://healthaffairs.org/healthpolicybriefs/brief_pdfs/healthpolicybrief_86.pdf.

apps provided by the health IT developer from those that are not provided by the health IT developer. We note that the proposed individuals' access measure does not distinguish between third-party apps selected by individuals versus third-party apps offered by health care providers, as these may be difficult to differentiate from each other.

We believe this proposed individuals' access measure will provide a national view into how individuals access their EHI and will inform ONC and health IT community efforts to empower individuals with access to their EHI. We welcome comments on our proposed measure.

Measurement Area: Clinical Care Information Exchange

We propose two measures under the "Clinical Care Information Exchange" area in §§ 170.407(a)(2) and (3). The proposed measures are titled, "Consolidated Clinical Document Architecture (C-CDA) Documents Obtained Using Certified Health IT by Exchange Mechanism" and "C-CDA Problems, Allergies and Medications Reconciliation and Incorporation Using Certified Health IT." These measures are primarily focused on characterizing the state of information exchange between health care providers who are customers of health IT developers with certified health IT, in contrast to other measures that capture exchange with individuals, public health agencies, and other entities.

Consolidated Clinical Document Architecture (C-CDA) Documents Obtained Using Certified Health IT by Exchange Mechanism Measure

There are numerous mechanisms by which information can be exchanged between organizations using certified health IT, such as point-to-point, developer network-facilitated, or through state health information exchange. Neither the current level of exchange by particular mechanisms nor trends of exchange by mechanism is clear. For example, the use of surveys to gather this information is limited. Based on a national survey analysis of hospitals,[339] on average hospitals reported using 3.6 methods to electronically send, 2.9 methods to receive and 2.4

[339] https://www.healthit.gov/data/data-briefs/use-certified-health-it-and-methods-enable-interoperability-us-non-federal-acute.

methods to query data from external sources. While this information is useful in that it provides some visibility into the number and types of mechanisms used, it does not provide insight into the volume of exchange by varied mechanisms at a national level as such information is not feasible to collect from end users. In contrast to measures of adoption which might not reflect intensive or beneficial use, data on the volume of information exchanged would provide the means to assess the extent that patient information is moving between providers to facilitate high value care. National surveys of physicians on health IT have not measured the types of methods used because physicians are not always aware of the specific mechanisms underlying the exchange of information, and hospitals do not always capture the volume of exchange being facilitated through various mechanisms.

Some health information networks do publish the volume of exchange they facilitate. For instance, DirectTrust[340] indicates that it facilitated exchange of 254 million messages in the fourth quarter of 2021 and Carequality[341] announced that it supported exchange of over 90 million documents in 2020. However, these headline numbers are difficult to interpret without also knowing the number of encounters occurring at sites using these methods, the number of patients being treated, and other measures of volume. Further, it is not clear whether these methods are exchanging unique information from different sources or prior encounters and thus should be added together or are largely exchanging duplicate information.

Therefore, we propose to adopt the "Consolidated Clinical Document Architecture (C-CDA) Documents Obtained Using Certified Health IT by Exchange Mechanism" measure, which would report on the volume of C-CDA documents obtained using certified health IT by exchange mechanism relative to patient volume. A developer of certified health IT with Health IT Modules certified to the "clinical information reconciliation and incorporation" certification

[340] https://directtrust.org/.
[341] https://carequality.org/carequality-reaches-new-milestone-of-one-billion-clinical-documents-exchanged/.

criterion in § 170.315(b)(2) would be required to report the proposed numerators and denominators for this measure.

There are four numerators and four denominators for this proposed measure. As noted earlier in this section, we plan to generate multiple metrics from different combinations of these numerators and denominators. For example, a single numerator can be used with two different denominators to produce two different metrics. We propose to adopt the following numerators for this measure: (1) number of unique C-CDA documents obtained (which we define for the purpose of this proposal as either C-CDAs that are received—that is, C-CDAs that have been sent or 'pushed' by others and received using certified health IT or C-CDAs that are queried—that is, C-CDAs that were found or 'pulled' from a network or central repository using certified health IT) using certified health IT and Direct Messaging[342] during the reporting period; (2) number of unique C-CDA documents obtained (received or queried) using certified health IT and a local/regional health information exchange (HIE) or national HIN during the reporting period; (3) number of unique C-CDA documents obtained (received or queried) using certified health IT and a developer-specific HIN (i.e., a network that facilitates exchange between entities using the same health IT developer's products) during the reporting period; and (4) number of unique C-CDA documents obtained (received or queried) using certified health IT and a method not listed above and not including electronic fax during the reporting period.

We propose to adopt the following denominators for this measure: (1) number of encounters during the reporting period; (2) number of unique patients with an encounter during the reporting period; (3) number of unique patients with an associated C-CDA document during the reporting period; and (4) number of unique C-CDA documents obtained (received or queried) using certified health IT during the reporting period. We propose to include denominators for the number of encounters during the reporting period and the number of unique patients seen (i.e., with an encounter) during the reporting period to provide a sense of the volume of C-CDA

[342] https://wiki.directproject.org/w/images/e/e6/Applicability_Statement_for_Secure_Health_Transport_v1.2.pdf.

documents exchanged relative to the number of instances when a C-CDA document might be useful. We believe these data points will provide complementary information against which to measure the volume of exchange. In contrast, an existing CMS measure, "Support Electronic Referral Loops by Receiving and Reconciling Health Information," originally finalized for clinicians in the Promoting Interoperability performance category of the MIPS in their CY2019 Physician Fee Schedule[343] "Revisions to Payment Policies under the Physician Fee Schedule" final rule (83 FR 59811) and for eligible hospitals and CAHs in the Promoting Interoperability Program in the FY2019 IPPS final rule[344] (83 FR 41661), is tied to notions of referral or transitions of care, which we are not proposing to reference in our proposed denominator. We believe that defining the scope of clinical scenarios in which a C-CDA document might be helpful is challenging, and effectively defining and identifying transitions of care and referrals in a consistent way across developers (as opposed to by clinicians or hospitals in the case of the CMS measures) may not be feasible. We instead use more general measures of unique patients or encounters. Again, we welcome comments on the proposed approach for reporting on encounters and alternatives to the proposed approach.

The data collected for this proposed measure would enable ONC to calculate the following metrics:

- The number of unique C-CDA documents obtained using a local/regional HIE or national HIN divided by the number of unique C-CDA documents obtained using certified health IT within the reporting period.

---

[343] "Medicare Program; Revisions to Payment Policies Under the Physician Fee Schedule and Other Revisions to Part B for CY 2019; Medicare Shared Savings Program Requirements; Quality Payment Program; Medicaid Promoting Interoperability Program; Quality Payment Program-Extreme and Uncontrollable Circumstance Policy for the 2019 MIPS Payment Year; Provisions From the Medicare Shared Savings Program-Accountable Care Organizations-Pathways to Success; and Expanding the Use of Telehealth Services for the Treatment of Opioid Use Disorder Under the Substance Use-Disorder Prevention That Promotes Opioid Recovery and Treatment (SUPPORT) for Patients and Communities Act."

[344] "Medicare Program; Hospital Inpatient Prospective Payment Systems for Acute Care Hospitals and the Long-Term Care Hospital Prospective Payment System and Policy Changes and Fiscal Year 2019 Rates; Quality Reporting Requirements for Specific Providers; Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs (Promoting Interoperability Programs) Requirements for Eligible Hospitals, Critical Access Hospitals, and Eligible Professionals; Medicare Cost Reporting Requirements; and Physician Certification and Recertification of Claims."

- The number of unique C-CDA documents obtained using developer-specific networks divided by the number of unique C-CDA documents obtained using certified health IT within the reporting period.
- The number of unique C-CDA documents obtained using Direct Messaging divided by the number of unique C-CDA documents obtained using certified health IT within the reporting period.
- The number of unique C-CDA documents obtained using other means divided by the number of unique C-CDA documents obtained using certified health IT within the reporting period.
- The number of unique patients with associated C-CDA documents obtained within the reporting period divided by the number of unique patients with an encounter within the reporting period.
- The number of unique C-CDA documents obtained using certified health IT within the reporting period divided by the number of unique patients with an encounter during the reporting period.
- The number of unique C-CDA documents obtained using certified health IT within the reporting period divided by the number of unique patients with an associated C-CDA documents obtained within the reporting period.
- The number of unique C-CDA documents obtained using certified health IT within the reporting period divided by the number of encounters during the reporting period.

This proposed measure would capture C-CDA documents obtained by electronic transport mechanisms, including national HINs (e.g., Carequality, CommonWell), state/ regional HIEs, Direct Messaging, and developer-specific networks (e.g., Epic Care Everywhere; athenahealth network). Additionally, we propose to measure the extent to which different exchange mechanisms are being used by volume of patients. In combination, this measure would

result in a patient-centered approach relative to existing measures of clinician or hospital adoption because it would provide insights into the degree to which electronic exchange of C-CDA documents is occurring relative to the volume of encounters and the number of patients whose data is exchanged by type of mechanism. This measure, together with the proposed measure related to C-CDA Problems, Allergies and Medications Reconciliation and Incorporation Using Certified Health IT, would provide a foundation for understanding how often external information is exchanged and used in certified health IT.

Using data gathered under this measure, we would also be able to examine trends in the use of various mechanisms for exchange of health information over time. Monitoring the volume of exchange by various mechanisms is critical to monitoring the implementation of key ONC policies that support exchange and interoperability, including most recently TEFCA (87 FR 2800). ONC seeks to facilitate exchange so that interoperability is best supported. Understanding varying usage of different mechanisms could better inform ONC policies because not all exchange mechanisms may adequately support true interoperability. Understanding where the market is with regards to the usage of exchange mechanisms that support interoperability (versus those that do not) is critical to informing ONC policy. Furthermore, examining variation in usage of exchange mechanisms can provide insights into what mechanisms may be limited to certain use cases, and whether some mechanisms implicitly or explicitly favor some parties (e.g., developer exchanges). Thus, information on exchange by mechanism will allow ONC to better target its support for interoperable exchange. Furthermore, these data can be used by ONC to assess the impacts of these various efforts, including the role certified health IT plays in supporting exchange through various mechanisms. The Program supports a number of different exchange mechanisms; understanding their uptake and use is important for informing future development and improvements.

We seek comment on whether it would be meaningful to further reduce the mechanisms of exchange measure into fewer categories, by combining regional HIE and/or national HIN and

developer-specific HINs into one category (network-mediated exchange) and combining Direct Messaging and "other methods" into a second category (exchange directly between two entities). Thus, an alternative proposal would be to reduce the exchange mechanisms from three categories to two categories. We also seek comment on whether the expected burden associated with this measure would, in practice, be reduced if the number of categories were reduced.

C-CDA Medications, Allergies, and Problems Reconciliation and Incorporation Using Certified Health IT Measure

We propose to adopt the "C-CDA Medications, Allergies, and Problems Reconciliation and Incorporation Using Certified Health IT" measure, which would capture the number of C-CDA documents that are reconciled and incorporated (as defined in § 170.315(b)(2)(iii)) as part of a patient's record by clinicians or their delegates. A developer of certified health IT with Health IT Modules certified to the "clinical information reconciliation and incorporation" certification criterion in § 170.315(b)(2) would be required to provide information on how data in C-CDA documents are used, focusing on the reconciliation and incorporation of medications, allergies and intolerances, and problems.

We propose the numerator to be the total number of C-CDA documents of the Continuity of Care Document (CCD), Referral Note, Discharge Summary document types that are obtained and incorporated across all exchange mechanisms supported by the certified health IT during the reporting period. The numerator would increment, or increase in number, upon completion of clinical information reconciliation of the C-CDA documents for medications, allergies and intolerances, and problems, as described in the certification criterion in § 170.315(b)(2).

We propose the denominators for this measure to match the denominators for the "C-CDA Documents Obtained Using Certified Health IT by Exchange Mechanism" proposed measure, using the definition of "encounter" described previously in this proposal. The data collected for this proposed measure would enable ONC to calculate the following metrics:

- The total number of C-CDA documents (CCD, Referral Note, Discharge Summary) obtained and incorporated divided by the number of encounters during the reporting period.
- The total number of C-CDA documents (CCD, Referral Note, Discharge Summary) obtained and incorporated divided by the number of unique patients with an encounter during the reporting period.
- The total number of C-CDA documents (CCD, Referral Note, Discharge Summary) obtained and incorporated divided by the number of unique patients with an associated C-CDA document during the reporting period.
- The total number of C-CDA documents (CCD, Referral Note, Discharge Summary) obtained and incorporated divided by the number of unique C-CDA documents obtained (received or queried) using certified health IT during the reporting period.

This proposed measure can be used to inform the extent to which information is being incorporated into a patient's record as discrete data that is trackable over time. Our proposed measure includes several metrics intended to directly measure the success of certified health IT in supporting reconciliation and incorporation of C-CDA documents. Our specifications are intended to ensure the measure captures several key dimensions of information reconciliation. First, we intend the measure to capture the success of certified health IT at facilitating maintenance of a patient's record composed of discrete data that is trackable over time through the incorporation of medications, allergies and intolerances, and problems into the medical record as appropriate. This would help us understand the degree to which information received from C-CDA documents is subsequently available for use after receipt and incorporation. Second, the measure is intended to provide a national view of information reconciliation by users of certified health IT. Third, the measure is intended to capture the incorporation of all available C-CDA documents and is not tied to specific events such as transitions of care. We believe that

developers may vary in their approach to defining transitions of care (and other events like referrals), which may make it more difficult to comprehensively capture the reconciliation of medications, allergies intolerance, and problems. Fourth, we intend the measure to capture the extent to which unique C-CDA documents are reconciled, as we are aware that in the current landscape, some clinicians and hospitals are able to receive C-CDA documents through multiple methods and it is possible to receive multiple copies of the same C-CDA (i.e., via Direct Messaging and an HIE). We believe that by only including unique C-CDA documents in both the numerator and denominator, we will avoid undercounting reconciliation. If duplicates were not excluded, undercounting would be likely because relevant denominators (e.g., the number of C-CDAs obtained) would be larger due to the inclusion of duplicate documents for which reconciliation and incorporation (i.e., the numerator) would not offer clinical value and be infrequent. Lastly, we intend the measure to capture the rate of C-CDA documents reconciled relative to several alternative denominators, including the number of C-CDA documents received and the number of unique patients treated. We believe that these alternative denominators provide important complementary information on the extent of information exchange.

This measure is closely related to a measure used by CMS in the Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program. CMS generally describes their measure "Support Electronic Referral Loops by Receiving and Incorporating Health Information" (originally finalized in 83 FR 59811 and 83 FR 41661, respectively) as capturing the rate at which problems, medication allergies, and medications were reconciled and incorporated out of all transitions of care or referrals for which a health care provider received an electronic summary of care record. In contrast to the CMS measure, our proposed measure would provide a more nationally representative view of the use of certified health IT since many clinicians, including those in small practices, do not report for the Promoting Interoperability performance category of MIPS. Among those that do report for the Promoting Interoperability performance category of MIPS, many do not report this

information, either because they claim an exclusion from reporting the measure or they report on the optional Health Information Exchange (HIE) Bi-Directional measure in lieu of reporting performance on the Support Electronic Referral Loops by Receiving and Incorporating Health Information measure.[345] As a result, the Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program data alone provides an incomplete view of the degree to which health care providers successfully incorporate C-CDA documents. Our measure would provide a broader measure of incorporation of information in C-CDAs that, unlike the CMS measure, is not tied to transitions of care, referrals, or new patient encounters.

We note that a majority of developers of certified health IT should already be capable of supporting some components of our proposed measure because of the existing requirements for the Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program and ONC certification criteria related to measuring exchange under "automated numerator recording" (§ 170.315(g)(1)) and "automated measure calculation" (§ 170.315(g)(2)). We note that approximately 68% (517 of 818) of Health IT Modules listed on CHPL are certified to one or both of these criterion as of the second quarter of the 2022 calendar year. Therefore, we believe our proposed measure should impose a low burden on a majority of developers of certified health IT to fully implement as part of this Insights Condition. We request comment on the anticipated burden associated with this measure.

We request comment on whether focusing on the three types of C-CDA documents described above in the proposed numerator (CCD, Referral Note, Discharge Summary) would impose a substantial burden beyond summary of care records. We request comment on the value of focusing on these three document types relative to all types of summary of care records. We also request comment on whether meaningful measures could be generated without de-duplication of C-CDAs, how often duplicate C-CDA documents may be obtained by customers

[345] Analysis of the publicly available 2020 Quality Payment Program Experience Data available here Quality Payment Program Experience - Centers for Medicare & Medicaid Services Data (cms.gov) indicates that 172,786 of 921,517 clinicians reported on this measure.

of certified health IT, and how much of a burden it will impose on developers of certified health IT to ensure that C-CDA documents are not duplicates.

Measurement Area: Standards Adoption and Conformance

We propose to adopt four measures in the "Standards Adoption and Conformance" area in §§ 170.407(a)(4) through (7) to provide insight into the role that standards play in enabling access, exchange, and use of EHI. We propose to measure the following aspects within this area: (1) availability of apps to support access to EHI for a variety of purposes; (2) the usage of FHIR-based APIs to support apps; (3) the use of bulk FHIR to support the access to EHI for groups of individuals; and (4) the use of EHI export functionality. Together, these measures would provide a foundation for understanding whether and to what extent ONC's policies to promote standards are supporting users of health IT, including patients, clinicians, researchers, and others, to access and use EHI via certified health IT for a variety of purposes. These measures would also provide visibility into industry adoption of standards required by the Program and provide data to inform future standards development work.

Applications Supported Through Certified Health IT Measure

We propose to adopt an "Applications Supported Through Certified Health IT" measure, which would provide information on how certified health IT is supporting the health app ecosystem by asking certain health IT developers under the Program to report app names and app developer names, intended app purposes, intended app users, and whether a registered app is in "active" use across a developer's client base (as further detailed below). This measure would result in a listing of apps that could be used to generate a variety of metrics. Only developers of certified health IT with Health IT Modules certified to the "standardized API for patient and population services" (§ 170.315(g)(10)) certification criterion would be required to report data for this proposed measure.

As there is currently no comprehensive source of this type of information, we believe that data reported through this measure would provide greater transparency regarding the apps that

are connected to certified health IT. This measure will provide information on most apps connected to developers of certified health IT with Health IT Modules certified to § 170.315(g)(10), including the types of intended users of these apps and the number of apps available that are in "active use." Some health IT developers of certified health IT currently have public app galleries;[346] however, the apps in public app galleries only represent a subset of apps connected to their APIs, and only a small subset of health IT developers have public app galleries. The information captured under this measure would go beyond the data currently publicly available in these app galleries and must include all apps connecting to certified health IT certified to § 170.315(g)(10), regardless of whether an app is currently publicly available in an app gallery or not. We note that this measure would also be required for health IT developers of certified health IT that do not currently maintain an app gallery.

Therefore, we propose that developers of certified health IT with Health IT Modules certified to § 170.315(g)(10) provide the following information about the apps that are connected to their certified technology. We propose that the app name and the developer (company/organization or individual) responsible for the app shall be reported for each app registered to a developer of certified health IT whose Health IT Module is certified to the § 170.315(g)(10) criterion. We note that the app registration process required under § 170.315(g)(10)(iii) may provide an opportunity for developers of certified health IT to gather standard information for apps connecting to their certified API technology as part of existing workflows. There may be other mechanisms besides the app registration process by which developers of certified health IT wish to obtain this information.

This measure would enable ONC and the public to understand to what degree apps are able to connect across different certified health IT products. The ONC Cures Act Final Rule (85 FR 25750) emphasized the importance of standardization, transparency, and pro-competitive

[346] The ecosystem of apps and software integrated with certified health information technology: https://academic.oup.com/jamia/article/28/11/2379/6364773?login=false.

business practices through the API Condition and Maintenance of Certification requirements that would make it easier for third-party apps to connect to certified health IT, and subsequently facilitate individuals' access to their EHI. By collecting the names of apps and developers connecting to developers of certified health IT whose Health IT Module is certified to § 170.315(g)(10), ONC and the public will be better able to identify whether certain apps are only connecting to one certified health IT product versus other apps that may be connecting to multiple different certified health IT products. This information provides insights into whether apps are able to connect to a variety of certified health IT products, which is important for enabling individuals' access to their EHI.

We propose that developers of certified health IT with Health IT Modules certified to § 170.315(g)(10) obtain and report the intended purpose(s) for each app connected to their certified API technology using the following categories:

- Administrative Tasks (e.g., scheduling & check-in, billing & payment)
- Clinical Tools (e.g., clinical decision support, risk calculators, remote patient monitoring)
- Individuals' Access to their EHI (e.g., enables patients to access their health information, medications, test results, vaccine records)
- Research (e.g., used to perform clinical research)
- Population Data (e.g., bulk transfer of data, population analytics & reporting)
- Public Health (e.g., electronic case reporting)
- Patient-Provider Communication (e.g., secure messaging, telehealth)
- Educational Resources (e.g., patient and provider educational resources)
- Other Intended Purpose
- Unknown (e.g., missing)

Developers of certified health IT to whom the measure applies would report the intended purpose(s) of the app for each app registered to their Health IT Module(s) certified to the §

170.315(g)(10) criterion. The categories we propose under this measure were informed by app category taxonomies in published literature from Barker & Johnson (2021),[347] Ritchie and Welch (2020)[348] and Gordon and Rudin (2022).[349] While we recognize this taxonomy may need to evolve over time, we believe the proposed categories represent a large majority of the current market. Understanding apps' intended purpose sheds light on the types of apps that are available. For example, based upon the prior analyses of these public app galleries, about one-fifth of apps in public app galleries supported patient engagement, whereas about four in ten were for administrative purposes. Although, as noted previously, the data source underlying these analyses are incomplete. The types of information, if reported on a complete set of apps, would provide insightful information to guide ONC's future efforts to support individuals' access to their EHI via apps, along with other priority uses, such as for research and clinical care. We welcome feedback on what alternative or additional functionalities should be included in the taxonomy to characterize the intended purpose of health apps.

We propose that developers of certified health IT with Health IT Modules certified to § 170.315(g)(10) obtain the following intended user(s) categories for each app connected to their certified API technology:

- Individual/Caregiver
- Clinician
- Healthcare Organization
- Payer
- Researcher
- Other Intended User

---

[347] The ecosystem of apps and software integrated with certified health information technology: https://academic.oup.com/jamia/article/28/11/2379/6364773?login=false.
[348] Categorization of Third-Party Apps in Electronic Health Record App Marketplaces: Systematic Search and Analysis: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7293052/.
[349] Gordon WJ, Rudin RS. Why APIs? Anticipated value, barriers, and opportunities for standards-based application programming interfaces in healthcare: perspectives of US thought leaders. JAMIA Open. 2022 Apr 6;5(2):ooac023. doi: 10.1093/jamiaopen/ooac023. PMID: 35474716; PMCID: PMC9030107.

- Unknown (e.g., missing)

These proposed categories include a variety of users and would provide a better understanding of the extent to which apps are available and in use for different types of users, since the intended purpose alone may not shed light on the types of users for which the app is intended. For example, some apps intended for research purposes may have both patients and researchers as users, whereas others may be intended for research alone. It is important to understand the breadth of intended users of apps to provide insights into the impacts of ONC's efforts on users' ability to access EHI via certified API technology through apps.

We propose that developers of certified health IT with Health IT Modules certified to § 170.315(g)(10) obtain the status for each app connected to their certified API technology using the following categories:

- Actively Used – An app is defined as "Actively Used" if EHI has been transferred to the app using certified API technology for 10 or more unique patients during the reporting period
- Not Actively Used – An app is defined as "Not Actively Used" if EHI has been transferred to the app using certified API technology for fewer than 10 unique patients during the reporting period

We recognize that apps registered to certified API technology may not necessarily be in production nor have any users, and thus an indicator of active use would be important to differentiate those apps in use, versus those not ready for use (or that may never make it to that stage). This will provide an accurate indicator of the availability of apps based upon the usage activity. Without this indicator of active use, we would not know if an app was registered but never in production, and thus the value of the overall data would be limited. We welcome comments on our proposed "active use" status categories, including their definitions, and welcome comment on whether these categories reflect how app status is currently monitored by developers of certified health IT.

We believe our proposed measure would provide information that would be useful to guide future policy and assess ongoing efforts to support app connectivity to certified health IT. This data would also provide insight into whether and how impactful ONC standards and policies are to expanding the availability of apps, including the "standardized API for patient and population services" (§ 170.315(g)(10)) certification criterion. Additionally, this measure would produce a list of apps that would provide information on the degree to which apps are able to connect to multiple different certified health IT systems in a seamless manner. We believe capturing this information over time would provide insights into the evolution of the types of apps that are available for meeting the needs of various end users of app technology to support a variety of critical purposes. We welcome comments on our proposed measure.

Use of FHIR in Apps Supported by Certified API Technology Measure

We propose to adopt a "Use of FHIR in Apps Supported by Certified API Technology" measure, which would capture the volume of FHIR resources transferred in response to API calls from apps connected to certified API technology by FHIR resource type. We also propose that the volume of FHIR resources transferred be reported by FHIR version used and by U.S. Core Implementation Guide version deployed. This measure would also require developers to report FHIR resources transferred in response to calls from two different endpoint types: patient-facing and non-patient-facing, the latter of which would include endpoints that do not facilitate individuals' access (e.g., clinician, payer, or public health endpoints). Finally, this measure would require developers of certified health IT with Health IT Modules certified to the "standardized API for patient and population services" (§ 170.315(g)(10)) certification criterion to report on the number of deployments they support across their customer base. Together, these data points would provide insights into the usage of certified APIs by collecting data on the volume of FHIR resources transferred to apps in response to API calls by FHIR resource type, type of endpoint, and U.S. Core Implementation Guide used. We believe this information could provide useful information in understanding the adoption of FHIR and the utility of specific FHIR resources.

This information could also be informative to industry-based standards development efforts in the future. We also believe it is possible to collect these kinds of data, based on some of the real world testing plans submitted by developers of certified health IT in December 2021.[350]

Similar to other measures, we propose a number of numerators and denominators that would be used to generate a variety of metrics. We propose the first numerator to be the number of FHIR resources returned/transferred in response to a call to a certified API technology by resource type. We propose the second numerator to be the number of distinct certified API technology deployments (across clients) associated with at least one FHIR resource returned/transferred in response to a call. We note that each of the numerators would be stratified (e.g., divide into subsets) by type of endpoint (patient-facing vs. non-patient-facing), by FHIR version, and by U.S. Core Implementation Guide.

We propose the denominator to be the total number of distinct certified API technology deployments (across clients). In addition, we propose this denominator to be stratified by type of endpoint (patient-facing vs. non-patient facing), FHIR version, and U.S. Core Implementation Guide. We note that non-FHIR APIs, such as those represented with proprietary standards, are excluded from this measure, including numerators and denominators.

The data collected for this proposed measure would enable ONC to calculate the following metrics:

- Percent of data transferred by type of FHIR resource for non-patient-facing APIs overall, by FHIR resource version and by U.S. Core Implementation Guide
- Percent of data transferred by type of FHIR resource for patient-facing APIs overall, by FHIR resource version and by U.S. Core Implementation Guide

[350] See Real World Testing plans available at: https://chpl.healthit.gov/#/collections/real-world-testing.

- Percent of certified API technology deployments where data was transferred for non-patient-facing APIs overall and by FHIR resource version and by U.S. Core Implementation Guide
- Percent of certified API technology deployments where data was transferred for patient-facing APIs overall and by FHIR resource version and by U.S. Core Implementation Guide
- Percent of certified API technology deployments by FHIR resource version and by U.S. Core Implementation Guide

This proposed measure could be used to monitor progress related to ONC's efforts to make EHI accessible through standardized APIs. The implementation of the "standardized API for patient and population services" certification criterion in § 170.315(g)(10) plays an important role in our approach to nationwide access, exchange, and use of EHI without special effort. As industry implements standard APIs for patient and population services, it is important to understand (1) the extent to which health IT capabilities are in place to support access to EHI via FHIR-based APIs; (2) the degree to which those capabilities are available to be used; and (3) the use of those capabilities in practice.

We are currently using multiple data sources to measure the use of FHIR in apps supported by certified API technology. By using data from the CHPL, CMS program data, and national survey data of hospitals, ONC has conducted analyses that provide insights into the capabilities of certified health IT to support FHIR APIs. Through the Lantern Project,[351] we will eventually have the means to analyze Capability Statements[352] made available through health IT developers' published service-based URLs for patient-facing endpoints that could provide insights on whether these available capabilities were actually "turned on" so that they can be used.

---

[351] https://lantern.healthit.gov/?tab=dashboard_tab.
[352] https://www.hl7.org/fhir/capabilitystatement.html.

The proposed measure would build on these other data sources and add to our collective understanding by assessing to what degree these capabilities are used in practice, as well as provide ONC and the public with data on the usage of certified API technology by capturing the number and types of FHIR resources that are transferred in response to an API call or request. We chose to propose the number of FHIR resources transferred instead of API calls because we believe data transfers will be an auditable event captured by health IT developers of certified health IT. We also believe that the number of FHIR resources transferred is a better reflection of use as this data would provide insights into the types of data elements or resources that are most frequently (and least frequently) used by end users of certified API technology. We believe this measure would have the potential to guide ONC's standards development efforts in the future. For example, the resource data would help SDOs and ONC prioritize resources that may need refinement. Although we have previously researched and tracked the total number of apps connecting to APIs managed by health IT developers of certified health IT using publicly available data from health IT app galleries, very little information has been reported on the volume of data transferred using certified API technology by end-users. This data is not easily measured using other data collection methods; however, it is our understanding that many health IT developers of certified health IT are already collecting this information using system-generated data (e.g., log audit data).

Requiring health IT developers of certified health IT to report FHIR resources transferred in response to calls from two different endpoint types, patient-facing endpoints and non-patient-facing (e.g., clinician, payer, or public health endpoints), would provide insights into the types of data elements used by patients as compared to other types of users. This information would allow ONC to develop more targeted efforts that address patient needs for different types of data as compared to other users.

As stated above, this proposed measure would also require that developers report the volume of FHIR resources transferred in response to calls by FHIR version and by U.S. Core

Implementation Guide. While Health IT Modules certified to § 170.315(g)(10) are required to respond to requests according to FHIR version Release 4, we are aware that in the future there will be newer versions of FHIR supported by newer versions of the U.S. Core Implementation Guide. Gaining insights into the frequency in use of U.S. Core Implementation Guides would help inform ONC regarding variability in the implementation of FHIR across developers. Having these measures stratified by FHIR resource version, in addition to the U.S. Core Implementation Guide, could help ONC advance the use of FHIR APIs. Knowing which FHIR and U.S. Core Implementation Guides are in use would provide insights into where the industry is currently, and where it may be headed with regards to the implementation of specific versions of FHIR.

We request feedback on whether information on both aspects of the measure, FHIR version and U.S. Core Implementation Guide, are necessary as each provides unique insights or whether focusing on just one of these (either FHIR version or U.S. Core Implementation Guide) would be feasible and sufficient for understanding where the industry is with regards to the implementation of FHIR. We also seek comment on the feasibility of reporting the use of different HL7 FHIR implementation guides and FHIR versions overall, versus stratified by type of endpoint, type of FHIR resources, and by the number of certified API technology deployments.

Finally, as this proposed measure would require developers to report on the number of certified API technology deployments they support across their customer base, we believe it is important to examine usage not only at the product level of a health IT developer with certified health IT, but also across the organizations that are using those products. Therefore, we propose to require health IT developers of certified health IT to whom the proposed measure would be applicable to report the number of certified API technology deployments (as a proxy for organizations that have installed certified API technology) where FHIR resources were transferred in response to a call (relative to the total number of certified API technology deployments). This information can shed light on whether usage is concentrated versus

dispersed, indicating the breadth of usage across end users and organizations. However, given that API deployments may vary across developers, we seek feedback on whether this measure would be a good proxy for understanding usage across their client bases. Overall, data on the usage of FHIR resources by type of resource, endpoint, version, and U.S. Core Implementation Guide, would provide greater transparency and insights on the availability and use of different data elements available through certified API technology. In addition, we would also be able to monitor trends as data is reported over time and gain a sense of whether and how useful standards required by the "standardized API for patient and population services" certification criterion are to understanding the state of health data interoperability. We welcome comments on our proposed measure.

Use of FHIR Bulk Data Access through Certified Health IT Measure

We propose to adopt the "Use of FHIR Bulk Data Access through Certified Health IT" measure, which would measure the number of bulk data downloads completed through certified health IT relative to the number of certified health IT deployments or installations. Specifically, this measure would provide information on how certified health IT is being used to perform "read" services for a specified patient population using the HL7® FHIR® Bulk Data Access (Flat FHIR) V1.0.1 standard. A developer of certified health IT with Health IT Modules certified to the "standardized API for patient and population services" (§ 170.315(g)(10)) certification criterion would be required to report under this proposed measure.

We propose the first numerator to be the number of data/download requests completed during the reporting period using certified health IT certified to the "standardized API for patient and population services" (§ 170.315(g)(10)) in response to a bulk data download request to export all data for patients within a specified group. We propose the second numerator to be the number of distinct certified health IT deployments or installations certified to the "standardized API for patient and population services" (§ 170.315(g)(10)) (across clients) that successfully completed at least one bulk data download request during the reporting period.

We propose the denominator to be the total number of distinct certified health IT deployments or installations (across clients).

The data collected for this proposed measure would enable ONC to calculate the following metrics:

- Percent of certified health IT deployments or installations with at least one successfully completed bulk data download request.
- Rate of bulk data download requests successfully completed per certified health IT deployments or installations.

Our current ability to measure the Bulk FHIR access is limited to using national survey data through which hospitals self-report on their capabilities. Such survey data does not provide insight into use of this capability across other settings, nor do we have insights into the frequency of use and for what type of requests. We believe this measure would address these gaps in measurement and provide transparency on the use of certified health IT to export all data for a specified patient population. The trends that this measure would allow us to determine the extent to which the HL7® FHIR® Bulk Data Access (Flat FHIR) V1.0.1 standard has been adopted over time. Additionally, this proposed measure would provide insights on the extent to which the "standardized API for patient and population services" (§ 170.315(g)(10)) certification criterion supports use of API-enabled "read" services for a specified patient population. For future measure development, in order to track and better understand the use of API-enabled "read" services for multiple patients, we seek comment on whether additional stratifications would provide valuable insights, what additional data are developers of certified health IT collecting; and what effort developers of certified health IT are devoting to collecting additional data such as: (1) intended use case (e.g., population analytics, reporting, research); (2) entity calling the API (e.g., healthcare organization, payer, public health agency); and (3) automated queries (refreshing the data at certain intervals) vs. ad hoc queries. For future measure development, we also seek comment on whether it is possible to collect information on the number of authorized

users calling a bulk FHIR API, the level of effort required to collect this information, and whether it would provide valuable insights.

We also note and clarify that non-standard or proprietary resources (e.g., non-FHIR based) transferred would be excluded from this measure, and that we propose data for this measure would not include patient-facing applications, as individual patients only have the right to access their own records or records of patients to whom they are a personal representative. We welcome comment on our proposed measure.

Electronic Health Information Export through Certified Health IT Measure

We propose to adopt the "Use of Electronic Health Information Export through Certified Health IT" measure which would capture the use of certified health IT to export single patient and patient population EHI. A developer of certified health IT with Health IT Modules certified to the "electronic health information (EHI) export" (§ 170.315(b)(10)) certification criterion would be required to report data under this proposed measure.

We propose a count for this measure (rather than a numerator and denominator) that includes the number of full data EHI exports requests processed during the reporting period and reported by the following subgroups: (1) by a single patient EHI export; and (2) by patient population EHI export. While this stratification differs from what the Urban Institute reported, we believe that it will give more precise insights into how the EHI export certification criterion is used. We also propose reports should include a "yes" or "no" attestation for enabling direct-to-individual EHI exports.

The data collected for this proposed measure would enable ONC to calculate the following metrics:

- Count of full data EHI export requests processed by single patient and patient populations requests.
- Whether or not the certified Health IT Module supports direct-to-individual EHI exports.

The EHI export certification criterion in § 170.315(b)(10) requires that certified health IT have the capability to export single patient and population-level data. This function provides a means for patients to obtain copies of their EHI and equips health care providers with better tools to transition patient EHI from one health IT system to another. The proposed measure would report on the number of EHI export requests processed by a health IT developer and provide insights on the implementation of the EHI export capability. Current data sources to provide insights on the use of the EHI export function are limited, and our experiences with surveys of health care providers indicate that many health care providers, particularly office-based clinicians, may not be familiar with the technical terminology, and thus survey data would not serve as a useful data source for the use of this functionality. Therefore, by requiring data to be reported under this measure, we would be able to understand if the capability is functioning in the market as intended. We welcome comments on our proposed measure.

We noted in the ONC Cures Act Final Rule (85 FR 25695) that the EHI Export certification criterion in § 170.315(b)(10) does not require "direct-to-patient" functionality in order for a developer to demonstrate conformance to the criterion. However, we did not preclude this functionality, and we seek comment as part of this proposed rule on whether any products support direct-to-patient EHI Export functionality to inform future policy decisions. We also seek comment on whether it would be valuable for this measure to be reported by "use case" for why the data was exported (e.g., moving to another certified health IT system, use for a population health tool), and how feasible would it be for impacted developers to report in this manner. Lastly, we seek comment on whether it would be valuable, and if so, how valuable, for this measure to include reports regarding the types of recipients (e.g., patients, organizations) of the exported data, and how feasible would it be for impacted developers to report this data in this manner.

Measurement Area: Public Health Information Exchange

The COVID-19 pandemic has exposed many gaps and challenges in the nation's public health infrastructure, including a need for more accurate and timely data, increased electronic exchange of patient health information between health care providers and public health agencies, and greater support for vulnerable individuals and communities disproportionally affected by the pandemic.[353] Therefore, we propose two measures within the "Public Health Information Exchange" area in proposed §§ 170.407(a)(8) and (9) for reporting health care providers' use of certified health IT to exchange data with an immunization information system (IIS). The insights from these measures could help ONC (and HHS more broadly) assess the public health capabilities of certified health IT. While ONC has attempted to capture similar data via surveys, sample size and health care providers' level of knowledge regarding their health IT systems' capabilities have limited the ability to generate insights. For example, a national survey of office-based physicians' use of health IT in 2019 found that twenty-five percent of physicians who participated in the survey responded "Don't Know" to questions about electronic public health data exchange[354]. Furthermore, the proposed measures go beyond the Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program's measurement of "active engagement" with public health agencies, which does not indicate the volume of data successfully transmitted to public health agencies or address immunization queries made by heath care providers.

Our proposed public health information exchange measures would address these gaps by measuring whether and to what extent providers are using their certified health IT to electronically send and receive public health information to and from public health agencies. We believe that more detailed measurement of health care providers' ability to use certified health IT

---

[353] Dixon BE, Rahurkar S, Apathy NC. Interoperability and health information exchange for public health. In Public health Informatics and information systems 2020 (pp. 307-324). Springer, Cham. https://doi-org.ezproxyhhs.nihlibrary.nih.gov/10.1007/978-3-030-41215-9_18.

[354] Richwine C., Dustin, C., & Patel, V. (August 2022). Electronic Public Health Reporting & Recording of Social & Behavioral Determinants of Health Among Office-Based Physicians, 2019. ONC Data Brief, no.60. Office of the National Coordinator for Health Information Technology: Washington DC. https://www.healthit.gov/data/data-briefs/electronic-public-health-reporting-recording-social-behavioral-determinants-health.

to successfully exchange health information with public health agencies would provide critical data for pandemic response and other public health emergencies.

Immunization Administrations Electronically Submitted to an Immunization Information System through Certified Health IT Measure

In furtherance of our efforts to assess public health exchange, we propose to adopt a public health exchange measure that would report on the volume of immunization administrations electronically submitted to an immunization information system through certified health IT. This measure would capture the use of certified health IT to send information on vaccination and immunization administrations to an IIS. Specifically, this measure would require health IT developers of certified health IT with Health IT Modules certified to the "transmission to immunization registries" (§ 170.315(f)(1)) criterion to report on the number of records of immunizations administered that were sent electronically to an IIS during the reporting period. We propose that developers of certified health IT with Health IT Modules certified to § 170.315(f)(1) that do not have users that administered immunizations during the reporting period would attest that they are unable to report on this measure.

The intent of the proposed "Immunization Administrations Electronically Submitted to an Immunization Information System through Certified Health IT" measure is to ensure that ONC has the information necessary to assess whether Health IT Modules certified to § 170.315(f)(1) are being used to support electronically sending vaccination information data to IIS, which has proven to be critical to public health preparedness and response. While ONC has attempted to capture similar data via surveys, the data is limited by sample size and may not fully reflect certified health IT usage for exchanging data with an IIS since survey-based data does not provide information on actual usage. Thus, our proposed measure would give a more complete view of sending data to an IIS. In addition, this proposed measure goes beyond the Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program's measurement of "active engagement," which does not indicate the volume of data

successfully transmitted to public health agencies. Our proposed measure would address these information gaps by measuring transactions whereby health care providers use their certified health IT to electronically send public health information on vaccines administered to public health agencies.

For the numerator, we propose developers of certified health IT with Health IT Modules certified to § 170.315(f)(1) report the number of immunization administrations from which the information was electronically submitted to an IIS successfully during the reporting period by IIS and age group. We propose that the numerator and denominator counts would be reported overall (across IIS and age subgroups) and by the following subgroups: (1) number of administrations by IIS; and (2) number of administrations by IIS and age group (adults (18 years and over) and children/infants (17 years and under)). The definition of a successful submission to an IIS would be the total number of messages submitted minus acknowledgments with errors (2.5.1, severity level of E). We believe this definition will avoid limitations from IIS jurisdictions that do not send HL7 Acknowledgment messages (ACKs) for this measure. Given that we propose that ACKs with an error (severity level of E)[355] would not be counted, we seek comment on whether ACKs with a warning (severity level W) should still be counted in the numerator. We also seek comment on whether the number of immunizations administered can be linked to immunizations submitted to the IIS, effectively creating a subset of the numerator (immunizations administered). Additionally, we seek comment on whether a successful submission should be counted if a health care provider is able to successfully submit to at least one registry, as opposed to all the registries they submitted to (e.g., health care providers who operate in multiple states sending data for the same administration to multiple IISs).

We are also considering whether "replays," which involve resubmitting administrations until they are successfully submitted, qualify as a successful submission. In other words, we seek

[355] HL7 Version 2.5.1. Implementation Guide for Immunization Messaging. Release 1.5. October 1, 2014. https://www.cdc.gov/vaccines/programs/iis/technical-guidance/downloads/hl7guide-1-5-2014-11.pdf.

comment on whether successful submissions should be limited to the first attempt to submit. We believe "replays" should qualify as a successful submission since the purpose of this proposed measure is to identify administrations successfully submitted, not necessarily those submitted on the initial try, and welcome public comment on this.

We propose the denominator for this measure to be the number of immunizations administered during the reporting period. We propose this denominator be stratified by the following subgroups: (1) number of administrations reported to each IIS; and (2) number of administrations reported to each IIS, by age group (adults (18 years and over) and children/infants (17 years and under)). This measure differs from that developed by the Urban Institute by the inclusion of stratifications by IIS and age group. Given the variation in immunization reporting requirements and patient consent by state or jurisdiction, reporting of administrations by IIS is critical to interpreting the data correctly, therefore we propose this measure to be stratified by IIS. In addition, given that immunization requirements are different for children and adults, we propose stratifying by age group as well. Reporting by these subgroups will assist in interpreting the data and in creating public awareness that could inform IISs and others in the public health community about the progress being made in immunization data exchange. To further inform public health exchange efforts, we also seek comment on whether adolescents/infants should be further stratified by age, and by what age limits. For providers who operate in multiple states, and thus would be sending data for the same administration to multiple IISs, we seek comment on whether a successful submission should be counted if a provider is able to successfully submit to at least one registry versus all the registries to which the provider submitted.

The data collected for this proposed measure would enable ONC to calculate the percent of immunizations administered where the information was electronically submitted to an IIS.

We believe this measure would inform public health information exchange efforts about how frequently and effectively health care providers are using their certified health IT to send

immunization data to an IIS. In addition, we believe that more detailed measurements of health care providers' engagement in public health exchange would provide critical data in response to a pandemic or other public health emergencies. We welcome feedback on the proposed "Immunization Administrations Electronically Submitted to an Immunization Information System through Certified Health IT" measure.

Immunization History and Forecasts Measure

We propose to adopt a public health information exchange measure to require reporting on the number and percentage of IIS queries made per individual with an encounter.[356] The "Immunization History and Forecasts" measure would capture the use of certified health IT to query information from an IIS under the "transmission to immunization registries" certification criterion (§ 170.315(f)(1)). Therefore, developers of certified health IT with Health IT Modules certified to § 170.315(f)(1) would be required to report for this proposed measure. We believe understanding whether health care providers are engaging in electronically querying immunization information from IIS is critical to public health preparedness.

For the numerator, we propose developers of certified health IT with Health IT Modules certified to § 170.315(f)(1) report the number of query responses received successfully from an IIS overall and by subgroup, by IIS and age group (adults (18 years and over) and children/infants (17 years and younger)) during the reporting period. The definition of a successful response from an IIS should be the total number of messages submitted minus acknowledgments with errors (2.5.1, severity level of E). However, since HL7 Z42 messages contain both immunization history and forecast, whereas Z32 messages exclusively contain history, we seek comment on whether both message types should be included in the measure numerator.

[356] For purposes of this measure, the definition of an encounter would be based on NCQA and SNOMED encounter codes. For outpatient codes, developers should use NCQA's Outpatient Value Set. For inpatient codes, developers should use SNOMED codes 4525004, 183452005, 32485007, 8715000, and 448951000124107.

The first denominator we propose for this measure would be the total number of immunization queries overall and by subgroup, by IIS and age group (adults (18 years and over) and children/infants (17 years and younger)) during the reporting period. We propose to add this denominator to the measure proposed by the Urban Institute to provide data on the total number of query responses that are and are not successfully received from an IIS. This will give further insights into any potential technical challenges that may be occurring during query exchange. The second denominator we propose for this measure would be the total number of encounters overall and by subgroup during the reporting period. However, since it is unlikely that queries happen for every patient encounter, we seek comment on whether the second denominator should capture to total number of applicable patient encounters during the reporting period regardless of whether a query was sent to an IIS. The numerator and denominator counts would be reported overall (across IIS and age subgroups) during the reporting period and by the number of IIS queries made by IIS and age group (adults (18 years and over) and children/infants (17 years and younger) during the reporting period. We believe reporting by these subgroups would be necessary to interpret the data and create public awareness that could inform IISs and other public health participants about the progress being made in immunization data exchange. We seek comment on whether children/infants should be furthered divided and by what age limits.

The data collected for this proposed measure would enable ONC to calculate the following metrics:

- Percent of immunization forecast queries responses from an IIS electronically received among all queries sent.
- Percent of immunization forecast queries responses from an IIS electronically received among all patient encounters.

We propose developers of certified health IT with Health IT Modules certified to § 170.315(f)(1) would attest that they are unable to report on this measure if they have no users that administered immunizations during the reporting period. There may also be providers who

do not administer immunizations but would want to query an IIS to determine whether their patient has received a vaccination. We seek comments on whether we should include this exclusion or suggestions on how we could better refine it.

We believe the measures under this area will inform public health information exchange efforts related to how frequently health care providers are using their certified health IT to send and query immunization data to an IIS, providing critical data for a response to a pandemic or other public health emergency. We welcome feedback on the proposed Public Health Information Exchange measures.

3. Insights Condition and Maintenance of Certification Requirements

The Cures Act specifies that a health IT developer be required, as a Condition and Maintenance of Certification requirement under the Program, to submit responses to reporting criteria in accordance with the "Electronic Health Record Reporting Program" established under section 3009A of the PHSA, as added by the Cures Act, with respect to all certified technology offered by such developer. We propose to implement the Cures Act "Electronic Health Reporting Program" Condition and Maintenance of Certification requirements as the "Insights Condition and Maintenance of Certification" (Insights Condition) requirements in § 170.407. As a Condition of Certification, we propose that health IT developers of certified health IT would submit responses to comply with the Insights Condition's requirements, described in this section of the preamble in relation to the Insights Condition's measures and associated certification criteria.

As stated earlier in the preamble, the intent of the Insights Condition is to address information gaps in the health IT marketplace, as well as provide insights on how certified health IT is being used, consistent with Program certification criteria and associated conformance to identified technical standards. As required by section 3009A(a)(3)(C) of the PHSA, ONC worked with an independent entity, the Urban Institute, to develop measure concepts for the Insights Condition that would not unduly disadvantage small and startup developers. We propose

modifications to the measures the Urban Institute developed to further ensure measures would not unduly disadvantage small and startup developers. The measures we propose reflect the functions of certified health IT and the ability of users to successfully use those functions, rather than reflect the resources and market share of any single developer. We initially designed and selected the Insights Condition measures to provide ONC and the public with information that would aid our collective understanding of how certified health IT is contributing to interoperability nationally, rather than provide a comparative view of individual (large and small) developers. This means that large and small developers would have equal opportunity to contribute to understanding how well interoperability is progressing based on their products' performance of the functions and certification criteria to which the measures apply. As stated previously in section III.F.1, we anticipate evolving and adding to the measures over time to cover additional dimensions identified in the Cures Act, including usability, security, and other topic areas, which may include additional applicable certification criteria and would likely expand the number of certified Health IT Modules impacted.

Therefore, we propose to implement the Insights Condition requirements in a way that does not unduly disadvantage small and startup health IT developers of certified health IT. We understand that developers of certified health IT would need to invest resources to capture and report on these proposed measures. We generally understand these resources to be relatively consistent across developers, regardless of the developer's organizational size. Given this understanding and with the objective to avoid unduly disadvantaging small and startup health IT developers of certified health IT, we propose to establish minimum reporting qualifications that a developer of certified health IT must meet to report on the measure. Developers of certified health IT who do not meet the minimum reporting qualifications (as specified under each measure), would submit a response to specify that they do not meet the minimum reporting qualifications under the Insights Condition measure. In this way, all developers of certified

health IT would report on all measures, even if some report that they do not meet the minimum reporting qualifications.

The minimum reporting qualifications include whether a health IT developer has any applicable Health IT Modules certified to criteria associated with the measure, and whether the developer has at least 50 hospital users or 500 clinician users across its certified health IT products, which serves as a proxy for its size or maturation status (e.g., whether it is a startup). If a developer of certified health IT does not meet these minimum reporting qualifications, it would be required to submit a response that it does not meet the minimum reporting qualifications on specific measures for a given Health IT Module(s) subject to the Insights Condition requirements. In addition, if a health IT developer does not have at least one product that meets the applicable certification criteria specified in the measure requirements, or a developer of certified health IT that is certified to the criterion or criteria specified in the applicable measure during the reporting period but does not have any users using the functionality, the developer would still be required to submit a response that it does not meet the applicable certification criteria or the number of users required to report on the measure.

In sum, a developer of certified health IT would be expected to report as required by each measure under the following circumstances:

- If the developer has at least 50 hospital users or 500 clinician users across their certified health IT products;
- Applicable criterion/criteria associated with the measure; and
- If the developer has any users of the applicable criterion/criteria associated with the measure.

Otherwise, the health IT developer would report that it does not meet the minimum reporting qualifications.

Additionally, a developer of certified health IT who meets the minimum reporting qualifications, has an applicable criterion or criteria associated with the measure, and has users of that criterion or criteria would be expected to report the following for each measure:

- Measure results;
- Required documentation used to generate the measure; and
- Optional documentation used to generate the measure.

We also propose that health IT developers of certified health IT report measures aggregated at the product level, across product versions. We believe that product level data would provide insights on how performance on the measures vary by market (e.g., inpatient, outpatients, specialty) and by capabilities of products, whereas this type of insight would not be available at the developer level. A product-level focus is also aligned with other Program reporting requirements that allow for product level reporting, such as the Real-World Testing Condition and Maintenance of Certification (85 FR 25765). In considering alternatives, such as proposing to require developers to report measures at the health IT developer level or at the most granular level of product version/CHPL ID, we concluded that proposing to require data to be reported at the health IT developer level is unlikely to reduce burden given that data would still need to be obtained from each applicable product and then aggregated. We also concluded that proposing to require reporting at the product version/CHPL ID level could significantly increase burden because health IT developers of certified health IT would need separate reports for each version of their products.

As stated above, we propose to require all health IT developers of certified health IT to comply with the initial Insights Condition's requirements. Developers who do not meet the minimum reporting qualifications specified under each measure must still comply with the Insights Condition's requirements by submitting a response that they do not meet the minimum reporting qualifications. The certification criteria to which the initial Insights Condition requirements apply include the following (as listed in Table 2):

- Clinical information reconciliation and incorporation found in § 170.315(b)(2)
- Electronic health information export found in § 170.315(b)(10)
- View, download, and transmit to 3rd party, found in § 170.315(e)(1)
- Transmission to immunization registries, found in § 170.315(f)(1)
- Standardized API for patient and population services, found in § 170.315(g)(10)

Health IT developers of certified health IT that have less than 50 hospitals users or 500 clinician users across their certified health IT products would be required to submit a response that they do not meet the minimum reporting qualifications for each applicable measure. We believe this approach would allow us to collect nationally representative data, while allowing small and startup health IT developers of certified health IT to participate within their means. We seek comment on the effectiveness of this approach in ensuring that small and startup developers are not unduly disadvantaged.

Table 2. List of Proposed Measures Associated with the Insights Condition and Applicable Certification Criteria

Area	Measure	Related Criterion/Criteria
Individual Access to EHI	Individuals' Access to Electronic Health Information Supported by Certified API Technology	§§ 170.315(e)(1); 170.315(g)(10)
Clinical Care Information Exchange	C-CDA Documents Obtained Using Certified Health IT by Exchange Mechanism	§ 170.315(b)(2)
Clinical Care Information Exchange	C-CDA Medications, Allergies, and Problems Reconciliation and Incorporation Using Certified Health IT	§ 170.315(b)(2)
Standards Adoption & Conformance	Applications Supported Through Certified Health IT	§ 170.315(g)(10)
Standards Adoption & Conformance	Use of FHIR in Apps Supported by Certified API Technology	§ 170.315(g)(10)
Standards Adoption & Conformance	Use of FHIR Bulk Data Access through Certified Health IT	§ 170.315(g)(10)
Standards Adoption & Conformance	Electronic Health Information Export through Certified Health IT	§ 170.315(b)(10)

Public Health Information Exchange	Immunization Administrations Electronically Submitted to an Immunization Information System through Certified Health IT	§ 170.315(f)(1)
Public Health Information Exchange	Immunization History and Forecasts	§ 170.315(f)(1)

Associated Thresholds for Health IT Developers

As stated above, we propose the Insights Condition threshold for small and startup developers would only apply if a developer of certified health IT has no more than 50 non-federal acute care hospitals that participated (reported measure data and use of certified EHR technology) in the Medicare Promoting Interoperability Program and no more than 500 clinician users who participated in MIPS across all of the developer of certified health IT's products. The specific proposed threshold of no more than 50 hospital users or 500 clinician users across their products is based upon the goals of maximizing the number of certified health IT users represented through the program while not unduly disadvantaging small and startup health IT developers. The specific threshold of users is based upon the number of hospital users that participate in the Medicare Promoting Interoperability Program across a developer's products and the number of clinicians who participated in MIPS. The advantage of this approach is that the focus on clinicians and hospitals that participate in the Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program aligns with past policy efforts to increase adoption and use of certified EHR technology (CEHRT). Additionally, Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program data represent a consistent data source that can be used to set thresholds, though this approach may need to evolve over time as the market evolves. While most hospitals participate in the Medicare Promoting Interoperability Program, many clinicians

do not participate in the Promoting Interoperability performance category of MIPS.[357] In addition, other types of settings which may use certified health IT are not included in either of these programs. However, this approach does represent the best available data source for us to set thresholds with some degree of confidence. We note that although the proposed thresholds were developed based on analysis of the Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program data, we intend to implement these threshold requirements based on a developer's overall number of users and not just those users who participate in the Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program, as some developers may have few or no users who participate in these programs. We explored several alternatives to determining the number of hospital and clinician users of a developer's products based upon Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program data but were limited by the availability of other data sources. Other options we considered included expanding from Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program participants to all types of users, including skilled nursing facilities, behavioral health providers and other settings; however, each of these would require a tailored threshold as the markets differ across settings and we do not have recent, ongoing data sources to capture users across these settings to develop thresholds. Financial measures such as gross revenue of the developer was another alternative we considered; however, accessing these data would be difficult.

We have proposed thresholds based upon the goal of maximizing the number of end users on whose usage of certified health IT we receive data rather than the number of developers of certified health IT. We seek to receive data on a broad array of end users to ensure the measures are broadly representative; however, we also do not want to disadvantage small or startup health

[357] CDC, National Center for Health Statistics. National Electronic Health Record Survey. 2019 NEHRS public use file national weighed estimates. https://www.cdc.gov/nchs/data/nehrs/2019NEHRS-PUF-weighted-estimates-508.pdf.

IT developers of certified health IT. Thus, we developed criteria designed to balance these goals. We propose thresholds so that we cover approximately 99% of the inpatient and outpatient certified health IT market share, consisting of hospital users and clinician users as measured by Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program participation data (see analysis below). Setting this high bar would allow us to ensure that ONC and the public receive insights from a large share of certified health IT end users We used data from 2019 for the Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program to develop the proposed thresholds for number of hospital and clinician users. The data included 4,209 non-federal care acute hospitals and 691,381 clinicians who participated in the CMS program. After limiting hospitals and clinicians to those using existing 2015 Edition certification criteria, the 2015 Edition Cures Update criteria, or a combination of the two; and to those products of developers who had certified to at least one of the criteria associated with the measures proposed as described above (see Table 2), we ended up with 3,863 hospitals and 689,801 clinicians. Interested parties should note, given that § 170.315(g)(8) will be transitioned to § 170.315(g)(10),[358] for the purposes of determining the threshold and related calculations, we assume developers who have certified to § 170.315(g)(8) will also certify to § 170.315(g)(10). We then examined the various alternatives for setting user thresholds by determining the percentages of users of certified health IT with developers that would be represented or not in the Program (see Table 3 below). The thresholds we decided to propose maximize coverage and still permit small or start up developers to not be required to report on the specific measures.

Based upon a threshold of 50 hospitals, we would be able to include approximately 99% of all hospital users and the top 18 developers (based upon market share) while excluding the bottom 33 developers (based upon market share). This 99% value is based upon the percentage of users who are not exclusively using products from small developers based upon the threshold.

[358] https://www.federalregister.gov/d/2020-07419/p-724.

Therefore, in the case of a 50-hospital threshold, only 1.4% of hospital users are exclusively using products from small developers, and thus about 99% of the inpatient market would be covered.

Table 3. Thresholds options at the developer level

	Est. Number of Users Only Using Small Developers	Est. % of Users Only Using Small Developers	Est. Number of Small Developers	Est. Number of Remaining Developers
Hospitals				
Option (a) 100 Threshold	142	3.7%	39	12
Option (b) 50 Threshold	56	1.4%	33	18
Clinicians				
Option (a) 2,000 Threshold	21,075	3.1%	176	31
Option (b) 1,000 Threshold	11,251	1.6%	160	47
Option (b) 500 Threshold	7,828	1.1%	146	61

Data Source: ONC analysis of 2019 CMS Promoting Interoperability Program Data & CHPL

If we implement the Insights Condition, including the proposed thresholds, as proposed, and if we subsequently determine that the market differs from 2019 (the year upon which these proposed thresholds are based) and the goal of covering approximately 99% of the inpatient and outpatient market share cannot be met with the proposed thresholds, we will intend to revisit the proposed thresholds to ensure coverage goals are being met. We request comment on this approach for setting thresholds.

4. Insights Condition and Maintenance of Certification's Process for Reporting

We propose in § 170.407(b)(1) that, as a Maintenance of Certification requirement for the Insights Condition, health IT developers of certified health IT must submit responses every six months (i.e., two times per year). We believe overall that semiannual reporting would provide more actionable and valuable data, including enabling us to recognize trends and provide more

timely information to the health IT marketplace on the use of certified health IT. We also believe that this would provide an appropriate and balanced reporting period to review developer of certified health IT responses to the criteria, as well as base any enforcement actions as necessary under the Program. Therefore, we propose in § 170.407(b)(1) to require response submissions to be due semiannually, that is, twice a year, for any applicable certified Health IT Module(s) that have or have had an active certification at any time under the Program during the prior six months. We intend to align reporting requirements for the Insights Condition with our Program's "Attestations" Condition and Maintenance of Certification requirement (85 FR 25781) to reduce reporting burden for health IT developers of certified health IT.

The HITAC recommended that ONC begin and end the reporting periods mid-year, ensuring that certain public health data (e.g., influenza immunizations) coincide with the reporting period.[359] Our proposal aligns with the HITAC's recommendation while also reducing burden for health IT developers of certified health IT by proposing to align with the calendar year identical to other Program requirements (i.e., Attestations),[360] as well as aiming for overall alignment among other programs with reporting requirements (i.e., Promoting Interoperability performance category of MIPS and the Medicare Promoting Interoperability Program).

To further minimize burden, we propose to provide developers of certified health IT with ample time to collect, assemble, and submit their data. We propose that developers of certified health IT would be able to provide their submissions within a designated 30-day window, twice a year. Under this proposal, health IT developers of certified health IT would begin collecting their data twelve months prior to the first 30-day submission window. The first six months of this period would be the period that health IT developers of certified health IT would report on for the first 30-day submission window. Health IT developers of certified health IT would then have the next six months to assemble this data for reporting. During the second six months of this

---

[359] https://www.healthit.gov/sites/default/files/page/2021-10/2021-09-09_EHRRP_TF_2021__HITAC%20Recommendations_Report_signed_508.pdf.
[360] https://www.federalregister.gov/d/2020-07419/p-1580.

period, health IT developers of certified health IT would begin collecting data for the next 30-day submission window and so on.

For example, if we establish the first 30-day submission window as April 1, 2025, we would expect developers of certified health IT to begin gathering data for the first six-month submission beginning April 1, 2024 (this reporting period would cover April 2024 through October 2024) and spend from October 2024 to April 2025 assembling their data for submission. Meanwhile, we would expect, under this example, developers of certified health IT would also be collecting data for the October 2025 submission during this same period, from October 2024 to April 2025. This would allow six months to collect data, and an additional six months to assemble and assess that initial data while simultaneously collecting data for the following reporting period. With this approach, we understand that data is less timely due to a six-month delay, however we believe it is important to give health IT developers of certified health IT reasonable time to assemble and report their data. Semiannual reporting will also help mitigate the six-month delay of data and may also reduce data storage burden for health IT developers of certified health IT.

As stated above, we propose in § 170.407(b)(1) to require a developer of certified health IT with any applicable Health IT Module(s) that have or have had an active certification at any time under the Program during the prior six months to provide responses to the Insights Condition of Certification specified in paragraph (a) of this section semiannually (i.e., every six months). We propose in § 170.407(b)(1)(i) that a developer of certified health IT must provide responses beginning April 2025 for the following measures: (1) Individuals' access to electronic health information; (2) Applications supported through certified health IT; (3) Immunization administrations electronically submitted to an immunization information system through certified health IT; and (4) Immunization history and forecasts. We propose in § 170.407(b)(1)(ii) that a developer of certified health IT must provide responses beginning April 2026 for the remaining measures: (1) C-CDA documents obtained using certified health IT by

exchange mechanism; (2) C-CDA medications, allergies, and problems reconciliation and incorporation using certified health IT; (3) Use of FHIR in apps supported by certified API technology; (4) Use of FHIR bulk data access through certified health IT; and (5) Electronic health information export through certified health IT.

We believe that initiating developer submission of responses for certain measures (as identified above) in April 2025 would allow us to both calculate and prioritize data relevant to ONC policy priorities and broader public interests. Monitoring patients' access to their electronic health information was identified as priority of the Cures Act, and ONC has taken major initiatives to enable that access, including improving patient access to their EHI through standard-based APIs. It is critical to assess the availability and ability for applications to integrate with EHRs in order to make that data accessible to individuals. The COVID-19 pandemic has enhanced the need for electronic exchange between health care providers and public health agencies. Therefore, we are also prioritizing the proposed measures related to immunization exchange. We believe the submission of responses for the remaining specified measures in April 2026 provides adequate time for developers of certified health IT to make necessary changes to their systems to collect data as described above – effectively giving developers from the time this rule is finalized to April 2025 to modify their systems to begin collecting data for submission in April 2026.

We welcome comments on our proposed approach, as well as the proposed frequency of reporting, other frequencies of reporting such as more or less frequent, and any additional burdens that should be considered for health IT developers of certified health IT to meet the proposed Insights Condition and Maintenance of Certification requirements.

We also note that there may be other factors that could impact a developer of certified health IT's ability to easily collect data to comply with the Insights Condition's requirements. For example, a developer of certified health IT may have contracts or business agreements that inhibit the health IT developer's ability to collect data from its customers. We note that in such

scenarios, developers of certified health IT would need to renegotiate their contracts if we finalize our proposals. We expect developers of certified health IT would work to mitigate any issues and provisions affecting their ability to comply with this Condition and Maintenance of Certification requirement. Therefore, a developer of certified health IT that is required to meet the Insights Condition's requirements must submit responses or may be subject to ONC direct review of the Conditions and Maintenance of Certification requirements, corrective action, and enforcement procedures under the Program. We believe this is consistent with the enforcement for any noncompliance with the Conditions and Maintenance of Certification requirements and note that our goal is to work with health IT developers of certified health IT to remedy any noncompliance in a timely manner. We welcome comments on our approach, as well as any specific hardships health IT developers of certified health IT may encounter with the Insights Condition of Certification.

We propose that responses to the Insights Condition would occur via web-based form and method, consistent with the requirements in § 3009A(c) of the PHSA. We note that under the statute, developers of certified health IT must report to an "independent entit[y]" to "collect the information required to be reported in accordance with the criteria established." We intend to award a grant, contract, or other agreement to an independent entity as part of the implementation of the Insights Condition and will provide additional details through subsequent information. We intend to make responses publicly available via an ONC website, and we intend to provide developers of certified health IT the opportunity to submit qualitative notes that would enable them to explain findings and provide additional context and feedback regarding their submissions.

Further, we propose a new Principle of Proper Conduct for ONC-Authorized Certification Bodies (ONC-ACBs) in § 170.523(u) that would require ONC-ACBs to confirm that applicable health IT developers of certified health IT have submitted their responses for the Insights Condition of Certification requirements in accordance with our proposals. We expect

that the ONC-ACBs would confirm whether or not the applicable health IT developers submitted responses for the Insights Condition of Certification requirements within the compliance schedule. The intent of this responsibility is not to duplicate the work of the independent entity in collecting and reviewing the response submissions. Rather, it is instead meant to support the ONC-ACBs' other responsibility in § 170.550(l) to ensure that health IT developers of certified health IT are meeting their responsibilities under the Conditions and Maintenance of Certification requirements before issuing a certification.

We welcome comments on the proposed Insights Condition and Maintenance of Certification requirements.

G. Requests for Information

1. Laboratory Data Interoperability Request for Information

We seek public feedback that may be used to inform a study and report required by Division FF, Title II, Subtitle B, Ch. 2, Section 2213(b) of the Consolidated Appropriations Act, 2023 (P.L. 117-328, Dec. 29, 2022), or future rulemaking regarding the adoption of standards and certification criteria to advance laboratory data interoperability and exchange.

a. Background

ONC has long recognized the importance of enabling the electronic exchange of laboratory data and has addressed laboratory interoperability through a variety of activities. These include adoption of multiple certification criteria and standards related to laboratory data and interoperability as part of the Program. For example, the current certification criterion "Transmission to public health agencies - reportable laboratory tests and values/results" in § 170.315(f)(3) relates to Electronic Lab Reporting (ELR) to public health agencies and references the "Electronic transmission of lab results to public health agencies" standard in § 170.205(g). Other current Program criteria and standards associated with laboratory data interoperability include:

- "Computerized provider order entry – laboratory," certification criterion (§ 170.315(a)(2));
- "View, download, and transmit to 3rd party," certification criterion (includes laboratory test report(s) in § 170.315(e)(1)(i)(A)(*6*));
- "Transmission to public health agencies – reportable laboratory tests and values/results," certification criterion (§ 170.315(f)(3));
- Laboratory tests, vocabulary standard (§ 170.207(c));
- Electronic transmission of lab results to public health agencies, content standard (§ 170.205(g));

In the proposed rule titled "2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications" (80 FR 16804), ONC proposed to adopt certification criteria specific to laboratory ordering that included HL7 version 2.5.1 Laboratory Order Interface (LOI) Release 2, Electronic Directory of Services (eDOS), and Laboratory Results Interface (LRI) Release 2 Implementation Guides (IGs). However, with consideration of public comments on the proposal, ONC did not adopt these IGs in the 2015 Edition Final Rule based on a number of factors that included insufficient readiness of the best versions of the IGs for the associated certification criterion (80 FR 62617 and 62685).

The COVID-19 pandemic has highlighted gaps in laboratory data exchange, particularly in reporting test results. Advancing standards-based exchange of data from the health IT used by ordering clinicians to laboratories' in vitro diagnostics systems and laboratory information systems, and from laboratories' systems to public health agencies and the EHR systems and other health IT used by health care providers or patients would be beneficial to laboratories, other types of health care providers, patients, and public health authorities. Over the past decade, new standards for health data exchange have emerged and gained acceptance, such as HL7® Fast Healthcare Interoperability Resources (FHIR®), and existing IGs for transmission of laboratory

data using HL7 v2.5.1 have gained maturity and could be leveraged to improve laboratory interoperability.

Section 2213(b) of the Consolidated Appropriations Act, 2023 includes a provision directing ONC to conduct a study (and issue a report to Congress) on the use of standards for electronic ordering and reporting of laboratory test results.[361] The provision specifies that in conducting the study, ONC shall determine the extent to which clinical laboratories are using standards for electronic ordering and reporting of lab test results, assess trends in laboratory compliance with such standards and their effect on the interoperability of laboratory data with public health data systems, identify challenges related to collecting and reporting demographic and other data with respect to laboratory test results, identify challenges using or complying with standards and reporting laboratory test results with data elements identified in standards, and review other relevant areas determined appropriate by ONC.[362]

b. Request for Information

We seek public comment generally on any topics identified above for the Consolidated Appropriations Act, 2023, Section 2213(b) study on the use of standards for electronic ordering and reporting of laboratory test results, such as the use of health IT standards by clinical laboratories, use of such standards by labs and their effect on the interoperability of laboratory data with public health systems, including any challenges of the types identified above. We also seek comment on whether ONC should adopt additional standards and laboratory-related certification criteria as part of the ONC Health IT Certification Program. ONC specifically seeks comments from the public on the following:

1. Which implementation guides or other standards should ONC adopt in certification criteria for health IT supporting transmittal and receipt of laboratory orders, laboratory results and directory of services?

[361] H.R.2617 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2023, H.R.2617, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/2617.
[362] https://www.congress.gov/bill/117th-congress/house-bill/2617/text.

2. The utility and maturity of existing HL7 v2 and C-CDA standards supporting laboratory interoperability and the impact of moving to FHIR-based laboratory data exchange.
3. What barriers would additional health IT certification criteria for laboratory interoperability create for developers and other interested parties, and how might this affect adoption and use of such technology?
4. Would developers of laboratory information systems or in vitro diagnostics systems that have not traditionally submitted products for certification under the Program seek out and benefit from certification to criteria relevant to such developers' products?
5. Are there any other steps that ONC and HHS should consider taking to advance laboratory interoperability?

2. Request for Information on Pharmacy Interoperability Functionality within the ONC Health IT Certification Program including Real-Time Prescription Benefit Capabilities

a. Background

Section 119 of Title I, Division CC of the Consolidated Appropriations Act, 2021, (Pub. L. 116-260) (CAA), requires PDP sponsors of prescription drug plans to implement one or more real-time benefit tools (RTBTs) after the Secretary has adopted a standard for RTBTs and at a time determined appropriate by the Secretary. The law specified that a qualifying RTBT must meet technical standards named by the Secretary, in consultation with ONC. Section 119(b)(3) also amended the definition of a "qualified electronic health record" in section 3000(13) of the PHSA to specify that a qualified electronic health record must include or be capable of including an RTBT. In the 2014 Edition Final Rule, ONC established the term "Base EHR," based on the "Qualified EHR" definition, for use within the ONC Health IT Certification Program (Program) (77 FR 54262).

We intend to propose in future rulemaking the establishment of a real-time prescription benefit health IT certification criterion within the Program and include this criterion in the base EHR definition in § 170.102. We intend to propose a criterion that would certify health IT to enable a provider to view within the electronic prescribing workflow at the point of care patient-specific benefit, estimated cost information, and viable alternatives. We are also considering a proposal to adopt and reference the National Council for Prescription Drug Programs (NCPDP) Real-Time Prescription Benefit (RTPB) standard version 12 as part of the potential certification criterion.[363] This standard would enable the exchange of patient eligibility, product coverage, and benefit financials for a chosen product and pharmacy, and identify coverage restrictions and alternatives when they exist.

While we believe that implementing RTBT functionality required for inclusion in the Program under the CAA would be an important step towards improving prescribing experiences for providers and patients, we recognize that it is only one of a series of capabilities that are part of a comprehensive workflow for evaluating and prescribing medications. Other key processes working in concert with real-time prescription benefit capabilities may include:

- Drug Interaction Checks.
- Medication History.
- Formulary and Benefit Management.
- Eligibility Checks.
- Electronic Prior Authorization.
- Electronic Prescribing.

For example, if a prescriber initiates the real-time prescription benefit process when the prescriber launches an electronic prescribing application and chooses a clinically appropriate medication, the prescriber may have the ability to discuss prescription costs and other options

[363] For further information about implementing the NCPDP RTPB standard version 12, see resources at https://standards.ncpdp.org/Access-to-Standards.aspx.

with a patient at the point of care, and during this same process, receive notification that a prior authorization is needed for the prescription. Within the same workflow, prescribers could initiate electronic prior authorization processes, answer any questions, and complete any other requirements before transmitting the electronic prescription to the patient's preferred pharmacy. When the patient arrives at the pharmacy, the medication could be filled and dispensed immediately, and the patient would already be aware of price and copay responsibility information. This scenario is only one of many possibilities.

Today, the Program addresses these additional capabilities in a limited manner. For instance, in the ONC Cures Act Final Rule, ONC adopted NCPDP SCRIPT standard version 2017071 and updated the "electronic prescribing" certification criterion in § 170.315(b)(3)(ii) to reflect this standard, including specifying electronic prior authorization transactions supported by the standard as optional transactions, which health IT developers can elect to have explicitly tested, or not, as part of certification of a product to § 170.315(b)(3) (85 FR 25680).

A "drug-formulary and preferred drug list checks" certification criterion had been established for the 2015 Edition in § 170.315(a)(10) but was later removed from the Program by the ONC Cures Act Final Rule (85 FR 25660). ONC removed the criterion due to the lack of associated interoperability standards and to reduce certification burden on developers as this functionality had been widely adopted across industry.

We request comment from the public about specific issues related to establishing a certification criterion using NCPDP RTPB standard version 12 and other potential actions that could support complementary and interoperable workflows. Given the statutory definition in PHSA § 3000(13) of "qualified electronic health record" as an electronic record of health-related information on an individual that includes, or is capable of including, RTBT functionality, we seek to understand whether ONC should offer or require certification of other capabilities to optimize the value of real-time prescription benefit capabilities to clinicians and patients.

First, we present in section III.G.2.c (below) a series of scenarios and specific questions regarding the real-time prescription benefit criterion we intend to establish through future rulemaking. Areas for input include: the specific transactions that should be included in the criterion; amendments to conformance requirements related to the NCPDP RTPB standard version 12 that we believe may help to improve interoperability; and whether to propose a certification criterion, or propose revisions to an existing criterion, that would require for certification certain segments and vocabularies that are optional or situational within the NCPDP RTPB standard.

We then turn in section III.G.2.d (below) to the broader electronic prescribing ecosystem for pharmacy interoperability. Specific areas for input include: whether ONC should adopt additional standards and certification criteria that support real world electronic prescribing workflows; whether ONC should explore developing certification criteria bundles that mimic real world workflows; and how ONC should approach structuring certification criteria for Health IT Modules that must interact as part of these workflows.

Reviewers who may be interested in commenting on this RFI are encouraged while reviewing it to consider identified data, standards and specifications, and technical capabilities from an ecosystem perspective. Commenters are also encouraged to consider interoperability between certified Health IT Modules and other relevant systems, including third-party applications, electronic prescribing networks and intermediaries, drug knowledge databases and content provider systems, pharmacy information systems, prescription benefit manager systems, and payer systems. Further, we are interested in commenters' views on how developers of certified health IT may be able to support drug price transparency, patient choice, and meet other market demands while ensuring reliable and trusted performance.

c. Real-Time Prescription Benefit Certification Criterion

i. Potential transactions and capabilities to test

ONC is currently considering certification testing scenarios that would assess the capacity of the Health IT Module under test to: capture data specified in the NCPDP RTPB standard version 12; format a RTPB Request transaction; and deliver a RTPB Request transaction to a processor, prescription benefit manager, or adjudicator either directly or via an intermediary or switch. As part of these potential testing scenarios, Health IT Modules would also need to demonstrate the capacity to: receive a RTPB Response transaction; display RTPB Response information for the health care provider to review within their electronic prescribing workflow; and (potentially) to display RTPB Response information for a patient.

Specifically, we are considering a set of scenarios in which the Health IT Module under test would need to demonstrate capacity:

- That allows end users to choose a specific patient, product, and pharmacy, then successfully transmit a request for patient and product specific benefit information directly to a Pharmacy Benefit Manager (PBM), or optionally to a PBM through an intermediary;
- To receive a response correctly displaying price and coverage details of the submitted and covered products, including alternative pharmacies or medications;
- To receive a response correctly displaying that a component of the request (e.g., quantity) is not covered;
- To receive a response correctly displaying a message indicating "Patient not found" or "Patient not eligible;"
- To receive a response correctly displaying the identified product is considered a benefit exclusion;
- To receive a response correctly displaying the identified product is not on the patient's formulary;
- To receive a response correctly displaying Step Therapy is required;

- To receive a response correctly displaying a Drug Utilization Evaluation (DUE) Alert;
- To receive a response correctly displaying Out-of-Network pharmacy;
- To receive a response correctly displaying Out-of-Network provider;
- To receive a response correctly displaying the submitted provider is not an allowed provider;
- To receive a response correctly displaying Prior Authorization is required;
- To receive a response correctly displaying not an allowed pharmacy (a pharmacy, mail order pharmacy, specialty pharmacy, or other restricted pharmacy where the product may not be covered); and
- To receive status and error messages such as "Transmission accepted and transaction processed," "Transmission accepted and transaction not processed," and "Transmission rejected, and transaction not processed" for different scenarios.

ONC requests comment on whether inclusion of these testing scenarios under a real-time prescription benefit certification criterion would effectively test a certified Health IT Module's capacity to successfully send and receive RTPB transactions in accordance with the NCPDP RTPB standard version 12, specifically:

- Is the set of testing scenarios described above appropriate for a real-time prescription benefit certification criterion?
- Should ONC consider other testing scenarios as part of a real-time prescription benefit certification criterion?
- Are there other testing considerations ONC should take into account in structuring a real-time prescription benefit certification criterion?

ONC is also considering ways to support the standardized capture and exchange of negotiated price, as required in Section 119 of the CAA. Section 119(a)(2) of the CAA specifies "[c]ost-sharing information and the negotiated price for such drug and such alternatives at

multiple pharmacy options, including the individual's preferred pharmacy and, as applicable, other retail pharmacies and a mail order pharmacy," as information that technology meeting the definition of "qualified electronic health record" in PHSA § 3000(13)(C), as added by section 119(b)(3) of the CAA, must be capable of incorporating. In the 2019 "Modernizing Part D and Medicare Advantage to Lower Drug Prices and Reduce Out-of-Pocket Expenses" proposed rule, CMS encouraged, but did not propose to require, plans to use RTBTs to promote full drug cost transparency by showing each drug's negotiated price in addition to the beneficiary's out-of-pocket cost (83 FR 62166). CMS has also encouraged plans to provide additional cost data comparing the beneficiary and plan cost comparisons for each drug and its alternatives.

The NCPDP RTPB standard version 12 does not include fields to support the exchange of negotiated price. We understand that this information was not included because of concerns regarding the confidentiality of drug pricing agreements as well as the inherent challenges in determining the negotiated price in real time — for example, rebates calculated later, the definition of negotiated price under revision, and exclusion of Usual and Customary price information. We seek comment on the value of negotiated price to patients and prescribers to aid in their discussions and decision-making during prescribing. Patient cost-sharing responsibilities are often driven by their plan design, deductible, copay requirements, and other related factors, thus it is unclear whether including such information will improve the utility or usability of technology certified to a real-time prescription benefit certification criterion.

ii. Requirements for Use of XML or EDI Format

The NCPDP RTPB standard version 12 supports the exchange of RTPB transactions in both extensible markup language (XML) and electronic data interchange (EDI) formats. We understand that the pharmacy industry is currently moving away from EDI for reasons that include its lack of flexibility and human readability as well as EDI's higher overall development and maintenance costs. XML defines a set of rules for encoding documents in a format that is both human and machine readable and allows developers to create and manage their own XML

files, but this high level of customizability may pose challenges during exchange. The NCPDP RTPB standard version 12 Implementation Guide contains guidance intended to assist alignment across exchange partners. XML also facilitates compliance with the FDA's requirements for prescription drug labeling submissions,[364] improves patient safety and enhances manufacturing efficiencies.

The NCPDP SCRIPT standard version 10.6 adopted in § 170.205(b)(2) and referenced by the electronic prescribing criterion in § 170.315(b)(3)(i) supports both EDI and XML format. However, the ONC Cures Act Final Rule adopted the NCPDP SCRIPT standard version 2017071 in § 170.205(b)(1) and finalized an updated version of the "Electronic prescribing" criterion in § 170.315(b)(3)(ii) to reference this standard, which only supports the use of XML (85 FR 25678). Certification to the § 170.205(b)(2) criterion has not been available since June 30, 2020. The real world testing provisions in § 170.405(b)(5) required developers with health IT certified to § 170.315(b)(3) prior to June 30, 2020, to update the technology to provide customers of that health IT to be compliant with § 170.315(b)(3)(ii) and provide the updated technology to their customers by December 31, 2022. However, a variety of health IT products that support the older NCPDP SCRIPT standard version 10.6 may remain in use — including by entities who do not use certified health IT and do not need to meet Medicare Part D requirements for electronic prescribing transactions.

We are concerned that legacy or other health IT may not be prepared to adopt XML at this time and that there may be challenges exchanging data between systems conformant only with EDI and those conformant only with XML. We are seeking comment on whether the real-time prescription benefit certification criterion under consideration should only require and test XML format or both XML and EDI formats.

iii. Requirements for Use of NDC or RxNorm Codes

[364] https://www.fda.gov/industry/fda-data-standards-advisory-board/structured-product-labeling-resources.

The NCPDP RTPB standard version 12 supports the exchange of RTPB transactions containing both NDC and RxNorm code sets. National Drug Codes (NDC) provide a unique identifier for products such as vaccines or medications. Each product is assigned a unique 10- or 11-digit, 3-segment number that identifies the labeler, product, and trade package size. RxNorm is a drug terminology providing a set of normalized medication names and codes based on a collection of commonly used public and commercial vocabularies of drug names and their ingredients. The National Library of Medicine provides an RxNorm unique identifier of drug substance and dose form to identify all the products that contain the same substance. Each of these coding systems serves an important role in supporting medication matching, medication reconciliation, formulary checks, drug allergy checks, clinical decision support, and other clinical and operational applications. However, because these coding systems were created by different contributors at different times and for different purposes, their content coverage varies, as does their use in health IT.

The NCPDP RTPB standard version 12 supports the exchange of representative NDCs in transactions originating from prescribing providers, which may be any NDC belonging to the same product concept that is nationally available, not repackaged, not obsolete, not private label, and not unit dose (unless it is the only NDC available). A product concept describes a medication or non-medication product that has the same active ingredient, strength, route, dosage form, drug delivery system or packaging, or therapeutic use/indication. Product concepts also have brand and generic distinctions. The Centers for Disease Control (CDC) has also developed NDC and CVX crosswalk resources to facilitate the use of NDCs for vaccines.[365]

RxNorm (currently adopted in § 170.207(d)(3) and proposed in § 170.207(d)(1), see section III.C.3 of this preamble) is required in the electronic prescribing certification criterion in § 170.315(b)(3)(ii)(A) and (B) as a minimum standard code set for a drug. Where no RxNorm code exists, nothing prohibits another allowable code from being used; however, where

[365] https://www2a.cdc.gov/vaccines/iis/iisstandards/ndc_crosswalk.asp.

corresponding RxNorm codes exist, certified health IT must be able to use those codes. Under the NCPDP RTPB standard version 12, NDC is required and RxNorm is situational, where RxNorm is required only when populated in the RTPB Product Segment. The Product Segment is mandatory for an RTPB request. We are concerned that "situational" may be viewed as optional by health IT developers seeking certification, leading to a lack of coded values. Missing codes may limit the utility of this data for clinical decision support and pharmacy interoperability and have negative downstream effects on claims and billing.

ONC has received comments and feedback from the HITAC and other industry participants stressing the need to reconcile the use of NDC and RxNorm codes, and to support accurate NDC-RxNorm mapping.[366] The Interoperability Standards Priorities Task Force 2021 Recommendations Report included a recommendation that "ONC work with FDA, NLM and CMS to continue to harmonize NDC to RxNorm, treating RxNorm as the source terminology set, and to harmonize administrative and electronic prescribing standards to use RxNorm as the single source of clinical data for clinical care, research and administrative workflows, replacing NDC for such purposes."[367]

We believe that requiring RxNorm in addition to NDC for a real-time prescription benefit criterion could facilitate the adoption, maintenance, and harmonization between NDC and RxNorm. However, we understand that adoption alone will not support concept and code mapping between NDC and RxNorm. We are requesting comment on whether a potential real-time prescription benefit certification criterion should require demonstration of compliance with both NDC and RxNorm, specifically:

- Would requiring demonstration of compliance with both NDC and RxNorm in a real-time prescription benefit criterion support improved adoption, maintenance, and harmonization between code sets?

---

[366] *See* https://www.healthit.gov/sites/default/files/facas/2019-09-17_ISP_TF_Draft_Final_Report_508.pdf.
[367] *See* https://www.healthit.gov/hitac/committees/interoperability-standards-priorities-task-force-2021.

- How would requiring Health IT Modules to demonstrate compliance to both code sets for certification to a real-time prescription benefit criterion affect implementation of this capability? What benefits would this have for health care providers and other participants that support real-time prescription benefit transactions?
- What burden would demonstration of compliance with both code sets impose on developers of seeking or maintaining certification of Health IT Modules to this criterion?
- Would either NDC or RxNorm alone provide sufficient information for applications to provide reliable, accurate clinical decision support, such as dosing guidance, drug-drug interaction or drug allergy checks?
- What would be the consequences (positive or negative, intended or unintended) of establishing "RxNorm as the single source of clinical data for clinical care, research and administrative workflows, replacing NDC for such purposes," as recommended by the HITAC?[368]

iv. ICD-10-CM and SNOMED-CT in the Clinical Segment

The Clinical Segment in the NCPDP RTPB standard version 12 is used to specify diagnosis information associated with the prescription. Under this version of the standard, the segment is situational, meaning if it is used, it should be included in a RTPB Request transaction. It is required when needed for coverage determinations and assists with claims submissions and processing. However, if the Clinical Segment is not sent, diagnosis codes may not be transmitted to PBMs, which provide oversight for (and are sometimes delegated the responsibility of) coverage determinations and redeterminations. Given the importance of this information, ONC is strongly considering specifying mandatory use of the Clinical Segment (rather than situational

[368] *See* https://www.healthit.gov/sites/default/files/page/2021-07/2021-06-09_ISP_TF_2021_HITAC%20Recommendations_Report_Signed_508.pdf.

use) in RTPB Request transactions as part of a future proposal for a real-time prescribing benefit certification criterion.

The Clinical Segment specified in the NCPDP RTPB standard version 12 supports a DiagnosisCodeQualifierCode element that qualifies the external code list used for medication-associated diagnosis, supporting both the International Statistical Classification of Diseases and Related Health Problems (ICD) and SNOMED CT. SNOMED CT is a clinical healthcare terminology and infrastructure that provides a common language that enables a consistent way of capturing, sharing and aggregating health data across specialties and sites of care. SNOMED CT can serve as a common language between ICD-10-CM and ICD-11 and may help developers and providers during the transition between ICD versions should ICD-11 be adopted.

ONC seeks comments that may help inform our consideration of whether to require the Clinical Segment in the NCPDP RTPB standard version 12 as part of any future real-time prescription benefit certification criterion, and whether to require that Health IT Modules under pre-certification testing, real world testing after certification, and (as applicable) ONC-ACBs' in-the-field surveillance for such criterion demonstrate use of both ICD-10-CM and SNOMED CT within the Clinical Segment. Such requirements could specify that the technology must be able to transmit diagnosis codes for the patient in the RTPB Clinical Segment and be consistent with ICD-10-CM and SNOMED CT. Further, the RTPB Clinical Segment must be able to support up to two diagnosis codes to be fully conformant with the NCPDP RTPB Standard Implementation Guide, Version 12. Specifically, we are requesting comment on the following:

- Would a requirement to demonstrate use of both ICD-10-CM and SNOMED CT within the Clinical Segment as part of an RTPB certification criterion support a more seamless transition between ICD-10-CM and ICD-11, in the event ICD-11 is adopted? Are there other benefits to requiring certified Health IT Modules demonstrate compliance with both terminologies?

- What additional burden would demonstration of compliance with both ICD-10-CM and SNOMED CT impose on health IT developers seeking or maintaining certification of Health IT Modules to a real-time prescription benefit criterion?

v. Patient Specific Benefit Information

One of the most challenging areas of real-time prescription benefit functionality is the need to match patient records to their medical and pharmacy benefit records in order to facilitate the exchange of patient specific benefit information between pharmacies, EHRs, and PBMs/adjudicators. We are currently considering requiring real-time prescription benefit implementation within the electronic prescribing workflow and requiring health IT certified for electronic prescribing capabilities be capable of ingestion and integration of this information. In addition, we expect health care providers will typically send a NewRx soon after receiving an RTPB Response transaction. In order to better support these transactions and support improved patient matching we are considering a more comprehensive Patient Segment than that which is required in the NCPDP RTPB standard version 12.

After reviewing and comparing Patient Segments across NCPDP SCRIPT standard version 2022011, NCPDP RTPB standard version 12, and the NCPDP Formulary and Benefit standard version 54, we are considering requiring support for the patient identity segment as outlined in NCPDP SCRIPT standard version 2022011 as part of a real-time prescription benefit certification criterion. We acknowledge that both NCPDP SCRIPT standard version 2022011 and NCPDP RTPB standard version 12 support the exchange of unique, but not universal, identifiers produced by vendors, but because not all providers have access to these services, and patients lack access to these types of unique identifiers, demographics-based patient matching must also be enabled to support most health care providers and patients across the country.

We are requesting comment on whether a real-time prescription benefit certification criterion should require conformance to the Patient Segment specified in NCPDP SCRIPT standard version 2022011 (replacing the NCPDP RTPB standard version 12 Patient

(Demographic) Segment) to support the identification and linkage of records needed to support the successful exchange of patient-specific benefit information, specifically:

- Would requiring the Patient Segment identified in NCPDP SCRIPT standard version 2022011 as part of a real-time prescription benefit certification criterion support improved patient matching?
- What additional burden would requiring the Patient Segment identified in NCPDP SCRIPT standard version 2022011 as part of a real-time prescription benefit certification criterion impose on health IT developers seeking to certify Health IT Modules to this criterion?
- Should ONC consider requiring alternative or additional demographic data elements or sets of demographic data elements as part of a real-time prescription benefit certification criterion to further improve patient matching? For instance, should ONC consider requiring the Patient Demographics/Information data class identified in USCDI Version 3? What additional benefit would this offer to health IT developers, health care providers, patients, and the healthcare industry in general? What additional burden would these or other alternatives impose on health IT developers?

vi. System and Workflow Integration

As added by Section 119 of the CAA, section 3000(13)(C) of the PHSA specifies that a qualified electronic health record: "includes, or is capable of including, a real-time benefit tool that conveys patient-specific real-time cost and coverage information with respect to prescription drugs that, with respect to any health information technology certified for electronic prescribing, the technology shall be capable of incorporating the information described in clauses (i) through (iii) of paragraph (2)(B) of section 1860D–4(o) of the Social Security Act." We believe that PHSA § 3000(13)(C) as a whole requires that a real-time prescription benefit certification criterion must require a Health IT Module certified to the criterion to demonstrate capabilities both to convey real-time prescription benefit information and ingest and integrate real-time

prescription benefit information for use by other health IT services, components, or combinations thereof that are part of the electronic prescribing workflow. While we expect some health IT developers may plan to develop real-time prescription benefit functionality as part of a suite of electronic prescribing capabilities contained within one health IT product, we also expect that some health IT developers who participate in the ONC Health IT Certification Program may prefer to obtain certification to a criterion that allows them to leverage a third-party real-time prescription benefit tool. Under such a certification approach, we would seek to ensure through requirements and testing for conformance to those requirements that integration between systems is conducted effectively.

Workflow integration refers to the capacity of health IT to launch and perform all functions within the electronic prescribing workflow without the need for the user to sign into a separate web-based platform or otherwise leave the electronic health record system, or prescribing application, user interface to send and receive RTPB transactions. Data integration refers to the capacity of a receiving system to receive, ingest, and reuse all data elements received in accordance with the standards and other requirements as stated in a certification criterion. For instance, for electronic prescribing, data integration is necessary for health IT to conduct drug interaction checks and alerts. In real-time prescription benefit processes, data integration embeds patient-specific benefit, estimated cost information, and viable alternatives into the electronic prescribing workflow at the point of care.

We believe that a real-time prescription benefit certification criterion should address concepts of both workflow and data integration in order to facilitate, where lawful and appropriate, the free flow of and reuse of EHI and other prescription benefits data across the healthcare landscape and reduce burden and high potential for error associated with manual data entry, translation across disparate formats and standards, and other challenges related to limited interoperability. For instance, as part of a certification criterion, we could require systems under test to demonstrate the capacity to integrate and reuse data received through transactions sent by

PBMs or through intermediaries. We are seeking comment on how to address the statutory requirements and policy goals for the criterion with respect to workflow and data integration:

- How can ONC most effectively address the definition of "qualified electronic health record" in PHSA § 3000(13)(C) as added by the CAA to achieve the benefits of workflow and data integration while minimizing potential burden on health IT developers seeking to certify health IT to the real-time prescription benefit tool criterion?
- Should ONC consider alternative paths to certification to a real-time prescription benefit criterion based on whether a Health IT Module relies on a third-party application or other intermediary to successfully demonstrate full integration and capacity to reuse the data that received from other systems involved in real-time prescription benefit information exchange?
- How should ONC address alignment of a real-time prescription benefit criterion to the electronic prescribing criterion in § 170.315(b)(3)?

vii. Real Time Prescription Benefit Certification Scope

Medications are likely to be the primary product type chosen by health care providers when initiating real-time prescription benefit processes at this time. However, the COVID-19 pandemic highlighted the need to ensure vaccine availability in various care settings including pharmacies, as well as needs to collect, aggregate, and report information to immunization registries and submit reimbursement claims for administering vaccines to patients. Requiring health IT certified to a real-time prescription benefit criterion to support RTPB transactions that include vaccines could lead to higher levels of benefit coverage for vaccines obtained from contracted pharmacies, improved eligibility checks, and lower out of pocket costs for routine preventive care that is covered by most plans. In addition, technology certified to a real-time prescription benefit criterion could also support RTPB transactions for medical devices or

supplies and exchange this data using device identifiers supported by the NCPDP Formulary and Benefit standard.

The NCPDP RTPB standard version 12 will continue to mature and evolve over time in response to new or unidentified challenges and as needs emerge. We believe that one area of the standard in need of advancement and alignment is how the standard supports the exchange of unique identifiers for devices. The FDA has discontinued use of legacy FDA identification numbers assigned to devices (21 CFR 801.57) where National Health-Related Item Codes (NHRIC) or NDCs assigned to devices are rescinded, and manufacturers may no longer provide an NHRIC or NDC on the label of their devices or on any device package. The FDA has since released guidance[369] stating that it would not object to the use of NDCs on device labels and device packages for finished devices that are manufactured and labeled prior to September 24, 2023.

We are requesting comments on whether a real-time prescription benefit criterion should also require demonstration of support for products that are not defined as medications but may also be included in a RTPB transaction, namely vaccines and medical devices or supplies, specifically:

- What benefits would come from supporting the exchange of prescription benefit information for vaccines, medical devices, or supplies?
- What challenges would be involved in supporting the exchange of prescription benefit information for vaccines, medical devices, or supplies?
- What additional burden would exchange of information on vaccines, medical devices, or supplies as part of a certification criterion impose on health IT developers?
- To what extent should ONC require as part of certification to a real-time prescription benefit criterion support for devices or supplies as defined within the NCPDP RTPB standard version 12?

[369] https://www.fda.gov/media/95794/download.

- Alternatively, should ONC require conformance to the NCPDP Formulary and Benefit Standard for devices? The NCPDP Formulary and Benefit Standard supports the exchange of UDIs for devices, and adoption of this standard may support other critical RTPB processes. What are effective ways to support accurate device identification within and beyond the real-time prescription benefit workflow, while aligning with FDA regulations and related requirements?
- What additional opportunities might arise from requiring conformance to the NCPDP Formulary and Benefit Standard?

d. Health IT Ecosystem for Pharmacy Interoperability

We seek information on formulary and benefit management and electronic prior authorization capabilities that work in tandem with real-time prescription benefit functionality in the context of electronic prescribing workflows.

i. Formulary and Benefit Management

When used appropriately, formularies can help manage drug costs without negatively impacting patient health. For example, tiered formularies allow providers and patients to choose lower cost medications for the same clinical indication. With more accurate and timely formulary and benefits data, providers can demonstrate better management of care for their high-risk patients, reducing time-to-therapy with less administrative overhead. Providers who have access to a formulary can use this information to determine appropriate medications consistent with a patient's pharmacy benefit prior to submitting a benefit check.

ONC previously finalized a "drug-formulary and preferred drug list checks" certification criterion for the 2015 Edition of health IT certification criterion in § 170.315(a)(10); however, ONC did not adopt the NCPDP Formulary and Benefit standard to support this criterion. In the 2015 Edition Proposed Rule, ONC proposed to require a Health IT Module to receive and incorporate a formulary and benefit file using the NCPDP Formulary and Benefit standard

version 3.0[370] (80 FR 16821). However, in the 2015 Edition Final Rule, ONC noted responses from commenters that the static, group-level formularies supported by the proposed standard did not provide desired information about individual patient benefits and cost sharing. Commenters also suggested that it was not necessary for ONC to offer certification to this functionality because most health IT systems already supported NCPDP's Formulary and Benefit standard version 3.0 due to the Medicare Part D electronic prescribing requirements. For these reasons, ONC did not finalize use of the standard as a requirement under the "Drug-formulary and preferred drug list checks" certification criterion in § 170.315(a)(10) (80 FR 62623).

The ONC Cures Act Final Rule removed the "drug-formulary and preferred drug list checks" criterion from the Program as of January 1, 2022 (85 FR 25660). We stated that we were retiring the criterion because it was a functional criterion that did not require the use of any specific interoperability standards, and therefore did not provide sufficient value to health care providers or patients to justify the criterion-specific Program compliance burden on developers and health care providers. We also stated that we did not believe it was necessary to continue to require certification of the functionality under the Program in order to ensure it remained widely available (85 FR 25661).

We note that formulary validation is now ubiquitous across the healthcare industry, using distributed formulary and benefit files. Multiple parties are involved in creating, processing, and disseminating these files, and any variation in timing, scope, processing burden, and accessibility introduces additional complexity and delays. Because each health IT developer follows different schedules, for example, information may be out-of-date by the time the health care provider views it in the electronic health record or electronic prescribing application. In addition, the increasing size of these formulary files have led to an increase in the time and resources it takes for a health IT developer to process this data to be available for health care providers when they need it. All these factors may call into question the timeliness and accuracy of the formulary data

[370] https://standards.ncpdp.org/Access-to-Standards.aspx.

available to health care providers at any given time, and any discrepancy between the medication prescribed and its formulary data may impede the success of real-time prescription benefit processes, and slow claims and billing workflows. Simply checking whether a formulary exists for a given medication is no longer sufficient to support the interoperability of formulary and benefits data, especially as real-time prescription benefit and other capabilities emerge that more heavily rely on the real-time availability of accurate formulary data.

While ONC previously declined to finalize the NCPDP Formulary and Benefit standard version 3.0[371] in the retired "Drug-formulary and preferred drug list checks" criterion, we note that the Standard continues to evolve to provide pharmacy benefits managers and payers ways to communicate formulary and benefits information to providers via health IT. The NCPDP Formulary and Benefit standard version 53 includes significant changes and updates since NCPDP Formulary and Benefit standard version 3.0, and many of these changes address some of the issues identified in NCPDP Formulary and Benefit standard version 3.0 that prevented ONC from finalizing it previously. For example, formulary and benefit files have been normalized, made smaller, reusable, and valid only during specified time periods. The alternative and step medication file size has also been reduced and further developed to support diagnostic codes. The step medication files support a more complex step medication program, and coverage files have been updated to include support for electronic prior authorization and specialty medications. The copay files have been updated to allow a minimum and maximum copay range without a percent copay and support for benefit stage copay/deductibles, pharmacy network support, Medicare Part D support and approximate drug cost.

Use of technology conformant to the NCPDP Formulary and Benefit standard can support real-time prescription benefit processes by helping clinicians avoid prescriptions that are not covered by a patient's pharmacy benefit or are more expensive than other prescriptions clinically appropriate for the indication. The standard also improves efficiency in several ways,

[371] https://standards.ncpdp.org/Access-to-Standards.aspx.

helping providers avoid callbacks and the need for additional clarifications on prescriptions or prior authorizations, reducing provider reliance on fax and prescribing burden overall.

We seek comment on whether we should further explore capabilities for Health IT Modules to support access to formulary and benefits information, specifically:

- Should ONC propose a new certification criterion that would enable a user to use a Health IT Module to obtain formulary and benefits information using a more recent NCPDP Formulary and Benefit standard?
- What current challenges do health care providers face in obtaining formulary and benefit information and would a standards-based criterion help to address these challenges?
- Should ONC consider incorporating functionality using the NCPDP Formulary and Benefit standard within the potential real-time prescription benefit criterion discussed above, rather than creating an independent criterion for formulary and benefits functionality?
- What are the key benefits health care providers would likely experience from availability of functionality within certified health IT utilizing the most recent NCPDP Formulary and Benefit standard? If formulary check capabilities have already been widely adopted, how would certification of these capabilities benefit providers?

ii. Electronic Prior Authorization

After receiving a RTPB Request transaction, a processor, PBM, or adjudicator will determine eligibility for the identified patient and determine if the product requires prior authorization. In the RTPB Response, a health care provider may receive notification that a prior authorization is needed for the prescription. Health care providers may benefit from being able to initiate an electronic prior authorization process within the same workflow. For example, within the same interface, health care providers should be able to quickly switch from real-time

prescription benefit functionality to electronic prescribing functionality, and send electronic prior authorization transactions (e.g., PAInitiationRequest, PARequest) in accordance with the "Electronic prescribing" criterion in § 170.315(b)(3), then return to real-time prescription benefit functionality to complete those processes before the prescription is electronically transmitted to the patient's preferred pharmacy.

As noted above, the ONC Cures Act Final Rule adopted the NCPDP SCRIPT standard version 2017071 and updated the "Electronic prescribing" certification criterion in § 170.315(b)(3)(ii) to reflect this standard, including four transactions for electronic prior authorization specified as optional (85 FR 25678). We stated that we adopted these transactions to support alignment with the "Secure Electronic Prior Authorization for Medicare Part D" proposed rule (84 FR 28450), in which CMS proposed to require Part D plan sponsors to support version 2017071 of the NCPDP SCRIPT standard for four electronic Prior Authorization (ePA) transactions, and that prescribers would be required to use that standard when performing ePA transactions for Part D covered drugs they wish to prescribe to Part D eligible individuals (85 FR 25685). CMS subsequently finalized this policy in the "Secure Electronic Prior Authorization for Medicare Part D" final rule with a compliance date of January 1, 2022 (85 FR 86824).

We invite comments on the potential incorporation of these transactions into the "Electronic prescribing" certification criterion and whether we should consider requiring certification to these transactions in a future rulemaking.

iii. Certification Approaches

The formulary and benefit maintenance, real-time prescription benefit, electronic prior authorization, and electronic prescribing capabilities discussed in this RFI are intended to comprise the elements of a unified electronic prescribing workflow. The capabilities and supporting standards noted in this RFI reflect shared data and code sets designed to facilitate re-use of data across the workflow and interoperability across systems. While the Program only includes one pharmacy interoperability criterion at this time (electronic prescribing), we believe

that the addition of capabilities contemplated in this RFI may require a different approach to the Program's design, policy, and testing infrastructure in order to reduce testing burden on health IT developers of certified health IT and better represent real world pharmacy interoperability workflows.

For instance, we are considering approaches in the Program that would allow a Health IT Module (or a health IT product incorporating multiple Health IT Modules to support multiple aspects of electronic prescribing workflow) to undergo testing for more than one pharmacy interoperability criterion during a single, streamlined testing event, while maintaining a modular approach to certification that allows health IT developers to certify to only those criteria relevant to their products. We are seeking public comment on the potential benefits or challenges of such an approach, including:

- If ONC were to propose and finalize additional pharmacy interoperability certification criteria similar to those discussed in this RFI, what would be the challenges of testing each criterion individually?
- Could a bundled approach to testing more than one pharmacy interoperability criterion in a single testing event address these challenges? What other principles or parameters should be applied to such an approach?
- If ONC were to propose an alternate approach to bundled testing for related certification criteria, should such an approach be required for any product a health IT developer seeks to certify to multiple criteria within the bundle, or should it be optional?
- Might there be additional opportunities to reuse testing resources and streamline the testing experience for health IT developers while taking additional steps to ensure that certified health IT is optimized for prescribing safety, efficiency, and usability?

3. FHIR Standard

This request for information focuses on the FHIR standard for APIs (including FHIR Subscriptions, CDS Hooks, FHIR standards for scheduling, and SMART Health Links) and aligns with our aims of advancing interoperability through the use of APIs for treatment, payment and operations use cases. We welcome technical and policy comments as we consider the potentially applicability of these standards and specifications for potential future rulemaking.

a. FHIR Subscriptions Request for Information

A FHIR API is a "RESTful"[372] API, which requires clients to query for information that is served by a FHIR server. The client application has no way of knowing if there has been any addition of new information or an update to existing information. So, in lieu of having that knowledge, the client application would "poll"[373] a FHIR server at regular intervals for new information. As the usage of FHIR APIs increases, so does the demand placed on FHIR servers to be able to provide responses to the clients in a performant manner.

FHIR Subscriptions[374] is a capability supported in the FHIR standard that provides the ability for a FHIR server to proactively notify a client when new information has been added or existing information has been updated. Once the client has received the notification, it can take appropriate action, including querying for the desired information. FHIR Subscriptions also includes the capability to transmit a payload with the "notification," greatly simplifying some interorganizational transactions. This "push-based"[375] subscription method has the advantage of reducing server load by eliminating expensive queries and generally promoting more efficient network behavior. Additionally, push-based subscription can be more easily used to automate system-based workflows using the FHIR standard, such as Admission, Discharge and Transfer (ADT) events.

---

[372] "Representational State Transfer"
[373] http://hl7.org/fhir/4.3.0-snapshot1/pushpull.html.
[374] https://build.fhir.org/subscriptions.
[375] http://hl7.org/fhir/4.3.0-snapshot1/pushpull.html.

FHIR Subscriptions are enabled by the following resources: Subscription[376], SubscriptionTopic[377] and SubscriptionStatus.[378] We seek input on the maturity of these resources in the FHIR Release 4 standard that is incorporated in 45 CFR 170.315(g)(10) (*see* section III.C.7 of this proposed rule). Additionally, we seek comment on whether the FHIR Subscriptions capability aligns with the adoption of the FHIR Release 5 standard, and whether alignment with FHIR Release 5 would avoid any costly refactoring of the resources and give more time for industry to test the various features and capabilities under development.

Furthermore, we request comment on whether there is a need to define a minimum set of Subscription Topics that can be consistently implemented by all health IT developers of certified health IT to provide a base level expectation for clients using the services. We also invite comments on appropriate industry led activities to maintain and keep the artifacts up to date.

Additionally, we welcome comments on security, channels, payloads, and any other areas that would need to be further specified to achieve our goal of providing subscription capabilities across certified Health IT Modules in a consistent and standardized manner using an already adopted standard.

b. Clinical Decision Support Hooks Request for Information

We are including in this proposed rule a RFI seeking input from the public on whether to require certified health IT systems to adopt the CDS Hooks FHIR Implementation Guide v1.0 as part of the requirements in the Program.

i. Background

Clinical decision-making is an important part of the foundation of care delivery. Each patient presents a unique combination of facts and circumstances that require ongoing assessment, planning, intervention, and evaluation. Each decision in the course of a patient's care

[376] http://hl7.org/fhir/4.3.0-snapshot1/subscription.html.
[377] http://hl7.org/fhir/4.3.0-snapshot1/subscriptiontopic.html.
[378] http://hl7.org/fhir/4.3.0-snapshot1/subscriptionstatus.html.

involves gathering, analyzing, and acting on information that may be complex, unclear, or incomplete. Clinical decision makers must account not only for information provided by the patient, but also the continuously evolving and growing body of medical and scientific knowledge.

Health IT has the potential to help address the complexities of clinical decision-making for providers and as part of shared decision-making with patients and care team members. CDS provides clinicians, staff, patients, and other individuals with knowledge and person-specific information, intelligently filtered and/or presented at appropriate times to enhance decision-making. CDS encompasses a variety of tools, including computerized alerts and reminders, clinical guidelines, condition-specific order sets, focused patient data reports and summaries, documentation templates, diagnostic support, and contextually relevant reference information.[379] Currently, the Program includes the certification criterion "clinical decision support (CDS)" in § 170.315(a)(9). If certified to that criterion, a Health IT Module must implement HL7 Version 3 and HL7 Clinical Document Architecture (CDA) standards to meet specific requirements outlined in the criterion. Sections III.C.5.a-c of this proposed rule provide additional discussion of the history of CDS-related certification criteria as well as proposed changes to these criteria, including proposed new requirements for some forms of decision support.

CDS is a common capability provided by EHR systems today. Computerized physician order entry (CPOE), for example, is often paired with CDS to help clinicians select the appropriate medications for their patients and provide alerts if a patient is allergic to a particular medication.[380] Likewise, federal agencies such as the Agency for Healthcare Research and Quality (AHRQ) have funded programs aimed at helping health care providers move patient-centered outcomes research (PCOR) evidence into practice through CDS.[381] AHRQ's CDS

[379] https://www.healthit.gov/topic/safety/clinical-decision-support
[380] https://www.ncbi.nlm.nih.gov/books/NBK543516/
[381] https://cds.ahrq.gov/

Connect is an online platform including a repository of CDS artifacts and tools for creating, testing, and sharing CDS.[382]

Although there have been numerous studies demonstrating the value and efficacy of CDS, available evidence suggests the CDS must be carefully implemented and managed to achieve its potential.[383] One of the challenges associated with CDS involves interoperability. For example, a CDS system may exist as a standalone system or lack the ability to communicate effectively with other systems.[384] Disparate EHRs and health IT systems may use different data models and CDS integration methods, which limits the widespread dissemination of effective CDS content.[385]

Standards development organizations like HL7 provide standards that aim to address some of the CDS interoperability challenges. The FHIR CDS Hooks specification, for example, describes the RESTful APIs and interactions using JSON over HTTPS to integrate CDS between CDS Clients (e.g., EHRs or other health information systems) and CDS Services.[386] CDS Hooks enable users to invoke CDS services within a workflow.[387] By standardizing an approach for calling CDS services from within a workflow, the CDS Hooks specification provides a consistent set of capabilities around which CDS developers can design CDS services.

ii. Request for Information

Given the growing use of CDS and potential for CDS to improve clinical decision-making, we request comment on the scope and maturity of the FHIR CDS Hooks specification v1.0, which we are considering for future inclusion as part of the Program. Recognizing that CDS Hooks does not prescribe a default or required set of hooks for implementers, we further request comment on specific hooks that we might include in future certification criteria (the CDS Hooks specification, for example, defines a small set of hooks), as well as input on use of CDS

---

[382] https://cds.ahrq.gov/cdsconnect
[383] https://nam.edu/optimizing-strategies-clinical-decision-support/
[384] https://www.nature.com/articles/s41746-020-0221-y
[385] https://nam.edu/optimizing-strategies-clinical-decision-support/
[386] https://cds-hooks.org/specification/current/
[387] https://www.healthit.gov/sites/default/files/page/2023-02/SDOH-CDS-Feasibility-Brief.pdf

Hooks for supporting workflow improvement and reducing health care provider burden. To the extent commenters have specific CDS Hook use cases for supporting the latter, we welcome input on this including comment on the readiness and feasibility of such use cases including, as an example, for the screening and assessing of social risk and health related social needs or history.[388]

c. FHIR Standard for Scheduling Request for Information

Based on public engagement and published analysis,[389] we have identified that the use of standards-based APIs for access to and booking of appointments for patients would result in significant long-term improvements in reducing health disparity and improving public health. One such example relates to the recent immediate need for making vaccine appointments for COVID-19 more widely available.

During the launch of COVID-19 vaccination in US, many individuals experienced difficulties in obtaining timely vaccination appointments, including signing up for waitlists at multiple clinics, constantly refreshing different websites that advertised vaccine availability, and repeatedly calling busy phone lines.[390] One of the key takeaways from the analysis reported by U.S. Digital Response was that while vaccine providers reported their vaccine inventory data to public health authorities, the inventory data did not directly or accurately reflect appointment availability. Indeed, their finding indicated that inventory-based vaccine finders were a root cause of frustration for eligible U.S. residents in states across the nation.[391]

Once these issues within vaccine appointment scheduling became known, the health IT industry came together to address the situation in a rapid manner. One such industry-led solution that was developed during the time, and has since gained widespread support, is SMART

---

[388] ONC Social Determinants of Health Clinical Decision Support Feasibility Brief, February 2023: https://www.healthit.gov/sites/default/files/page/2023-02/SDOH-CDS-Feasibility-Brief.pdf
[389] https://medium.com/u-s-digital-response/what-vaccine-appointment-data-tells-us-three-major-takeaways-from-covid-19-cb6adcaa8acf
[390] https://medium.com/u-s-digital-response/usdrs-appointment-finder-tools-and-services-for-faster-easier-access-to-covid-19-vaccines-92e87a722efa
[391] https://medium.com/u-s-digital-response/usdrs-appointment-finder-tools-and-services-for-faster-easier-access-to-covid-19-vaccines-92e87a722efa

Scheduling Links.[392] SMART Scheduling Links is a FHIR standard-based specification that enables providers to advertise their available vaccine appointments using a lightweight, scalable API that is based on the same FHIR Release 4 standard that is widely implemented by the health IT industry as part of the Program criterion in § 170.315(g)(10).

In this RFI, we seek input on the maturity and scope of the SMART Scheduling Links Implementation Guide that is aligned with FHIR Release 4, to be considered for future certification as part of the Program.

Furthermore, we request comment on the guidance specified in the SMART Scheduling Links Implementation Guide for publishers to advertise the API endpoints and whether there are other approaches that ONC could take to ensure that the APIs are easily discoverable by users of the API.

We also invite comments on any other appropriate industry led activities that we should consider for potential models and approaches, such as the Argonaut Scheduling Implementation Guide.[393] Additionally, we welcome any other comments on how to ensure accuracy and timeliness of appointment information. Finally, we welcome comments on how to support the scalability of the standard for use in a variety of healthcare settings, in order to achieve our goal of providing this capability across all certified Health IT Modules in a consistent and standardized manner using an already adopted standard.

d. SMART Health Links Request for Information

The SMART Health Cards[394] standard has seen rapid adoption in the past few years as a reliable and easy way for consumers to receive verifiable clinical information, such as COVID-19 vaccination history or test results. It has been widely supported across the U.S. by public

[392] https://github.com/smart-on-fhir/smart-scheduling-links
[393] http://fhir.org/guides/argonaut/scheduling/index.html#introduction
[394] https://smarthealth.cards/en/

health departments in several states, nationwide pharmacies, developers of certified health IT and test providers.[395]

While the COVID-19 pandemic certainly played a major role in rapid response by industry, we have heard from industry that some of the key reasons for the implementation success of SMART Health Cards included the focus on a limited data set, which could be provided by health care providers in a verifiable and secure manner using existing FHIR API technologies available in their health IT, and packaged using QR[396] format that allows individuals to easily share this information with others.

ONC is generally supportive of such innovative efforts to advance API capabilities for targeted needs. We have been tracking industry advances in not only the SMART Health Cards standard, but also a more recent effort, called SMART Health Links Protocol.[397]

Our understanding is that, conceptually, the SMART Health Links Protocol[398] takes some of the same approach used for SMART Health Cards for sharing data. This includes the use of a structured and cryptographically signed set of clinical data provided in the FHIR standard and made available to the individual in a QR format, which is intended to allow individuals explicit control over with whom they share their health information. At the same time, SMART Health Links aims to overcome some of the known limitations of the SMART Health Cards technology, including the small amount of data that can be fit in a QR, and the ability to share data that could be changing over time, rather than a static data set that is possible in a SMART Health Card. We are also aware that the SMART Health Links Protocol is in a very early conceptual stage and may not be ready for implementation in the next several years.

In this RFI, we seek input on the value and feasibility of the SMART Health Links Protocol, as well as concerns regarding its implementation. Furthermore, we invite comment

---

[395] https://smarthealth.cards/en/issuers.html
[396] https://spec.smarthealth.cards/#creating-a-qr-code-or-a-set-of-qr-codes-from-a-health-card-jws
[397] https://hackmd.io/@VCI/smart-health-links-protocol
[398] https://hackmd.io/kvyVFD5cQK2Bg1_vnXSh_Q

from the public on approaches ONC could take, within our authorities, to encourage rapid advancement of the technology.

We also request information on any other promising industry-led innovative activities that we should consider that are aligned with the FHIR standard, and which would help us advance towards achieving our goal of improving interoperability using health information technology.

IV. Information Blocking Enhancements

A. Defined Terms

1. Offer Health Information Technology or Offer Health IT

Health IT developer of certified health IT is defined for purposes of the information blocking regulations as: "an individual or entity, other than a health care provider that self-develops health IT for its own use, that develops *or offers* health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj-11(c)(5) (ONC Health IT Certification Program)" (*emphasis added*, 45 CFR 171.102). Preamble discussion in both the ONC Cures Act Proposed Rule (84 FR 7511) and Final Rule (85 FR 25798 through 25799) addressed that the definition includes offerors of certified health IT who do not themselves develop certified health IT or take responsibility for the health IT's certification status under the Program.

Specifically, we explained that "an individual or entity that offers certified health IT" would include "any individual or entity that under any arrangement makes certified health IT available for purchase or license" (85 FR 25798). Both individuals or entities that otherwise fall into at least one category of actor as defined in 45 CFR 171.102—such as health care providers—and individuals or entities who otherwise would not fit the definition of any category

of actor could offer certified health IT that they did not themselves develop or present for certification. As offerors of certified health IT, these individuals or entities could engage in conduct that constitutes information blocking as defined in § 171.103, such as through contractual terms or practices undertaken in operating and maintaining health IT used by another individual or entity.

In the ONC Cures Act Final Rule (85 FR 25642), we noted that PHSA section 3022(b)(1)(A) expressly references both "a health information technology developer of certified health information technology" and "other entity offering certified health information technology" in the context of authority to investigate claims of information blocking (85 FR 25798). We further explained that including both developers and other offerors in the definition of "health IT developer of certified health IT" is consistent with the policy goal of holding all entities who could, as a developer or offeror, engage in information blocking accountable for their practices that are within the definition of information blocking in § 171.103 (85 FR 25799).

We received comments on the ONC Cures Act Proposed Rule (84 FR 7424) expressing concern about holding offerors who do not themselves develop the health IT accountable for design features or other things done by the developer of the health IT. We did not receive public comments on the ONC Cures Act Proposed Rule (84 FR 7424) questioning or expressing concerns specifically about our interpretation that "individual or entity that offers certified health IT" would include an individual or entity that *under any arrangement* makes certified health IT available for purchase or license (*emphasis added*, 84 FR 7511). The policy we finalized (85 FR 25642) makes no distinction between making certified health IT available for sale, resale, license, re-license, or sublicense under other types of arrangements and making certified health IT available under arrangements designed to benefit the recipient of free or below-cost certified health IT. We did not, in the ONC Cures Act Final Rule, specifically define what it means to *offer health information technology* or *offer health IT*.

Following the publication of the ONC Cures Act Final Rule, public feedback has been received through our Health IT Feedback and Inquiry Portal and through real-time interactions with interested parties in various venues on many points of information blocking policy. Specific to the definition of *health IT developer of certified health IT* (as defined in § 171.102) and what makes an individual or entity one that *offers* certified health IT for purposes of this definition, interested parties posed questions and expressed concerns that health care providers and entities not otherwise information blocking actors[399] might stop funding subsidies to providers who cannot otherwise afford certified health IT. A key source of concern identified was a lack of certainty as to whether such subsidies could be considered to be offering health IT, resulting in the donor/benefactor entities making available funding subsidies becoming subject to the definition of *health IT developer of certified health IT* across all of their technology, business lines, and activities. This is of significance to current and potential donors who are either not otherwise information blocking actors of any type or otherwise would be considered *health care providers*[400] for purposes of the information blocking regulations. For (potential) donors who are not otherwise information blocking actors, such as philanthropic organizations or health plans,[401] a key concern reportedly affecting their willingness to subsidize certified health IT to providers in need under current policy is presumably that their choice to *offer* certified health IT is also a choice to subject all of their technology and business practices potentially affecting access, exchange, or use of EHI across their entire business to the information blocking regulations in 45

---

[399] Although not specifically excluded from the actor definition, a wide variety of entities, including charitable organizations, philanthropic foundations, and health plan issuers are not specifically included in the definition of "actor" in § 171.102 and thus will be subject to the information blocking regulations only to the extent they engage in activities that cause them to meet the definition of *health care provider, HIN/HIE* or *health IT developer of certified health IT*. (For more information, see IB.FAQ13.1.2020NOV and 85 FR 25803.)

[400] As defined in § 171.102, health care provider has the same meaning as "health care provider" in 42 U.S.C. 300jj. For more information about this definition in a convenient format, please consider viewing the Health Care Provider Definition (PDF - 361 KB) fact sheet.

[401] A health plan, or health plan issuer, could also meet the definition of one or more types of information blocking actor regardless of whether they donate or otherwise supply certified health IT to individuals or entities other than their own employees and contractors. However, a health plan that does not meet the § 171.102 definition of any type of information blocking actor is not considered an information blocking actor for purposes of the information blocking regulations in 45 CFR part 171.

CFR part 171 as well as up to $1 million per violation civil monetary penalties authorized in the Cures Act's information blocking provision (42 U.S.C. 300jj–52(b)(2)(A)).

Although health care providers are already information blocking actors, those who might be in a position to offer cost subsidies to other providers may be hesitant to do so because of the differences in the information blocking definition and consequences for a *health IT developer of certified health IT* compared with those for a *health care provider.* First, it is significant that information blocking, when conducted by a *health care provider,* is defined in part by whether the health care provider "knows that such practice is unreasonable and is likely to interfere," which is for the actor, a less exacting knowledge standard than that applied to conduct of a *health IT developer of certified health IT*: whether the developer "knew or should have known that such practice is likely to interfere" (§ 171.103, *see also* 42 U.S.C. 300jj–52(a)(1)). Second, while *health care providers* who are found to have engaged in information blocking will be subject to appropriate disincentives set forth by the Secretary,[402] *health IT developers of certified health IT* who are found to have engaged in information blocking are subject to the 42 U.S.C. 300jj–52(b)(2)(A) civil monetary penalty of up to $1 million per violation. This concern has been raised since the publication of the ONC Cures Act Final Rule in both written informal correspondence and real-time interactions by third parties concerned about small, safety net and other lower-resource providers' ability to afford certified health IT.

We have also received, through public interaction in various venues, several requests that we clarify, in a manner providing certainty, that a provider using certified health IT acquired from a developer or other offeror will not come to be considered a *health IT developer of certified health IT* if the provider implements features and functionalities in their EHR systems, such as APIs for patients and clinicians to use third-party apps[403] of their choosing. We had

---

[402] Health care provider disincentives specific to information blocking are expected to be set forth in a separate rulemaking action.

[403] In this discussion, for ease of discussion, we use "third party" to reference any and all entities other than the actor from whom EHI access (as "access" is defined in § 171.102) is sought or the entity by or on whose behalf the EHI that would be modified is maintained. We use "third-party app" to reference any and all sorts of software products

discussed, in the ONC Cures Act Final Rule preamble specific to health care providers that self-develop certified health IT "for their own use," that several of these activities would not be considered offering or supplying health IT to other entities.[404] Feedback we received indicated that providers who do not self-develop the certified health IT they implement would experience less uncertainty if we were to provide definitive assurance that we do not consider activities such as a hospital issuing login credentials allowing licensed healthcare professionals who are in independent practice to use the hospital's EHR to furnish and document care to patients in the hospital to be "offering" certified health IT to other entities when the hospital in question uses health IT they obtained from a developer or offeror (such as a reseller).

To give clarity about the definitional implications under information blocking regulations of making available funding subsidies and certain features or uses of certified health IT, we now propose to codify a definition of what it means to *offer* certified health IT. The definition we propose generally includes providing, supplying, or otherwise making available certified health IT under any arrangement or terms, but explicitly excludes certain activities for one of two purposes:

(1) to encourage beneficial arrangements under which providers in need can receive subsidies for the cost of obtaining, maintaining, or upgrading certified health IT; or

(2) to give health care providers (and others) who use certified health IT concrete certainty that implementing certain health IT features and functionalities, as well as engaging in certain practices that are common and beneficial in an EHR-enabled healthcare environment, will *not* be considered an offering of certified health IT (regardless of who developed that health IT).

---

or applications developed and/or offered by a third party, regardless of the types of hardware on which such app might run (e.g., mobile device versus server). We also use "third-party app" in this context to include the full variety of purposes and users such apps might support (e.g., licensed healthcare professionals, patients) and without regard to whether such "third party" is or is not a HIPAA covered entity or business associate of any HIPAA covered entity, as such terms are defined in 45 CFR 160.103.

[404] 85 FR 25799

We further propose potential exclusions we are considering that would provide that an individual or entity is not considered to be *offering health IT* under the proposed definition while furnishing certain legal, health IT expert consulting, or management consulting services to health care providers or others who obtain and use health IT.

a. Exclusion of Certain Funding Subsidy Arrangements from *Offer* Definition

As finalized in the ONC Cures Act Final Rule and consistent with the Cures Act's information blocking provision (42 U.S.C. 300jj–52), an individual or entity that *offers* any certified health IT currently stands on exactly the same footing as an individual or entity that develops certified health IT. The "health IT developer of certified health IT" definition finalized in the ONC Cures Act Final Rule applies to an individual or entity that develops or offers at least one certified Health IT Module across any and all of their conduct meeting the definition of information blocking in § 171.103 (85 FR 25797). For reasons discussed in the ONC Cures Act Final Rule, we believe this is the most appropriate approach to the *health IT developer of certified health IT* regulatory definition in the context of the plain language of the information blocking provision in the Cures Act itself.[405]

As stated in the ONC Cures Act Proposed (84 FR 7511) and Final (85 FR 25798) Rules, under current information blocking regulations (45 CFR part 171) "an 'individual or entity that offers certified health IT' would include an individual or entity that under any arrangement makes certified health IT available for purchase or license."

We have believed since long before we issued the ONC Cures Act Proposed Rule, and we continue to believe today, that arrangements that help small or safety net providers afford certified health IT items and services are generally beneficial to the recipient providers and their patients. We further believe policy goals for interoperability, information sharing, and equity throughout the U.S. healthcare system are supported by encouraging the provision of grants or

[405] 21st Century Cures Act, Pub. L. 114-255. The Cures Act information blocking provision (§ 4004 of the law) is codified at 42 U.S.C. 300jj–52.

funding subsidies, consistent with other applicable laws, to health care providers who may otherwise struggle to afford modern, interoperable health IT.

Now that we have been made aware of concerns regarding the potential inclination of some health care providers and other donors to stop making available funding subsidies toward the cost of certified health IT for providers who may not otherwise be able to afford it, we believe it is appropriate to consider ways to modify our policy. Specifically, in the proposed definition of what it means to offer health IT in § 171.102, we propose to explicitly exclude certain beneficial arrangements providing funding subsidies for providers to obtain, maintain, and/or upgrade certified health IT.

Exclusion (1) would remove from the definition of *offer health information technology* or *offer health IT* the provision of subsidies, in the form of funding or cost coverage subsidy arrangements for certified health IT. The exclusion depends, however, on the subsidy being made without any conditions limiting the interoperability or use of the technology to access, exchange, or use electronic health information for any lawful purpose. We would interpret conditions broadly, to include not only the explicit terms of any written agreement but also oral statements and patterns of conduct on the part of the subsidy's source(s) toward, in the presence of, or made known by the source(s) to the subsidy's recipient. For an illustrative example, a health system offers to give any independent safety net provider in its multi-state service area a code that enables the safety net provider to contract with a developer for a (developer hosted and fully supported) EHR product suite that includes all certified functionality needed to participate successfully in Medicare's Quality Payment Program (QPP) and have the cost of that EHR subscription charged to and paid by the health system. In this illustrative example, the health system clarifies that it is willing to cover the costs of what is minimally necessary for QPP, and a particular level of service from the EHR developer. The safety net provider in this example may, without discouragement, interference, or inducement on the part of the health system choose at its own expense to contract with the developer for additional functionalities or levels of service,

or contract with other developers for other applications to interface with and use in complement to the EHR suite supported by the health system. So long as the health system does not, in writing or through oral statements or courses of conduct, condition any initial or continued payment of the safety net provider's subscription costs on the safety net provider limiting its use of health IT or its access, use, or exchange of EHI in ways specified or signaled by the health system, the health system's cost coverage subsidy of the safety net provider's EHR suite subscription would not be considered an *offer* of certified health IT under the proposed definition.

We note that we do not believe it is necessary to assess, for purposes of determining whether a funding subsidy should be considered an offer of certified health IT, whether the source(s) of the subsidy conditions the subsidy on a recipient health care provider referring patients to or away from the source. Other law—not limited to but notably including 42 U.S.C. 1320a–7b(b) where payment for any item, service, or good may be made in whole or part under a "Federal health care program" (as defined in 42 U.S.C. 1320a–7b(f))—is implicated by solicitation or receipt of any remuneration in return for referral steering and similar conduct. The proposed tailoring of the funding subsidies exclusions from the *offer health information technology* or *offer health IT* definition are thus not intended to address referral steering or similar conduct focused on healthcare services volume, demand, or market share. Rather, these exclusions are conditioned on the source(s), donor(s), or giver(s) of any such subsidy or supplier of such subsidized technology not limiting uses of the technology or access, exchange, or use of EHI specifically as a safeguard against inappropriate exploitation of this exclusion by entities seeking to distort the health IT items and services market—including through limiting recipients' options to use additional technology—or otherwise impede innovations and advancements in health information access, exchange, and use.

If an individual or entity engages in conduct that meets the *offer health IT* definition, it would be considered a *health IT developer of certified health IT* under the definition, even if it

engages in other conduct that meets an exclusion. We are not proposing to create any categorical exclusions of particular classes of individuals or entities. None of the proposed exclusions from the *offer health IT* definition are designed or intended to function as loopholes through which individuals or entities who engage in separate conduct that would otherwise meet the definition of *offering health IT* would no longer be considered health IT developers of certified health IT.

Similarly, an individual or entity that otherwise meets the definition of an information blocking *actor* in § 171.102 (such as a health care provider, health information network or exchange, or individual or entity who develops certified health IT) would not be able to claim that they are excluded from any definition of actor by meeting an exclusion from the definition of *offer health IT*. An individual or entity that meets an exclusion from the definition of *offer health IT*, but otherwise meets one of the definitions of information blocking actors continues to meet that definition of an actor.

b. Implementation and Use Activities That Are Not an Offering

In the ONC Cures Act Final Rule preamble, we noted that there are certain actions taken by health care providers who self-develop health IT for their own use that we do not interpret as them offering or supplying certified health IT to others. Specifically, we noted that "some use of a self-developer's health IT may be made accessible to individuals or entities other than the self-developer and its employees without that availability being interpreted as offering or supplying the health IT to other entities in a manner inconsistent with the concept of 'self-developer,'" and we provided examples of activities that we do not consider offers (85 FR 25799). Some of the examples we noted were discussed in context of customary practices amongst hospitals that purchase commercially marketed health IT as well as self-developer hospitals.

We do not, and do not believe anyone else should, consider the examples discussed at 85 FR 25799 to be offerings of health IT in any sense relevant to the *health IT developer of certified health IT* definition, *regardless* of who developed the certified health IT that may be needed, used, or otherwise involved in these examples. We also believe there may be examples of

activities we did not discuss at 85 FR 25799 that should not be considered offers of health IT, as described below. We therefore propose to explicitly exclude from the *offer health information technology* or *offer health IT* definition in paragraph (2) of the definition the implementation, operation, or maintenance, by any health care provider or other entity (such as a HIN/HIE or public health authority) of any and all of the following:

- Issuing login credentials to employees (whether "W2"/traditional or "1099"/contracted or "gig" employee) of the individual or organization for purposes of accessing, using, or exchanging EHI within the scope/duties of their employment or contract. This would include, though it is not limited to, in-house counsel while acting within scope of their engagement as in-house counsel.
- Production instances of API technology supporting patient (also known as "individual") access or other legally permissible access, exchange, or use of EHI that the individual or entity has in its possession, custody, control, or ability to query from/across a HIN/HIE.
- Production instances of online portals for patients, clinicians, or other health care providers (including employed, affiliated, non-affiliated, or independent providers), or public health entities to access, exchange, or use EHI that the that the individual or entity has in its possession, custody, control, or ability to query from/across a HIN/HIE.
- Issuing login credentials or user accounts to production or development/testing environments to public health authorities or such authorities' employees as a means of accomplishing or facilitating access, exchange, and use of EHI for public health purposes including but not limited to syndromic surveillance.

We also propose to explicitly exclude from the *offer health information technology* or *offer health IT* definition the issuance of login credentials such as EHR login credentials, by the operator of a healthcare facility—such as a hospital, nursing facility, clinic, or dialysis center—

for non-employed/independent healthcare professionals who furnish care in the facility to use the facility's EHR in connection to furnishing and documenting that care.

We reference production instances in proposed paragraph (2) but do not propose to establish a formal definition of "production instance" specific to this purpose. We do not believe that is necessary because we observe health IT developers, resellers, and customer organizations communities generally using and understanding a production instance as a particular implementation of a given health IT product that has "gone live" in a production environment. Production environments, in turn, we observe are generally understood as being the setting where health IT is implemented, run, and relied on by end users in day-to-day conduct of their profession (such as medicine, nursing, or pharmacy) or other business (such as a payer processing healthcare reimbursement claims or a patient managing their health and care). Many health care provider organizations, such as small clinician office practices, may only obtain use of a production instance of whatever health IT they use (such as a patient portal). However, other health care provider organizations' enterprise IT setups do include test, staging, or other pre-production environments where new or updated software or other health IT can be configured and confirmed to operate well in the overall environment before it "goes live" to end users in the production environment.

The reference to production instances in the proposed paragraph (2) explicitly does *not* mean that simply having any pre-production instance(s) of health IT would, of itself, constitute offering health IT. It also explicitly does *not* mean that using non-employee volunteers, such as patient volunteers or independent clinician volunteers, in user experience testing and improvement activities with pre-production instances of any health IT would, of itself, constitute offering health IT. These types of testing activities, again by nature and purpose, do not make the technology available for use and reliance by end users in practice of their profession or conduct of their other business. We have focused the proposed exclusion on production instances of things like portals simply because that is where the question has arisen: does making a portal that

is part of a certified health IT product available for use by someone who is not a provider's (contracted or W2) employee mean the provider is offering certified health IT to others? The question has not arisen for pre-production instances of health IT. We infer this is because development, test, staging or other pre-production instances of health IT are, by nature, not used or relied upon by end users of the health IT in day-to-day conduct of their profession or business.[406] We seek comment on this proposal, including whether we should consider revising or refining any of the descriptions or wording of the functionalities, features, actions, or activities listed in the draft regulation text or whether we should consider explicitly excluding additional activities, actions, or health IT functionalities from what it means to *offer* certified health IT.

c. Consulting and Legal Services Exclusion from *Offer* Definition

In defining what it means to *offer health information technology* or *offer health IT*, we are also considering whether it would be beneficial to explicitly establish an exclusion of certain management consulting services that play important roles in some providers' approaches to operational management of their practice, clinic, or facility. Therefore, we have chosen to propose an exclusion to the *offer health IT* definition so that we could take binding action more quickly than would otherwise be possible in the event we conclude, in consideration of comments and information we receive in response to this proposal, that finalizing this exclusion—in whole or in part, and with or without modifications —would better support important policy goals such as advancing interoperability and information sharing or reducing clinician burden.

The bundled exclusions we propose in paragraph (3) of the definition would address specific legal and consulting services related to obtaining and maintaining health IT or involving

---

[406] To note, "end users of the health IT" means, for example, the patients who use a patient portal or clinicians who use an e-prescribing Health IT Module. "End users" do not in this context include health IT professionals whose day-to-day professional practice or other business is developing, testing, and/or maintaining health IT products. Some IT professionals might conduct a majority, if not the entirety, of their day-to-day work in technology development, testing, maintenance, and support of health IT intended for using the pre-production environments and instances alongside other tools.

health IT in certain ways. The services addressed by the subparagraphs of the paragraph (3) "consulting and legal services" exclusion would include:

- legal services furnished by attorneys that are not in-house counsel[407] of the provider (commonly referred to as "outside counsel");
- health IT expert consultants' services engaged to help a health IT customer/user (such as a health care provider) define their business needs and/or evaluate, select, negotiate for or oversee configuration, implementation, and/or operation of a health IT product that the consultant does not sell/resell, license/relicense, or otherwise supply to the customer; and
- clinician practice or other health care provider administrative or operational management consultant services where the clinician practice or other health care provider administrative or operational management consulting firm effectively stands in the shoes of the provider in dealings with the health IT developer or commercial vendor and manages the day-to-day operations and administrative duties for health IT and its use alongside other administrative and operational functions that would otherwise fall on the clinician practice or other health care provider's partners, owner(s), or staff.

Questions have arisen for us regarding if or when a health care provider's outside counsel risks becoming an individual or entity that offers certified health IT by virtue of various representational activities. At (3)(a) in the proposed *offer health information technology* or *offer health IT* definition's proposed regulatory text, we propose to explicitly exclude legal services furnished by outside counsel in any matter or matters pertaining to the client's seeking, assessing, selecting, or resolving disputes over contracts or other arrangements by which the client(s) obtain use of certified health IT. We can also foresee a potential for the question to arise among attorneys and litigation support experts as to whether special care might need to be taken if considering granting an opposing party or their own independent expert witnesses limited use

[407] As noted above, in-house counsel would for purposes of the offer definition be considered "employees" of the provider. Furnishing use of the provider's health IT to in-house counsel would no more be an offer of that health IT than would be furnishing use of that same health IT to members of the provider's nursing or medical records staff.

(e.g. view-only access) to a health care provider's EHR or to a test/litigation-only instance of the same software, in order to expedite discovery in negligence, malpractice, or other matters, or if this option must be entirely outside the realm of consideration specifically to avoid the law firm or its client health care provider becoming an offeror of health IT for information blocking purposes.

To be clear, no one has yet brought to our attention a fact pattern in which a law firm's provision of advice, counsel, or other legal services supporting the negotiation, drafting, or execution of agreements by which the provider obtains use of health IT crosses into the realm of activities we would interpret as equivalent to the law firm itself offering the health IT. We have yet to hear a single report of a health care provider or other prospective health IT customer being unable to obtain assistance of competent counsel for their dealings with health IT developers and vendors due to law firms being concerned by any aspect of the *health IT developer of certified health IT* definition having implications for the law firm. We have also neither seen nor heard of an actual instance where counsel would have made different, potentially more mutually efficient, use of the client's certified health IT in the discovery process but for concerns about the *health IT developer of certified health IT* definition in § 171.102.

However, as we are proposing the exclusion from the *offer health IT* definition of management and other consulting services, we think it is worth considering potential explicit exclusion of legal services rendered to a client in any matter or matters pertaining to the client's seeking, assessing, selecting, or resolving disputes over contracts or other arrangements by which the client(s) obtain use of certified health IT. We would not consider a licensed attorney, law firm, or law firm staff acting under supervision of one or more licensed attorneys, engaged as outside counsel to offer certified health IT when the attorney, attorneys, or law firm staff are furnishing legal services to a client that is a customer or user of certified health IT. Under this proposal, legal services of outside counsel (law firms of any size or individual attorneys not employed by the health IT customer/attorney's client) would remain outside the definition of

offer health information technology or *offer health IT* even when the services include representing or acting on behalf of the client health IT customer in seeking or assessing certified health IT or in the course of negotiations or disputes with a developer, vendor, or other supplier of certified health IT.

This proposed exclusion would: codify how we already view, in the context of the definitions currently codified in § 171.102, legal services furnished by outside counsel in certain matters; and remove an ambiguity that could, at least in theory, otherwise have unintended effects on how parties may in the future assess the best available options and mechanisms for efficient, cooperative discovery. The proposed exclusion for legal services furnished by outside counsel, like the proposed exclusion of health IT expert consulting services, would focus on the services provided and *not* on the type of organization providing them. The exclusion's provision for facilitating appropriately limited access or use of the client's health IT for specific purposes of legal discovery[408] is no exception: it would remain focused on the services provided and *not* on the type of organization providing them. Thus, neither an attorney nor a law firm would be categorically excluded from ever being considered an individual or entity that offers health IT. For example, a law firm that chose, directly or through an entity it owns or controls, to provide or supply certified health IT for use of one or more other, independent individuals or entities under any arrangement would under current regulations be considered to be offering health IT and thus a *health IT developer of certified health IT* for purposes of the information blocking regulations. Under the proposal, an attorney or law firm that engaged in any activities that are within the proposed definition of *offer health IT* would thus be considered an individual or entity that offers health IT and thus a *health IT developer of certified health IT* for purposes of the information blocking regulations.

---

[408] To learn more about what legal discovery is, information presented for general audiences is available at:

- https://www.americanbar.org/groups/public_education/resources/law_related_education_network/how_courts_work/discovery/ (last accessed March 16, 2023)
- https://www.peoples-law.org/maryland-circuit-court-discovery#:~:text=%22Discovery%22%20is%20a%20process%20you,claims%20being%20made%20against%20you. (last accessed March 16, 2023)

We focus this proposed exclusion from the *offer health IT* definition on outside counsel (law firms of any size or individual attorneys not employed by the health IT customer/attorney's client) because we consider attorneys who are employees of the provider to be a part of the provider's organization and operations when acting within the scope of their employment. Outside the scope of their employment by the health care provider, such attorneys' conduct would be assessed like that of any other individual: based on the facts and circumstances to determine whether they were in those outside activities offering health IT as we propose to define *offer health IT*.

We solicit comment on this proposal.

At (3)(b) in the proposed *offer health information technology* or *offer health IT* definition's proposed regulatory text, we propose to explicitly exclude health IT expert consultants' selection, implementation, and use services engaged to help a health IT customer/user (such as a health care provider, health plan, or HIN/HIE) do any or all of the following with respect to any health IT product that the consultant does not sell or resell, license or relicense, or otherwise supply to the customer under any arrangement on a commercial basis or otherwise: define their business needs; evaluate, or select health IT product(s); negotiate for the purchase, lease, license, or other arrangement under which the health IT product(s) will be used; or oversee configuration, implementation, or operation of a health IT product(s). This proposal would codify an exclusion from the definition of *offer health information technology* or *offer health IT*, with explicit parameters, activities for which a health IT customer/user may need or want assistance of individuals or firms with specialized health IT expertise in selecting new or additional health IT product(s) or in complement to the support services available from the developer or commercial vendor once product(s) are selected or implemented. In parallel to the proposed exclusion for legal services furnished by outside counsel, the proposed exclusion of health IT expert consulting services from the *offer health IT* definition would focus on the services provided and *not* on the type of organization providing them. In the health IT context,

the practical implication of the focus and contours of this exclusion mean that any given individual or entity could in its relationship with one of its clients, not be offering health IT but in its relationship with another client be functioning as a commercial vendor of particular products. In this example, where one individual or entity engages in activities that are not considered offering health IT and also, in separate dealings, also offers health IT, such individual or entity would be considered a *health IT developer of certified health IT* across all their health IT items and services like any other individual or entity that *offers* any health information technology that includes one or more certified Health IT Modules. By contrast, so long as an individual, firm, or company only furnishes health IT expert consultant services consistent with the proposed exclusion, and does not choose to also *offer health IT*, then such consultant firm would remain excluded from the definition as proposed.

We solicit comment on this proposal.

At (3)(c) in the proposed *offer health information technology* or *offer health IT* definition's proposed regulatory text, we propose to exclude comprehensive clinician practice or other health care provider administrative or operational management consultant services where the administrative or operational management consulting firm effectively stands in the shoes of the provider in dealings with the health IT developer or commercial vendor and manages the day-to-day operations and administrative duties for health IT and its use alongside a comprehensive array of other administrative and operational functions that would otherwise fall on the clinician practice or other health care provider's partners, owner(s), or staff.

Alone among the three proposed exclusions of consulting and legal services arrangements, the exclusion of clinician practice or other health care provider administrative or operational management consulting services would be likely to include, on a regular basis, arrangements where the health IT the health care provider uses is directly provided to them by the consultant—for example, as part of a comprehensive ("turn key") package of practice management or other provider administrative or operations management services. In proposing

this specific exclusion ((3)(c)), we call potential commenters' attention first and foremost to its implication for health care providers' accountability for acts or omissions of their consultants operating under the exception—particularly health care providers' administrative or operational management services consultants—that implicate the definition of information blocking in § 171.103: where a an administrative or operations management services firm would not be considered to be making an offer of certified health IT for which they contract on behalf of one or more practices (or facilities or sites of care) *because they are acting as the provider's agent or otherwise standing in the shoes of the provider* in selecting and contracting for a variety of services and supplies—including but not limited to the health IT that includes at least one certified Health IT Module—we would view the provider as retaining accountability for any information blocking conduct that the management services company perpetrates while thus acting on the provider's behalf. We recognize this may have implications for how providers may wish to structure administrative and operational services contracts in the future, potentially including a provider seeking representations and warranties giving the provider assurance that the administrative or operations management services company will not without the provider's direction, knowledge, or approval, engage in practices[409] not required by law or covered by an information blocking exception that is likely to interfere with access, exchange, or use of EHI and could be unreasonable. However, this exclusion is not intended to have—and we do not believe it would have—the effect of regulating or otherwise interfering with contracting relationships between health care providers and companies that do or might furnish them with practice, facility, location, or site management consulting and operational services packages. To the contrary, we propose it in part because we believe it would help some health care provider administrative and operational management services arrangements continue in a form more closely resembling the one they might have taken in the absence of the information blocking

[409] "Practice" used here as defined in § 171.102: an act or omission. This definition includes "by an actor" but applies in this context because the proposed exclusion would turn on the practice management consultant being able to be considered an agent or extension of the provider's own operations.

regulations, as the proposed exclusion would remove an incentive to carve out health IT items and services for separate handling from other items and services an administrative or operational management consultant obtains and manages on behalf of a client health care provider (e.g. an office or clinic's physical space, utilities, payroll processing, medical supplies). Whether styled as "practice management" or "administrative management" or "operations management" or "administration and operations management" services, we believe business arrangements whereby providers obtain these services from consultants or other service firm are meant to allow licensed healthcare professionals to focus more time engaging with patients and delivering patient care that requires their training and license, and less time focusing on business administration and operational management considerations. This would include, where a management consultant offers a comprehensive (sometimes called "turnkey") package of management services, routine administrative oversight and dealings with health IT developers and other health IT offerors on behalf of the client provider.

If practice management consultants become unwilling to include amongst their services those whereby they stand in the shoes of the provider to deal with health IT developers and other health IT offerors, the burden would shift to the provider's staff. Healthcare professionals in small office practices, safety-net clinics, or other lower-resource situations may be unable to afford to keep on staff persons with the necessary skills to ensure their operational items and services are managed effectively. Thus, if dealings with health IT developers were no longer available as part of practice management consulting services packages due to the consultants' concern over being considered "health IT developers of certified health IT," the provider's dealings with IT developers and other health IT offerors would in a variety of small and low-resource provider circumstances tend to shift to the licensed healthcare professional(s). It is not our intent that information blocking regulations increase the need for clinicians and other licensed healthcare professionals in small practices, safety net clinics, or low-resource settings of any type, to directly negotiate with health IT developers or other purveyors of health IT items

and services if or when such licensed healthcare professionals would prefer to engage a practice management firm to deal with health IT vendors along with vendors of all the other goods and services needed to operate an office practice, clinic, or other type of health care provider. Furthermore, we believe tailoring this exclusion to health IT items and services bundled with other items and services mitigates what could otherwise be a risk of non-developer purveyors of health IT items and services attempting simple, pretextual rebranding of their offerings of health IT items and services with the aim of evading accountability while engaging in conduct constituting information blocking as defined in § 171.103.

The key factors that would differentiate excluded clinician practice or other health care provider administrative or operational management consultant services from IT managed service provider (MSP) services and arrangements, as the proposed exclusion is drafted (see (3)(c)), would be:

- The individual or entity furnishing the administrative or operational management consulting services acts as the agent of the provider or otherwise stands in the shoes of the provider in dealings with the health IT developer(s) or commercial vendor(s) from which the health IT the client health care providers ultimately use is obtained.
- The administrative or operational management consulting services must be a package or bundle of services provided by the same individual or entity and under the same contract or other binding instrument, and the package or bundle of services must include a comprehensive array of business administration functions, operations management functions, or a combination of these functions, that would otherwise fall on the clinician practice's or other health care provider's partners, owner(s), or in-house staff.

To be considered "[c]omprehensive and predominantly non-health IT" services, the array of operations and functions the consultant administers[410] as a part of the bundle of business administrative and operational management consulting services must include multiple items and services that are ***not*** health information technology as defined in 42 U.S.C. 300jj(5). Additionally, non-health IT services must represent more than half of each of the following:

- the person hours per year the consultant bills or otherwise applies to the services bundle (including cost allocations consistent with Generally Accepted Accounting Principles), and
- the total cost to the client for, or billing from, the consultant per year (including pass-through costs for the health IT items and services).

Non-health IT services we have observed practice/operations management consultants offering to administer on behalf of health care providers include credentialing or contracting, medical supplies & equipment purchasing and leasing, staffing (also called human resources) management, and location or facility services. An arrangement where the health IT items and services that are passed through the consultant to the end-user health care provider[411] represent more than half of consultant person hours billed or otherwise attributed to services bundle, total dollar cost, or billing, from consultant to client for the bundle per year, or any combination thereof, would not be considered to be "comprehensive and composed predominantly of non-health IT items and services."

Similar to the other two potential exclusions proposed for legal and consulting services, this exclusion focuses on specific services that would be construed as outside the proposed definition of what it means to *offer health IT.* However, if the entity otherwise met the definition of health IT developer of certified health IT, then it would be considered a health IT developer of

[410] In context of this discussion, we use "administer" in a broad sense that includes managing, supervising, or managing and supervising.
[411] For example, but not limited to, a clinician office practice.

certified health IT regardless of whether it met this exclusion from the definition of offers health IT.

Thus, for one example, an individual or entity that enables client individuals or entities to obtain use of health IT exclusively through arrangements fitting this exclusion would avoid being considered a *health IT developer of certified health IT.* However, we offer the following example to illustrate a situation where the entity *would* be considered a *health IT developer of certified health IT*. A single entity has multiple lines of business. Under one business line, the entity furnishes management consulting services to some customers that are predominantly non-health IT services and include the management of health IT. Under another business line, the same entity also licenses certified health IT but does not provide management consulting services, or provides only limited or incidental management consulting services in complement to the health IT offered. We assume for purposes of this example that the business line that furnishes management consulting services falls within our proposed exclusion under (3)(c). However, the business line that licenses certified health IT would meet the definition of "offers health IT" and would not meet any exclusions from the definition. Since the business line meets the licensing of certified health IT definition of "offers health IT," the entity would be considered a health IT developer of certified health IT. And since we have previously stated that once an entity meets the definition of health IT developer of certified health IT that definition will apply to all practices of the entity, the entity will be considered a health IT developer of certified health IT for all practices, including the management consulting services. If an entity engages in conduct that meets the definition of "offers health IT," and some but not all of the conduct is excluded from the definition of "offers health IT," the entity will meet the definition of "offers health IT" and, therefore, meet the definition of health IT developer of certified health IT across all of its health IT and all of its business lines. Thus, any exclusion would have effect only for those individuals and entities that do not at any time engage in any activities that meet the *offer health IT* definition or develop certified health IT. Thus, developers who participate in the

Program and for commercial vendors of health IT, any exclusions from the definition of offer would be inapplicable.

We solicit comment on this proposal, specifically including comment on whether:

- this exclusion is more beneficial than harmful or confusing to the public, including the regulated community (health care providers, other information blocking "actors," and those who may be more likely to be considered a "health IT developer of certified health IT" in the absence of this exclusion); and
- different or additional criteria should factor into differentiating whether a particular arrangement is a practice/operational management services arrangement that happens to include health IT as one of many necessities to operate as a health care provider rather than an arrangement for supply of health IT that happens to include additional services.

2. Health IT Developer of Certified Health IT: Self-developer Health Care Providers

Currently, for reasons discussed in the ONC Cures Act Proposed (84 FR 7511 to 7512) and Final (85 FR 25799 to 25800) Rules, health care providers who self-develop certified health IT ***for their own use*** are excluded from the "health IT developer of certified health IT" definition. However, if a health care provider responsible for the certification status of any Health IT Module(s) were to offer or supply those Health IT Module(s), separately or integrated into a larger product or software suite, to other entities for those entities' use in their own independent operations, that would be inconsistent with the concept of the health care provider self-developing health IT for its own use.

In our experience, self-developers continue to comprise a very tiny segment of the health IT developer of certified health IT population. However, we do not have optimal visibility of the extent to which self-developer health care providers may be providing their self-developed certified health IT to other health care providers—particularly those who, like skilled nursing facilities and other long term/post-acute care (LTPAC) providers, are not eligible to participate in

any CMS programs that specifically track use of Certified EHR Technology (CEHRT)—on any terms.

To date, we have received no questions, concerns, or other feedback specific to treating, for purposes of information blocking, self-developer health care providers who offer or supply to others their self-developed certified health IT the same as we would any developer of certified health IT.

However, we believe it is appropriate to revisit the *health IT developer of certified health IT* definition in § 171.102 in light of the proposed new definition of what it means to *offer* certified health IT, to ensure it remains clear on the face of the definition when health care providers who self-develop certified health IT remain outside the definition of *health IT developer of certified health IT* and when they would fall within that definition.

Should we finalize the *offer health information technology* or *offer health IT* definition to include the exclusion in (1) of certain donation and subsidized supply arrangements, a self-developer health care provider that makes funding or cost coverage subsidies available to others consistent with the finalized (1) exclusion would stand on the same footing as any other health care providers who supply funding or cost coverage subsidies for certified health IT. We have not proposed to except self-developer health care providers from this exclusion. The provision of funding or cost coverage subsidies consistent with the (1) exclusion from the *offer health information technology* or *offer health IT* definition would ***not*** cause the self-developer health care provider to be considered a *health IT developer of certified health IT* under our proposed revision to the definition in § 171.102.

To ensure it is immediately clear from the face of the regulations' text that we had put all health care providers that engage in other activities consistent with exclusions (1) through (3) from the *offer health information technology* or *offer health IT* definition on the same footing regardless of who develops the health IT involved in these activities, we would revise the *health IT developer of certified health IT* definition in § 171.102. Specifically, we propose to replace

"other than a health care provider that self-develops health IT for its own use" with "other than a health care provider that self-develops health IT not offered to others." We have proposed this updated definition in the draft regulation text section of this rule to reflect this proposed change.

We note that regardless of whether we finalize this proposed change to the *health IT developer of certified health IT* definition, a health care provider that self-develops certified health IT and that *offers health IT* to others under any arrangements would continue to be considered a health IT developer of certified health IT (as such developers have been since the ONC Cures Act Final Rule became effective in 2020).

3. Information Blocking Definition

As finalized in the ONC Cures Act Final Rule (85 FR 25642) and the Cures Act Interim Final Rule (85 FR 70085), the definition of information blocking (§ 171.103) and the Content and Manner Exception (§ 171.301(a)) were limited to a subset of EHI that was narrower than the EHI definition ONC finalized in the ONC Cures Act Final Rule in § 171.102. The narrower subset included only the EHI identified by the data elements represented in the United States Core Data for Interoperability (USCDI) for the first 18 months after the applicability date for 45 CFR part 171 (85 FR 25792). The interim final rule extended the date to October 6, 2022 (85 FR 70069).

Because October 6, 2022, has passed, we propose to revise § 171.103 (information blocking definition) to remove § 171.103(b), which designates the period of time for which the information blocking definition is limited to EHI that consists of the data elements represented in the USCDI. Similarly, because we included the same date in two paragraphs of the Content and Manner exception (§ 171.301(a)(1) and (2)), we propose to revise § 171.301 to remove the existing § 171.301(a)(1) and (2) as no longer necessary. The proposed revised version of § 171.301 refers simply to EHI as defined in § 171.102. We further propose to renumber several of the existing provisions in § 171.301 accordingly; and rename the exception as the "Manner" exception.

B. Exceptions

1. Infeasibility

a. Infeasibility Exception – Uncontrollable Events Condition

In § 171.204, we created an exception under which an actor's practice of not fulfilling a request to access, exchange, or use EHI "due to" the infeasibility of the request would not be considered information blocking. In the preamble of the ONC Cures Act Final Rule (85 FR 25867), we specified that there may be situations when complying with a request for access, exchange, or use of EHI would be considered infeasible because an actor is unable to provide such access, exchange, or use due to unforeseeable or unavoidable circumstances outside the actor's control. We recited our proposals from the ONC Cures Act Proposed Rule, which noted that, as examples, an actor could seek coverage under the Infeasibility Exception if it was unable to provide access, exchange, or use of EHI due to a natural disaster (such as a hurricane, tornado, or earthquake) or war. Importantly, we noted that the actor would need to produce evidence and ultimately prove that complying with the request for access, exchange, or use of EHI in the manner requested would have imposed a clearly unreasonable burden on the actor under the circumstances (85 FR 25866). As part of revisions to add clarity to the Infeasibility Exception in the ONC Cures Act Final Rule, we established the "standalone" *uncontrollable events* condition of the Infeasibility Exception in § 171.204(a)(1). Under the uncontrollable events condition, an actor's practice of not fulfilling a request to access, exchange, or use EHI as a result of a natural or human-made disaster, public health emergency, public safety, incident war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority (§ 171.204(a)(1); 85 FR 25874) will not be considered information blocking provided such practice also meets the condition in § 171.204(b).

The fact that an uncontrollable event specified in § 171.204(a)(1) occurred is not a sufficient basis alone for an actor to meet the uncontrollable events condition of the Infeasibility Exception. Rather, the use of the words "due to" in the condition was intended to convey,

consistent with the ONC Cures Act Proposed Rule, and does convey that the actor must demonstrate a causal connection between not providing access, exchange, or use of EHI and the uncontrollable event. To illustrate, a public health emergency is listed as an uncontrollable event under § 171.204(a)(1). If the Federal Government or a state government were to declare a public health emergency, the mere fact of that declaration would not suffice for an actor to meet the condition. To meet the condition, the actor would need to demonstrate that the public health emergency actually caused the actor to be unable to provide access, exchange, or use of EHI for the facts and circumstances in question. The emergency need not be the *only* cause of a particular incapacity, but the actor needs to demonstrate that the public health emergency did in fact negatively impact the feasibility of that actor fulfilling access, exchange, or use in the specific circumstances where the actor is claiming infeasibility. While this condition has always required causal connection between the actor's inability to fulfill the request and the natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority, we propose to revise the condition by replacing the words "due to" with "because of." This revision may provide additional clarity, but we welcome comments on this proposal, including whether alternative or additional refinements to the wording of the condition may make the causal connection requirement more immediately obvious from the face of the text in § 171.204(a)(1).

b. Third Party Seeking Modification Use

We propose to renumber the Infeasibility Exception's (45 CFR 171.204) "infeasible under the circumstances" condition from paragraph (a)(3) to paragraph (a)(5) and to codify at (a)(3) a new condition "*third party seeking modification use*." We propose, as discussed in section IV.B.1.c below, another new condition that would be codified as paragraph (a)(4) of § 171.204.

The proposed § 171.204(a)(3) *third party seeking modification use* condition would apply in certain situations where the actor is asked to provide the ability for a third party (or its technology, such as an application) to modify EHI that is maintained by or for an entity that has deployed health information technology as defined in § 170.102 and maintains within or through use of that technology any instance(s) of any electronic health information as defined in § 171.102. Specifically, we propose that the *third party seeking modification use* condition of the infeasibility exception would be limited to situations when "[t]he request is to enable use of EHI in order to modify EHI (including but not limited to creation and deletion functionality), provided the request is **not** from a health care provider requesting such use from an actor that is its business associate" (proposed new § 171.204(a)(3), emphasis added).

In § 171.102, we define "use" for purposes of the information blocking definition to mean "the ability for electronic health information, once accessed or exchanged, to be understood and acted upon." We stated in the ONC Cures Act Final Rule that "acted upon" within the final "use" definition "encompasses the ability to read, write, modify, manipulate, or apply the information…." (85 FR 25806). Therefore, in § 171.204(a)(3), we propose to use the term "*third party seeking modification use*" to describe a set of requirements that must be satisfied in order for an actor's practice of interfering with another's *use* of EHI to meet the new proposed condition of the Infeasibility Exception. In particular, this new proposed condition focuses on requests to create and delete EHI held by or for a health care provider.

While the information blocking definition refers to the "access, exchange, or use" of electronic health information, in this portion of the preamble we will instead use the term "modify" or "modification use" to describe the particular type of "use" covered by this new condition. We do so in order to avoid confusion between this "modification use" and the HIPAA Rules' defined term "use" (45 CFR 160.103). The *third party seeking modification use* condition does not imply or indicate any change to any HIPAA Rules' definition, nor to the HIPAA Rules.

We propose this new condition to reduce actor burden and uncertainty by creating a condition whereby practices specific to declining *certain* requests for third party modification use of EHI held by or for a health care provider could be excepted from information blocking more efficiently than might be the case under other conditions in § 171.204(a) or other exceptions. For example, the condition could reduce the burden on actors to document each modification use request the same way that an actor would need to document its actions for the "infeasible under the circumstances" condition of the Infeasibility Exception (§ 171.204(a)(3)). The condition could also reduce an actor's burden to determine if another exception applies to the request, such as the Preventing Harm Exception (45 CFR 171.201) or the Security Exception (45 CFR 171.203). Of course, other exceptions, including other conditions of the Infeasibility Exception itself, may still apply under the circumstances of any particular request and always remain available for consideration by the actor. We simply note that it may be less burdensome for an actor to determine that this condition applies to one or more of its practices as compared to other exceptions. Below, we provide examples of when this condition could be used, and also when it would not be applicable but other conditions or exceptions might still apply.

To illustrate the purpose of this proposed condition, an actor may be concerned about the accuracy or reliability of data that a third party would like to add to an individual's designated record set maintained by the actor. Rather than spending resources determining if the Preventing Harm (§ 171.201) or Security (§ 171.203) Exceptions apply, or to consider all of the factors required to determine that a request may be infeasible under the circumstances (currently § 171.204(a)(3), proposed to be renumbered to § 171.204(a)(5)), an actor may be able to make use of the "modification use" condition, if finalized as proposed. More specifically for this example, an actor may be unable to complete a third party's request to modify or add EHI in the specific way that it was requested. Rather than working through all of the alternative manners (and then possibly even ending up using the proposed new "manner exception exhausted" condition of the infeasibility exception), the actor can use the *third party seeking modification*

use condition without needing to engage in information gathering or analysis that would often be needed to work through the available alternative manners. In other cases, an actor may have concerns that a third party seeking "modification use" of EHI could, through that use, pose specific threats to the confidentiality, integrity, or availability of data on its system. Rather than establishing that the practice meets the Security Exception, which requires a written policy or case-by-case determinations tailored to the specific security risk, an actor may find it more efficient to satisfy the Infeasibility Exception through the proposed new *third party seeking modification use* condition (in complement to the Infeasibility Exception's existing requirements in § 171.204(b)).

The *third party seeking modification use* condition of the Infeasibility Exception would be available to most actors to address situations where a third party's request is to modify EHI (including but not limited to creation and deletion functionality) stored or maintained by an actor. For reasons explained below, this proposed condition would not be available to an actor when the actor is a business associate of the health care provider who is making the modification use request (directly, or through another business associate of the health care provider). We emphasize that although this proposed condition of the Infeasibility Exception would not be available under these specific circumstances, other conditions within § 171.204(a) and all of the other exceptions would remain available for consideration by the actor as to their applicability to the situation and request. Moreover, we note that nothing in the information blocking regulations requires an actor to permit access, exchange, or use of EHI when such access, exchange, or use is prohibited by law.

We propose to exclude from applicability of this new condition requests from health care providers to their business associates where these business associates are other actors, such as health IT developers of certified health IT or HINs/HIEs, because the exceptions to the information blocking definition are intended to only cover reasonable and necessary practices of interference that would otherwise constitute information blocking. Covered entities (health care

providers) and their business associates (as permitted by their business associate agreement) need to access and modify relevant EHI held by other business associates of those covered entities on a regular basis. Ensuring that this condition does not apply to practices of one business associate/actor that are likely to interfere with health care providers' and their other business associates' ability to access, exchange, and use (including through modification use) EHI maintained by or for the health care provider promotes greater interoperability, efficient transitions of care, and protects the use of EHI as needed to maintain operations. In addition, there is often a level of trust and contractual protections between covered entities and business associates that removes some of the other concerns, such as security and data provenance, that led us to propose this new condition for the specific circumstances when it *would* be applicable. Further, many concerns were expressed by health care providers and their business associates to ONC in development of the Information Blocking Report to Congress and the ONC Cures Act Proposed Rule that certain business associates that were also actors under the information blocking regulations were committing interferences with access, exchange, and use of EHI (see examples of likely interferences by EHR developers at 84 FR 7518-19). We again note and emphasize that other Federal or State law may apply, and that other information blocking exceptions or conditions of the Infeasibility Exception are available and may apply to these relationships and requests for EHI access, exchange, and use.

Because this new proposed *third party seeking modification use* condition is not available when the request is from a health care provider requesting (directly, or through another business associate of the health care provider) such modification use from an actor that is its business associate, we propose to add the definition of "business associate" to § 171.102, and propose that the definition of "business associate" be the same as the definition of "business associate" found in the HIPAA regulations at 45 CFR 160.103. One example where the *third party seeking modification use* would not apply is when the developer of a health care provider's clinical support decision software requests to modify EHI within the provider's EHR system, which is

maintained by another business associate of the health care provider. In this example, the developer and the entity that maintains the provider's EHR system are both business associates of the health care provider. Because both parties are business associates of the same health care provider, *this* condition of the Infeasibility exception is not available to the business associate who maintains the EHR system for the reasons discussed above. Although the *third party modification use* condition is not available, other conditions and other exceptions are available and may apply. Whether information blocking has occurred depends on the specific facts and circumstances of the situation.

To provide additional clarity regarding circumstances that would *not* fall under this proposed condition but for which potentially another exception could apply, we provide the following example. A health IT developer of certified health IT (actor) who is a business associate of a health care provider who is a covered entity (and actor) and maintains the EHR on behalf of the health care provider could receive a modification use request from a third party who is also a business associate of the health care provider. The modification use request may be non-standardized or incompatible with the EHR technology, as well as require extensive technical and financial resource allocations by the health IT developer of certified health IT. At this point, though the *third party modification use* condition would not be available, the health IT developer of certified health IT could consider whether the new proposed "manner exception exhausted" condition (proposed § 171.204(a)(4)) or the "infeasibility under the circumstances" condition of the Infeasibility Exception are applicable to the situation. We remind all actors that all of the other relevant conditions of the Infeasibility Exception must also be met where the decision is made to rely upon the Infeasibility Exception. In addition, all of the other exceptions codified at 45 CFR part 171 remain available for consideration of their applicability to an actor's practices and specific circumstances.

We request comment generally on this new proposed condition and, if this condition were finalized, whether this condition should be of limited duration. More specifically, we

request comment on whether ONC should consider proposing, in the future, that the condition be eliminated if, at some point, health information technology is capable of supporting third-party modification use of EHI by *any* party with a legal right to do so (or no legal prohibition against it), with no or minimal infeasibility or other concerns.

As with every other condition in § 171.204(a), the proposed § 171.204(a)(3) *third party modification use* condition would stand alone. This means an actor's practice could meet it without needing to meet any other § 171.204(a) condition. It also means an actor's practice that fails to meet the § 171.204(a)(3) *third party modification use* condition could nevertheless satisfy another of the conditions, such as the *infeasible under the circumstances* condition (currently § 171.204(a)(3), proposed to be renumbered to § 171.204(a)(5)).

c. Manner Exception Exhausted

We propose to renumber the Infeasibility Exception's (45 CFR 171.204) "*infeasible under the circumstances*" condition from paragraph (a)(3) to paragraph (a)(5) and to codify at (a)(4) a new "*manner exception exhausted*" condition. The proposed *manner exception exhausted* condition would apply where an actor is unable to fulfill a request for access, exchange, or use of EHI despite having exhausted the Content and Manner Exception in § 171.301 (which we have proposed elsewhere in this proposed rule to rename the Manner Exception), including offering all alternative manners in accordance with § 171.301(b), so long as the actor does not currently provide to a substantial number of individuals or entities similarly situated to the requestor the same requested access, exchange, or use of the requested EHI.

In the ONC Cures Act Proposed Rule, we proposed an exception that would apply where an actor's practice of not fulfilling a request to access, exchange, or use EHI in a manner that is infeasible in the particular circumstances would not be considered information blocking, subject to a duty to provide a reasonable alternative (84 FR 7542). We noted that "in certain circumstances legitimate practical challenges beyond an actor's control may limit its ability to comply with requests for access, exchange, or use" (84 FR 7542). We explained that sometimes

those challenges may be related to, for example, technological capabilities. In other cases, however, we noted "the actor may be able to comply with the request, but only by incurring costs or other burdens that are clearly unreasonable under the circumstances" (84 FR 7542). Without such an exception, we noted that inefficiencies could be introduced such that, for example, "the actor may be able, but reluctant, to offer alternative means that would meet the requestor's needs while reducing the burden on the actor, leading to more efficient outcomes overall" (84 FR 7542). To safeguard the exception from inappropriate use, we proposed a two-step test that an actor would need to satisfy in order to meet the exception: first, that complying with the request would impose a substantial burden on the actor, and second, that the burden imposed would be plainly unreasonable under the circumstances (84 FR 7542-43).

In the ONC Cures Act Final Rule (85 FR 25642) we finalized a modified Infeasibility Exception to address concerns raised by commenters (*see* 85 FR 25866 through 25870). We eliminated the two-factor test in favor of three conditions that more specifically address situations where the Infeasibility Exception would be appropriately used. One of the conditions we finalized, *infeasible under the circumstances*, requires the actor to demonstrate, through a contemporaneous written record or other documentation, its consideration, in a consistent and non-discriminatory manner, of certain factors that led to its determination that complying with the request would be infeasible under the circumstances.

As discussed in the ONC Cures Act Final Rule (at 85 FR 25869 through 25870) rather than finalize the proposed requirement to provide a reasonable alternative in order for an actor's practice to satisfy the *infeasible under the circumstances* condition (45 CFR 171.204(a)(3)) of the Infeasibility Exception), we finalized at 45 CFR 171.301 the "Content and Manner Exception," which we propose in this current rule to rename and will therefore reference here as the "Manner Exception" (discussion of proposed updates to § 171.301 is in section IV.B.2, below). Under § 171.301, in order for the Manner Exception to apply, an actor must fulfill a request for access, exchange, or use of EHI in any manner requested, unless the actor is

technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request (45 CFR 171.301(b)(1)(i), as originally codified). If an actor and requestor reach agreeable terms and the actor fulfills a request described in the manner condition in any manner requested: (1) Any fees charged by the actor in relation to its response are not required to satisfy the Fees Exception in § 171.302; and (2) any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the Licensing Exception in § 171.303 (45 CFR 171.301(b)(1)(ii)) (85 FR 25877). Section 171.301(b)(2) (original codification) provides requirements for fulfilling a request to access, exchange, or use EHI in a manner other than the manner requested. If an actor does not fulfill a request in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request, the actor must fulfill the request in an alternative manner agreed upon with the requestor consistent with § 171.301(b)(2) (original codification) in order to satisfy the exception (85 FR 25877). The Manner Exception, therefore, offers certainty that an actor's practices that fully satisfy the Manner Exception's conditions will not be considered information blocking, which is meant to incentivize offering an alternative manner (with priority to interoperable manners based on HHS-adopted and available open standards) when the actor is unable to fulfill access, exchange, or use of the requested EHI in the manner initially requested.

The Infeasibility Exception, as finalized in the ONC Cures Act Final Rule, provides assurance to an actor that if it meets certain conditions of the exception at all relevant times, its practice will not be considered information blocking. We finalized most but not all of the factors we proposed in the ONC Cures Act Proposed Rule for *infeasible under the circumstances* (originally codified in § 171.204(a)(3)). Two of the factors we did *not* finalize for *infeasible under the circumstances* were whether the requestor and other relevant persons can reasonably access, exchange, or use the EHI from other sources or through other means; and the additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use (85 FR 25868). We explained that we did so because we moved away

from a relative burden analysis, and also because "consideration does not have to be given as to whether other means are available for access, exchange, or use of EHI or the cost to the requestor for that alternative means because of the new Content and Manner Exception (§ 171.301) and its relationship to this exception" (85 FR 25868).

We propose to renumber the *infeasible under the circumstances* condition and revise it by adding the new *manner exception exhausted* condition that would align with and advance the policy goal of fostering the use of standards-based interoperability in achieving access, exchange, and use of EHI. We have received feedback that actors are uncertain as to whether they have satisfied the *infeasible under the circumstances* condition in instances where they believe that fulfilling a request for access, exchange, or use of EHI is infeasible. Specifically, actors have expressed concern about circumstances where the actor's inability to satisfy the Manner Exception's conditions rests solely on the requestor refusing to accept access, exchange, or use in *any* manner consistent with § 171.301 and fulfilling the request in the manner requested would require substantial technical or financial resources, or both, in the view of the actor, including significant opportunity costs. We have observed this being more of a concern for actors with significant skills and other resources for developing unique technical solutions or new technological capabilities (e.g., EHR developers or HIN/HIEs) than for information blocking actors with few to no such resources (e.g., small clinician office practices or safety net clinics).

Amongst those actors with substantial skills and other resources to develop new, unique or unusual manners of supporting access, exchange, or use of EHI, we see actors who appear to be experiencing a problematic level of uncertainty about whether they will be engaging in information blocking if they decline demands from requestors for non-standard, non-scalable, solutions that they do not currently support *even after* they have offered to provide access, exchange, or use of EHI in the same manner(s) the actor makes generally available to its customers or affiliates, *and* through other standards-based manners, consistent with § 171.301—

including offering terms for such manners that are consistent with the Fees (§ 171.302) and Licensing (§ 171.303) Exceptions. We anticipate that this uncertainty will lead actors who, again, have already exhausted the Manner Exception (§ 171.301), to divert their development capacity to fulfilling requested manners of access, exchange, or use of EHI that they *could* invent to meet the demands of a requestor determined to accept only the original manner they specified and who are unwilling or unable to agree to terms consistent with the Fees (§ 171.302) and Licensing (§ 171.303) Exceptions for their requested manner or any alternative manner consistent with the Manner Exception (§ 171.301).

Therefore, this new condition is necessary to ensure actors reasonably allocate resources toward interoperable, standards-based manners rather than allowing requestors who, for whatever reason, do not build their products for compatibility with open consensus standards or other industry standards to attempt to force use of non-standard, non-scalable solutions by simply refusing to accept access, exchange, or use of EHI in any other manner. This diversion of resources away from standards-based, scalable manners of exchange detracts from, instead of supporting, achievement of key policy goals such as increased interoperability and innovation in use of open consensus standards to achieve secure, seamless exchange. Where novel approaches to system interfaces or other aspects of access, exchange, or use of EHI represent improvements over other available approaches, we anticipate these approaches will not need to be forced upon the industry but will instead find a natural foothold and diffuse according to a normal innovation curve.

To illustrate the situation we see and believe this new condition is necessary to remediate: an actor that develops or offers certified health IT may, for example, be uncertain as to whether an information blocking exception covers its practice of denying a requestor's demand for access, exchange, or use in a particular manner that relies on unique specifications instead of "interoperable standards" (for example, standards identified in 45 CFR 171.301(b)(2)(i)(B) and also specified below) because the actor has capabilities and resources that it *could* potentially

divert to the requestor's preferred manner. In such cases, the actor may also lose the opportunity to pursue other innovative endeavors or fulfill other customer requests. Health care provider and HIN/HIE actors with substantial technical and other resources also face demands from requestors who are interested only in their own preferred mechanisms, however unique and non-scalable. We are concerned that actors currently appear to experience such uncertainty even if, to continue this illustration, the actor is offering the requestor interoperable manners of access, exchange, or use based on open, consensus-based industry standards and diverting resources to build the new manner would mean the actor would need to delay for months or more deployment of innovations that will reduce burden on clinicians using the software. In these cases, we currently cannot advise these actors whether or not the requestor's demand is infeasible in the actor's unique circumstances. Thus, in this example, the actor concerned about this uncertainty diverts resources for innovation and development to requestors' unique, non-scalable builds at the expense of the actor investing in innovations and upgrades to better meet the needs of its users.

It is not our intent that the information blocking regulations drive actors to prioritize various requestors' non-standardized, non-scalable preferences for manners of achieving access, exchange, or use of EHI over directing the actors' development resources to developing and implementing scalable, interoperable solutions to meet patients' and health care providers' needs. Consistent with policy goals for advancing secure, interoperable access, exchange, and use of EHI, we would rather encourage use of standards-based and other generally available mechanisms whenever available to serve the access, exchange, or use need so that as many development resources as possible remain available to actors to focus on continuously improving generally available products' capabilities. The proposed new *manner exception exhausted* condition is intended to ensure information blocking regulations are not easily used to force actors to inefficiently allocate resources on non-standard, non-scaling manners of access, exchange, and use of EHI due to uncertainty about whether HHS expects them to develop any or every access, exchange, or use mechanism that might be feasible for an actor.

The proposed § 171.204(a)(4) *manner exception exhausted* condition provides actors the option of satisfying the Infeasibility Exception without needing to assess whether they *could* theoretically or technically meet the requestor's particularized demands regarding the manner and/or terms in which they want to achieve access, exchange, or use of requested EHI. In other words, the *manner exception exhausted* condition covers an actor's reasonable and necessary practice of prioritizing resources in favor of interoperable technology. To satisfy § 171.204(a)(4) *manner exception exhausted*, an actor would be considered "unable" to fulfill a request for access, exchange, or use of electronic health information when three factors are true:

(i) The actor could not reach agreement with a requestor in accordance with § 171.301(a) *manner requested* condition (as we have proposed it in this proposed rule) or was technically unable to fulfill a request for electronic health information in the manner requested;

(ii) The actor offered all alternative manners in accordance with § 171.301(b) *alternative manner* condition (as we have proposed it in this proposed rule) for the electronic health information requested but could not reach agreement with the requestor; and

(iii) The actor does not provide the same access, exchange, or use of the requested electronic health information to a substantial number of individuals or entities that are similarly situated to the requester.

As is the case for a practice satisfying any of the conditions codified in § 171.204(a), an actor's practice satisfying the § 171.204(a)(4) *manner exception exhausted* condition would also need to meet the requirements of § 171.204(b) *responding to requests* in order for that practice to be covered by the Infeasibility Exception. However, as is also the case for each of the other conditions codified in other subparagraphs of § 171.204(a), the Infeasibility Exception could be satisfied *regardless* of whether the actor's practice also satisfied one or more of the other conditions in § 171.204(a). Thus, where an actor's practice satisfies § 171.204(a)(4) *manner exception exhausted*, the actor does **not** need to demonstrate consideration of the factors

specified in the *infeasible under the circumstances* condition (original codified in § 171.204(a)(3), proposed to be renumbered to § 171.204(a)(5)) in order for that practice to be covered by the Infeasibility Exception.

By creating an infeasibility condition that can be met without the actor needing to demonstrate they considered the resources available to the actor, we believe we would accomplish the objective of assuring actors who do not want to develop one-off solution(s) that where the requestor is unwilling to accept an alternative manner of access, exchange, or use of the requested EHI consistent with the § 171.301(b) *alternative manner* condition, denying such requests will not be considered "information blocking" (as defined in § 171.103) so long as the actor's practice satisfies the § 171.204(a)(4) *manner exhausted* and § 171.204(b) *responding to requests* conditions of the Infeasibility Exception, ensuring that the actor's practice of "interfering" with the custom-build requests is both reasonable and necessary.

The second factor within the proposed § 171.204(a)(4) *manner exception exhausted* condition would require the actor to offer "all alternative manners in accordance with § 171.301(b) for the electronic health information requested." We believe it is important that the Manner Exception **not** be considered exhausted if the actor offers only one alternative manner, or only the least-interoperable "alternative machine-readable format" that would be codified in proposed § 171.301(b)(1)(iii) (presently codified in § 171.301(b)(2)(i)(C)). We also want to mitigate the risk of the proposed *manner exception exhausted* condition reducing actors' incentive to expand their capabilities to support access, exchange, or use of EHI. That is why we have not proposed that an actor need only have offered the alternative manners in accordance with § 171.301(b) that the actor has implemented for the electronic health information requested. However, we recognize that some actors, notably including health care providers ineligible to participate in the Medicare Promoting Interoperability (PI) Program or Merit-based Incentive Payment System (MIPS) Promoting Interoperability performance category, may not have technology certified to standards adopted in 45 CFR part 170. We are considering, and propose

in the alternative to the factor as detailed above (and in proposed § 171.204(a)(4)(i)), that the second of three factors that must be true to satisfy § 171.204(a)(4) *manner exception exhausted* condition would instead be that the actor offered at least two (or at least three) alternative manners in accordance with § 171.301(b), at least one of which was consistent with § 171.301(b)(1)(i) or (ii), for the EHI requested but could not reach agreement with the requestor. This alternative factor would offer actors with certified health IT the option of offering as few as two alternative manners that each make use of content and transport standards published by the Federal Government or a standards-developing organization accredited by the American National Standards Institute, or one such manner plus an alternative machine-readable format consistent with § 171.301(b)(1)(iii). This alternative version of the factor would also provide a clear option for an actor **without** certified health IT to satisfy the § 171.204(a)(4) *manner exception exhausted* condition either:

- by offering to fulfill the request in two manners that use content and transport standards published by the Federal Government or a standards-developing organization accredited by the American National Standards Institute; or
- by offering fulfilment in at least one such manner *and* an alternative machine-readable format consistent with § 171.301(b)(1)(iii).

In seeking comment on the proposed new § 171.204(a)(4) *manner exception exhausted* condition, we seek comment specifically on whether commenters expect the needs of patients, health care providers, and the advancement of interoperability, EHI exchange, and/or health IT innovation would be better served by the factor proposed in § 171.204(a)(4)(ii), requiring the actor have offered *all* alternative manners consistent with § 171.301(b)(1), *or* by simply requiring that the actors offer only two or three alternative manners so long as at least one of those manners used either certified technology consistent with § 171.301(b)(1)(i) or used content and transport standards consistent with § 171.301(b)(1)(ii) in order for the request to meet this condition. We note that an actor whose practices cannot meet § 171.204(a)(4) *manner exception*

exhausted condition could consider aligning their practices to satisfy the § 171.204(a)(5) *infeasible under the circumstances* condition instead. We also specifically request comment as to whether this alternative approach could lead to less incentive to adopt certified health IT.

The third factor within the proposed § 171.204(a)(4) *manner exception exhausted* condition (§ 171.204(a)(4)(iii)) is that the actor does not provide the same access, exchange, or use of the requested electronic health information to a substantial number of individuals or entities that are similarly situated to the requester. There are several features of this proposed factor to which we wish to call attention. First, we note that this factor as a whole serves a similar function to the § 171.204(a)(5) (originally codified in § 171.204(a)(3)) *infeasible under the circumstances* condition's factor considering whether the actor's practice is non-discriminatory, and the actor provides the same access, exchange, or use of electronic health information to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship. To note, we discussed the rationale for and functions of this factor of the *infeasible under the circumstances* condition in the ONC Cures Act Proposed Rule preamble beginning at 84 FR 7544 and in the ONC Cures Act Final Rule preamble beginning at 85 FR 25888.

The intent of the § 171.204(a)(4)(iii) factor is to provide a basic assurance that actors would not be able to misuse the § 171.204(a)(4) *manner exception exhausted* condition to avoid supplying some particular requestor(s) with manner(s) of access, exchange, or use of the requested EHI that would be more accurately characterized as generally available than as new, unique, or unusual. This factor ensures this condition cannot be satisfied by, for example, an actor simply choosing not to offer any requestor a general availability manner of access, exchange, or use of the requested EHI. The proposed regulatory language (a substantial number of individuals or entities that are similarly situated to the requester), while on its face may seem indefinite and *is* designed to address *any* potential request, is intended to ensure that the actor offers any requestor (individual or entity) the same access the actor provides to a substantial

number of its customers, preferred customers, owned or affiliated companies, or other non-competitors. We choose to structure the factor in this way to align with the concept of whether the manner requested (including involved interoperability elements) is in a stage of development or overall lifecycle that would roughly approximate the "general availability" phase of the software release lifecycle, or a conceptually analogous phase for non-software interoperability elements.[412] However, we do not propose to incorporate the terms "generally available" or "general availability" into the condition because we intend that this condition of the § 171.204 Infeasibility Exception to be available for all types of information blocking actors, and not only those who develop or market software products. For example, health care providers do not typically develop software for the market and in our observation are likely to characterize components of their health IT systems in more operational terms—such as what has "gone live" in their particular implementation—than in software release lifecycle terms. We believe avoiding the specific lifecycle term also avoids potential for misunderstandings among actors and requestors, or for gamesmanship on the part of actors, around when different actors consider a particular interoperability element to enter or to be withdrawn from "general availability" as the term is widely used in the software sector. However, we emphasize that our use of "provides" in the present tense is both precise and deliberative. This § 171.204(a)(4)(iii) factor tests for whether the actor *currently* provides the same manner to a substantial number of individuals or entities who are similarly situated to any given requestor. Looking only at what the actor currently provides excludes manners that are nearing or have exceeded the end of their supported life cycles. For example, using software release lifecycle terms for ease of discussion,[413] an actor would not currently "provide" a manner of access, exchange, or use of particular EHI that may once have been generally available but has since been withdrawn from general availability.

---

[412] Additional information about "general availability" in the software lifecycle is available from a variety of online sources such as https://www.techopedia.com/definition/32284/general-availability-ga (last accessed March 16, 2023).

[413] Use of software lifecycle terms does not, we reiterate for emphasis, imply and should not be construed as meaning, that we intend this § 171.204(a)(4) condition to be available only to software developers or only with respect to manners or interoperability elements fairly characterized as "software."

Limiting the condition to a particular manner of access, exchange, or use the actor currently provides also excludes from consideration technologies that the actor may be developing or testing but that are not yet ready for replication. Again, using software terms for ease of discussion, it excludes manners that may in the future become generally available but that are not yet ready to enter the general availability phase of their lifecycle. This factor ensures that the new condition covers only *reasonable* activities that could otherwise constitute information blocking.

The § 171.204(a)(4)(iii) factor is intended to ensure the condition cannot be satisfied where a manner (mechanisms, interoperability elements) is currently supported for a substantial number of individuals or entities but the responding actor wants to deny that mechanism to particular requestor(s) for inappropriate reasons, such as to discriminate against competitors, potential competitors, or those the responding actor may be concerned could use the resultant access, exchange, or use of EHI to furnish, develop, or facilitate development of products or services that could compete with those of the actor. We recognize that such practices are not reasonable and necessary, and therefore should not be covered by an exception to the definition of information blocking. The § 171.204(a)(4)(iii) factor is limited to actors providing the same manner of access, exchange, or use of the same EHI to a "substantial number" rather than a specific number to recognize variation in actors' operational contexts, including their organizational sizes. What may be a trivial number to a large health IT developer of certified health IT might be an important or consequential ("substantial") number for a small HIN/HIE. However, we propose in the alternative that we would, and thus seek comment on whether we should, instead construct the factor with a simple fixed threshold of "more than one," or more than another specific number between 1 and 10. Such fixed threshold would offer more simplicity to actors and potential requestors, while still assuring that an actor's practice would not fail to meet this factor on the basis of a single instance of a particular access, exchange, or use manner. For example, a health IT developer of certified health IT may have a single instance

of a manner deployed that has been custom developed for a customer with highly unique needs, or a health care provider may have a custom interface established with its local public health authority, that would be impractical to replicate for other individuals or entities who may be legally permitted to access, exchange, or use the same EHI. These examples of one-off manners we would not consider to be consistent with the broad concept of general availability, and thus should not cause the actor's practice of declining requests for additional instance(s) of these one-off manners, which might use an interoperability approach that is not based on open consensus standards or be otherwise ill suited to scaling up. In offering any potential fixed number in public comment, we remain concerned, such as for the reasons just described, that a fixed number could be considered arbitrary and not necessarily dispositive under the facts and circumstances. Therefore, we ask commenters suggesting a fixed number to also provide accompanying rationale.

The § 171.204(a)(4)(iii) factor includes whether the requestor is *similarly situated* to others to whom the actor might provide the same requested access, exchange, or use of the requested EHI. The *similarly situated* concept and wording should be familiar to information blocking actors, as we also used it in the Fees (§ 171.302) and Licensing (§ 171.303) Exceptions. It would serve here, as it does there, to indicate that different specific individuals or entities within a class of such individuals or entities who are similarly situated to one another should be treated in a consistent and non-discriminatory manner. For example, several large hospitals (above a certain established size threshold) to whom a technology or service is supplied, or for whom the technology is supported, may be similarly situated to one another, but by contrast a small, independent rural health clinic might be similarly situated to other such clinics and in a very different situation than any hospital (large or otherwise). Within a class of similarly situated entities, however, the intent of this factor is that requestors would not be treated differently based on extraneous factors, such as whether any of them may be competitors of the responding actor or may obtain more of their health IT from the actor's competitors than from the actor.

We remind readers that the intent of this condition, as noted above, is for actors to provide requestors the same access they provide to a substantial number of their customers, preferred customers, owned or affiliated companies, or other non-competitors. In this regard, we request comment on whether we should provide more textual specificity or clarity as to the proposed text "a substantial number of individuals or entities that are similarly situated to the requester." To further illuminate this question, if an actor provides a certain form of EHI access to health care providers, then that same form of EHI access should arguably be made available to individuals baring potential other considerations (e.g., privacy or security concerns). To be clear, it is not our intent for the "individuals or entities that are similarly situated to the requester" criteria of this new proposed condition to be used in a way that differentiates the same access to EHI simply based on the requestor's status, such as individual (e.g., a patient) or entity (e.g., a healthcare system).

We believe this new § 171.204(a)(4) *manner exception exhausted* condition ensures that a reasonable and necessary practice would not be considered information blocking and strikes the proper balance in achieving the information blocking polices and goals for removing barriers to the access, exchange, and use of EHI, advancing interoperability, and promoting innovation and competition. We seek comment on this proposal.

2. Manner Exception – TEFCA Reasonable and Necessary Activities

a. Background

In the ONC Cures Act Proposed Rule (84 FR 7552), we requested comments on whether we should propose, in a future rulemaking, a narrow exception to the information blocking definition for practices that are necessary to comply with the requirements of the Common Agreement. We stated that such an exception may support adoption of the Common Agreement and may encourage other entities to participate in trusted exchange through HINs that enter into the Common Agreement. We discussed that it would do so by providing protection if there are practices that are expressly required by the Common Agreement, or that are necessary to

implement Common Agreement requirements, that might implicate the information blocking definition and would not qualify for another exception. We noted that such an exception would be consistent with the complementary roles of the information blocking provision and other provisions of the Cures Act that support interoperability and enhance the trusted exchange of EHI (including the interoperable network exchange provisions (42 U.S.C. 300jj-11(c)(9)), the definition of interoperability (42 U.S.C. 300jj(9)), and the conditions of certification in 42 U.S.C. 300jj-11(c)(5)(D)). We further noted that we expected that any proposal would be narrowly framed such that contract terms, policies, or other practices that are not strictly necessary to comply with the Common Agreement would not qualify for the exception. Similarly, we expected that any future proposal would provide that an actor could benefit from this exception only if the practice or practices that the actor pursued were no broader than necessary under the circumstances. We commented that these limitations would ensure that the exception would be narrowly tailored to practices that are most likely to promote trusted exchange without unnecessarily impeding access, exchange, or use of EHI.

Comments we received in response to the request for information (RFI) varied. There were generally two overarching themes in the comments. The first theme was that it was premature to establish an exception until TEFCA was finalized. The second theme focused on the need for an exception. A majority of commenters asserted that there should be some form of "safe harbor" for TEFCA participants, while other commenters contended that such an approach was unwarranted and that all actors should be subject to the same information blocking policies and requirements. Overall, comments received in response to the RFI that were in favor of an exception outnumbered those that were not in favor. Some commenters advocating for an exception covering or incentivizing TEFCA participation noted that such an exception would provide certainty and reduce the compliance burden for the market. The HITAC's

recommendation[414] regarding the RFI urged ONC "to consider carefully the enduring demand of the Cures Act to promote information sharing and prohibit information blocking amongst all actors" and expressed a view that a careful balance needed to be struck between encouraging compliance with the information blocking regulations, potentially through the adoption of TEFCA, and the need to investigate information blocking practices and not inadvertently allow "bad actors" to circumvent compliance with the information blocking regulations.

During the development of TEFCA and since the publication of the Common Agreement on January 19, 2022,[415] ONC has continued to receive requests for clarification regarding the potential information blocking implications or interpretations of practices (actions or omissions) that the Common Agreement requires of QHINs, and of Participants or Subparticipants through the Common Agreement's required flow-down provisions in Participant-QHIN or Participant-Subparticipant Agreements (also referred to as Framework Agreements).[416] Interested parties have continued to request that ONC provide certainty that such practices would be considered reasonable and necessary activities that do not constitute information blocking.

b. TEFCA Condition for the "Manner" Exception

We propose to add a TEFCA condition to the proposed revised and renamed Manner Exception, to be codified in 45 CFR 171.301. The new condition, in proposed § 171.301(c), would read as follows: "If an actor who is a QHIN, Participant, or Subparticipant offers to fulfill a request for EHI access, exchange, or use for any permitted purpose under the Common Agreement and Framework Agreement(s) from any other QHIN, Participant, or Subparticipant using Connectivity Services, QHIN Services, or the specified technical services in the applicable Framework Agreement, then: (i) The actor is not required to offer the EHI in any alternative

---

[414] https://www.healthit.gov/sites/default/files/page/2019-07/2019-06-03_All%20FINAL%20HITAC%20NPRM%20Recs_508-signed.pdf

[415] https://www.federalregister.gov/documents/2022/01/19/2022-00948/notice-of-publication-of-the-trusted-exchange-framework-and-common-agreement

[416] *See* Common Agreement Section 1, Definitions and Relevant Terminology, available at https://www.healthit.gov/sites/default/files/page/2022-01/Common_Agreement_for_Nationwide_Health_Information_Interoperability_Version_1.pdf (accessed March 16, 2023)

manner; (ii) Any fees charged by the actor in relation to fulfilling the request are not required to satisfy the exception in § 171.302; and (iii) Any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the exception in § 171.303."

This proposal aligns with a foundational policy construct underpinning the Manner Exception in that it facilitates an actor reaching agreeable terms with a requestor to fulfill an EHI request and acknowledges that certain agreements have been reached for the access, exchange, and use of EHI (for example, by using standards consistent with the Common Agreement or applicable flow-down Framework agreements that the actor and requestor have agreed to abide by). Such TEFCA agreements could already fall under the current "manner requested" condition of the Manner Exception where the request is for EHI and is for an exchange purpose for which the QHIN, Participant, or Subparticipant is obligated to respond consistent with the Common Agreement or any applicable Participant-QHIN or Participant-Subparticipant Agreement(s). However, consistent with the information blocking regulations, we propose that this condition would apply for any and all EHI as defined in 45 CFR 171.102 and for exchange purposes beyond those required to be supported in the Common Agreement for Nationwide Health Information Interoperability, Version 1, as published on January 19, 2022, in the **Federal Register**.

Our proposal would offer actors certainty that fulfilling, or even attempting to fulfill, requests for EHI using Connectivity Services, QHIN Services, or the specified technical services in the applicable Framework Agreement (together referenced here as "TEFCA means," solely for ease of discussion) are covered by the Manner Exception when requestors are parties to the Common Agreement or a Framework Agreement under the Common Agreement, even when the EHI may exceed the minimum data classes and elements ***required*** by the Common Agreement as of the date a particular request is fulfilled. Through this proposed condition, the Manner Exception could be satisfied where the purpose of the requested access, exchange, or use is beyond those for which a response is explicitly required by the Common Agreement and

applicable Framework Agreements (together referenced here as "TEFCA governing agreements," solely for ease of discussion)—so long as the use of TEFCA for the purpose is ***permitted*** by the TEFCA governing agreements. (For purposes of this discussion, any "Exchange Purpose," as defined in the Common Agreement,[417] authorized under the terms of the Common Agreement and applicable Framework Agreement(s) may be described as one that is permitted, allowed, or "authorized" under TEFCA.) Importantly, this condition of the Manner Exception could be satisfied regardless of whether the requesting QHIN, Participant, or Subparticipant initially requested access, exchange, or use via TEFCA means or some other manner. To illustrate, if an actor fulfills a request to access, exchange, or use EHI from a QHIN, Participant, or Subparticipant through TEFCA means, then that would be sufficient for meeting this proposed new TEFCA condition. In this scenario, the responding actor would not be required to conform any fees or any license agreements to the Fees or Licensing Exceptions (45 CFR 171.302 and 171.303, respectively)—again, regardless of whether the requesting QHIN, Participant, or Subparticipant initially requested access, exchange, or use via Connectivity Services, QHIN Services, the specified technical services in the applicable Framework Agreement, or some other manner.

Another important feature of the proposed TEFCA condition is that it can be satisfied by the responding QHIN, Participant, or Subparticipant either fulfilling or *offering to fulfill* the requesting QHIN's, Participant's, or Subparticipant's request for EHI using Connectivity Services, QHIN Services, or the specified technical services in the applicable Framework Agreement. To illustrate, if a QHIN, Participant, or Subparticipant actor offers to fulfill a request to access, exchange, or use EHI from a QHIN, Participant, or Subparticipant through TEFCA means that are available to both the requestor and responding actor, then that would be sufficient

---

[417] *See, Common Agreement for Nationwide Health Information Interoperability, Version 1*, January 2022, Page 6. Available at: https://www.healthit.gov/sites/default/files/page/2022-01/Common_Agreement_for_Nationwide_Health_Information_Interoperability_Version_1.pdf (Last accessed March 16, 2023.)

for meeting this proposed new TEFCA condition even if the requesting QHIN, Participant, or Subparticipant initially requested access, exchange, or use in some other manner or refused to accept the responding actor's offer to fulfill the requested EHI access, exchange, or use through TEFCA means.

As discussed above regarding the ONC Cures Act Final Rule TEFCA RFI, this approach aligns with the Cures Act's goals for interoperability and the establishment of TEFCA by acknowledging the value of TEFCA in promoting access, exchange, and use of EHI in a secure and interoperable way. This approach furthers both of these goals (TEFCA adoption and interoperability) by offering actors subject to the Cures Act's information blocking provision that also choose to become QHINs, Participants, or Subparticipants certainty that their practice of declining to fulfill a request to access, exchange, or use EHI in other manners that a QHIN, Participant, or Subparticipant might initially seek will qualify for the exception so long as the responding actor fulfills (or at least offers to fulfill) the request using available TEFCA means. The proposed TEFCA condition also incorporates multiple aspects responsive to public comments and feedback received on the ONC Cures Act Proposed Rule (84 FR 7424). It recognizes and supports actors that choose to adopt and comply with the Common Agreement by providing certainty and burden reduction for those actors when it comes to information blocking and requests for access, exchange, or use of EHI by QHINs, Participants, or Subparticipants. The proposed TEFCA condition accomplishes these goals by, for example, limiting the need for an actor seeking assurance that their practices would not be considered information blocking to either satisfy a request in the non-TEFCA manner initially requested or by having to meet other conditions of the Manner Exception or another exception.

Each QHIN, Participant, or Subparticipant has chosen to become a part of the TEFCA ecosystem. Where mechanisms consistent with TEFCA's technical framework and other requirements relevant to particular type(s) of EHI and purpose(s) of exchange *can* support EHI access, exchange, use for *any* purpose permitted under the Common Agreement and applicable

Framework Agreement(s), we believe it is reasonable and necessary for actors who have chosen to become part of the TEFCA ecosystem to prioritize use of these mechanisms rather than other mechanisms—that are potentially less interoperable, less secure, or less scalable—for sharing EHI with requestors who have also chosen to become part of the TEFCA ecosystem. To be clear, the proposed TEFCA manner exception would identify as reasonable and necessary an information blocking actor's practice of prioritizing using, in lieu of other feasible manners, the appropriate TEFCA means:

- for any and all EHI for which access, exchange, or use can be supported by TEFCA means for both the actor and requestor;
- so long as the requestor is a QHIN, Participant, or Subparticipant and the purpose of the access, exchange, or use is permitted under the TEFCA governing agreements;
- regardless of whether the request is initially made through TEFCA means or otherwise; and
- regardless of whether all of the particular data class(es) or exchange purpose(s) requested are yet *required* by TEFCA's governing agreements to be returned in response to a TEFCA request.

In providing a clear, efficient path to regulatory certainty that prioritizes exchange amongst QHINs, Participants, and Subparticipants in TEFCA using TEFCA means of sharing any and all EHI that TEFCA means can support will not be considered information blocking, we hope to incentivize (and accelerate) all QHINs, Participants, and Subparticipants to embrace and accelerate their use of the available, interoperable, and secure TEFCA technical services to support the access, exchange, and use of as much EHI as possible for as many purposes as are permitted under the TEFCA governing agreements. To provide clarity, we note that the establishment of this condition would identify such prioritization on TEFCA means of responding to other QHIN, Participant, or Subparticipant requests for access, exchange, or use of EHI as reasonable and necessary for those QHINs, Participants, and Subparticipants who choose

that approach. The establishment of the TEFCA condition would not preclude a QHIN, Participant, or Subparticipant information blocking actor from making a different choice with respect to supporting non-TEFCA means in complement to TEFCA means of information sharing with others who choose to become QHINs, Participants, and Subparticipants.

In order to satisfy this condition, we are considering requiring that an actor would need to check an available directory of all QHINs, Participants, and Subparticipants under the TEFCA governing agreements in order see if the requestor is listed. As described in the QHIN Technical Framework, the "Directory Service will be the primary location for determining the HomeCommunityID and Responding QHIN for QHIN-to-QHIN data exchange. QHINs will be responsible for updating the RCE Directory Service with HomeCommunityIDs of their connected Participants and Subparticipants. QHINs are expected to maintain a local copy of the contents of the RCE Directory Service to support their Connectivity Services and facilitate query and message delivery transactions." While the listing or non-listing of a requestor in such a directory would not be dispositive as to the truth of the matter, an actor checking the directory would likely improve the efficiency of such interactions (i.e., EHI requests and responses) and would help inform the assessment of the actor's intent under the circumstances. We welcome comments on this potential requirement for satisfaction of the new proposed TEFCA condition. We also welcome comments on all aspects of the new proposed TEFCA condition for the Manner Exception.

C. Information Blocking Requests for Information

1. Additional Exclusions from Offer Health IT - Request for Information

We seek comment on whether we should consider proposing in future rulemaking any additional exclusions from the *offer health information technology* or *offer health IT* definition proposed in § 171.102 of this proposal. We seek comment in particular on health IT developers and users' experience with activities or arrangements that they believe are beneficial to patients and/or health care providers and that they can demonstrate may be occurring less often

specifically due to prospective participants' concerns about potential information blocking liability. We further welcome observations, evidence, or feedback specific to how potential additional exclusions could be structured or balanced by other measures to mitigate risks of unintended consequences of such exclusions—not limited to, but specifically including potentially insulating individuals or entities with shoddy practices or nefarious intent from accountability for subjecting their customers, clients, patients, or exchange partners to information blocking conduct. We also welcome comments on other steps that the public would recommend ONC consider taking to further encourage lawful donation or other subsidized provision of certified health IT to health care providers who may otherwise struggle to afford modern, interoperable health IT without reducing the assurances and other benefits ONC's information blocking and Health IT Certification Program regulations provide to these recipient health care providers in comparison to providers who obtain certified health IT directly from its developer or under other non-subsidized arrangements.

2. Possible Additional TEFCA Reasonable and Necessary Activities – Request for Information

We seek comment on whether any other particular practices that are not otherwise required by law but are required of an individual person or entity by virtue of their status as a QHIN, Participant, or Subparticipant pursuant to the Common Agreement pose a substantial concern or uncertainty regarding whether such practices *could* constitute information blocking as defined in 45 CFR 171.103. As a reminder, to constitute information blocking as defined in 45 CFR 171.103, the practice that is not required by law would have to be done with the requisite knowledge on the part of the actor engaging in the practice, would have to rise to the level of an interference, and not be covered by an existing information blocking exception—including but not limited to the Manner Exception as we propose to modify it. We seek comment on what, if any, particular practices required of QHINs, Participants, or Subparticipants may pose such concerns or uncertainty, and the specific source of the requirement, obligation, or commitment to

engage in the practice—such as the Common Agreement, flow-down requirements in Framework Agreements, the QHIN Technical Framework, or Standard Operating Procedures published by the ONC Recognized Coordinating Entity (RCE). We also request that commenters identify which practices they believe are not covered by existing information blocking exceptions and that commenters would advocate we assess for potential identification as reasonable and necessary activities that do not constitute information blocking as defined in 45 CFR 171.103. Recognizing that not all individuals or entities who may have a right or be allowed under applicable law to access, exchange, or use EHI may be in a position to become a QHIN, Participant, or Subparticipant, we also seek comment on whether and how any such identification of additional reasonable and necessary activities might pose concerns about unintended consequences for EHI access, exchange, or use by individuals or entities who are not QHINs, Participants, or Subparticipants.

For more information on TEFCA, please visit: https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement-tefca.

3. Health IT Capabilities for Data Segmentation and User/Patient Access – Request for Information

ONC believes that data segmentation is an integral capability for enabling the access, exchange, and use of electronic health information (85 FR 25705). While initiatives such as security tagging capabilities represent an initial step towards enabling appropriate access, exchange, and use of health information in accordance with applicable law and patient preferences, many additional data segmentation challenges remain, including the prevalence of unstructured data, the sharing of image files, the use of sensitive health information (see section III.C.10 of this proposed rule and 85 FR 25702), and other technical and non-technical (e.g. policy and regulatory) challenges.

We have received public feedback indicating that there is significant variability in health IT products' capabilities to segment data, notably including enabling differing levels of access to data based on the user and purpose. There are, as also discussed in section III.C.10 of this proposed rule, many situations in which segmentation of data may be required or requested, including use cases where special handling or other restriction of access, exchange, or use of particular portion(s) of a patient's EHI is required by law or consistent with an individual patient's expressed preference regarding their own or others' access to their EHI. In section III.C.10 of this proposed rule, we propose a new certification criterion specifically focused on supporting patient preferences related to their right to request a restriction on certain uses and disclosures of their PHI under the HIPAA Privacy Rule (see 45 CFR 164.522). This proposed functionality is focused specifically on supporting one health IT enabled mechanism for a patient to request a restriction on disclosure and for a covered entity to honor that restriction using a certified Health IT Module (See section III.C.10 for further detail).

In addition to the specific right to request a restriction on disclosure consistent with 45 CFR 164.522, there are other use cases related to patient preferences — and specific nuances within use cases — which present challenges from a technical point of view. Through public forums and correspondence with ONC, interested parties in the healthcare community have conveyed that their certified health IT lacks capabilities to differentiate the timing of release of certain EHI based on patients' individual preferences. Some interested parties have also indicated that their certified health IT may have little or no ability to restrict a patient's personal representative's access to only some of the patient's EHI using electronic means such as a portal or API or to easily hold back only some pieces of the patient's EHI, in response to or at the patient's request, while honoring the patient's simultaneous preference for the rest of their EHI to be shared with another of their health care providers. One example of a reason an individual might request that some of their information be withheld from (not disclosed to or shared with) some of their health care providers while the rest of their information continued to be shared

would be that the individual expects certain information could be associated with conditions or care that may be stigmatized by health care providers other than the one to whom the individual disclosed the information or who provided the specific care. A provider who knows a patient requested restrictions on (or expressed a preference not to share) specific information out of concern about potential stigmatization might want to honor the patient's request to as part of or in support of patient-provider confidentiality and patient trust, regardless of whether the health care provider shared the patient's concern about how other providers might react to the specific information the patient believes would be potentially stigmatizing. Out of respect for the patient's privacy and autonomy and fostering trust within patient-provider relationship, a provider might choose to honor a patient's request for restrictions on sharing of their EHI even if the provider did not *know* the patient's specific reasons for the request. Neither the 45 CFR 164.522(a) right to request restrictions under the HIPAA Privacy Rule nor the information blocking regulations' § 171.202(e)) *subexception respecting an individual's request not to share information* specify that the individual requesting restrictions should have particular reasons, or be required to share with the provider or other actor of whom they make the request their reasoning, for requesting restrictions.

We seek comment to inform steps we might consider taking to improve the availability and accessibility of solutions supporting health care providers' and other information blocking actors' efforts to honor patients' expressed preferences regarding their EHI. For example, patients may express a preference for a delay in the availability of information to them (such as in a health care provider's patient portal). Or, for another example, actor could choose to honor a patient request that to the actor withhold certain information from particular access, exchange, or use consistent with the individual right to request restrictions under the HIPAA Privacy Rule and the information blocking Privacy Exception.[418] We seek to support information blocking actors'

[418] This particular example assumes that the actor is also required to comply with the HIPAA Privacy Rule and that their practices in restricting access, exchange, or use of EHI are consistent with both § 164.522(a), the HIPAA

efforts to honor patients' expressed preferences that other law allows the actor to honor as well as actors' needs to complying with all applicable tribal, state, and federal laws restricting or placing specific preconditions on permissibility of information access (release of information) and sharing in situations (or "use cases") such as those described in the non-exhaustive assortment of examples below.

Based on questions and feedback we have received subsequent to the ONC Cures Act Final Rule, examples of situations (or "use cases") include, but are not limited to:

- A heath care provider needs to prove or validate consent of the patient (by electronic or manual means) regarding EHI subject to the Confidentiality of Substance Use Disorder Patient Records regulations, 42 CFR part 2 — or other federal law or applicable state or tribal law with specific consent requirements — prior to sharing it with another health care provider treating the same patient for other clinical concerns.
- A health care provider needs to identify and segment from particular access, exchange, or use by specific entities for specific purposes data subject to varying state laws requiring special handling or access restrictions in such situations—such as behavioral health information, HIV diagnosis and treatment, genetic testing, treatment of minors, or incidents of sexual violence.
- An actor's practice meets the conditions of the Preventing Harm Exception (§ 171.201) for withholding EHI for access, exchange, or use—such as access by the patient or by a particular personal representative of the patient— of ***some***, but not all, of the EHI the actor has for a particular patient.

Privacy Rule right of an individual to request restriction of uses and disclosures of their PHI, and § 171.202(e) *sub-exception - respecting an individual's request not to share information* under the information blocking regulations. We emphasize that this example assumes the restrictions are ones that the HIPAA Privacy Rule does *not* require covered entities to grant at patient request, in order to remind readers that where an actor is explicitly required by the HIPAA Privacy Rule to restrict access, exchange, or use of EHI the actor's practice of applying those restrictions is "required by law" and would not be considered information blocking (no exception needed, as we discussed in the Cures Act Final Rule at 85 FR 25794).

- A health care provider (or other actor) chooses to grant a patient's request to delay the release of certain EHI—such as new diagnoses or particular laboratory or imaging result(s)—to the patient or the patient's personal representative either for a particular period of time or until a particular event, such as communication between the patient and a clinician or patient educator, has occurred.[419]
- A health care provider (or other information blocking actor) wants to respect an individual's request, per the individual's privacy preference, not to share ***some of*** the individual's EHI with others to whom it could legally be disclosed–such as the individual's other health care providers or their personal representative.[12]
- The actor wishes to be certain their practices for respecting these patient privacy preferences will not be considered information blocking, so they set up their practices in accordance with § 171.202(e), the sub-exception to the privacy exception concerning respecting an individual's request not to share information.[420] (We direct readers to section III.C.10 for our health IT certification proposal specifically relevant to this example).
- A health care provider needs to identify and segment data for research purposes, according to the conditions outlined in the HIPAA Privacy Rule[421] and the Federal Policy for the Protection of Human Subjects ("Common Rule"), as applicable.[422]

It is our impression that at least some health care providers and their patients sometimes encounter various challenges as they work to provide patients or their personal representatives with electronic access to the information they want when they want it. These challenges notably include, though they are not necessarily limited to, shortfalls in the technical capability of some

---

[419] See also, https://www.healthit.gov/curesrule/faq/can-actor-grant-patients-request-delay-release-patients-test-results-eg-laboratory-or-image.
[420] 45 CFR 171.202(e)
[421] 45 CFR 164.512(i). See also, https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html
[422] See 45 CFR part 46. See also, https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html

health IT to segment and filter EHI for appropriate access, exchange, and use consistent with applicable law and patient preferences.

Examples of challenges or technical limitations to EHI segmentation and filtering to facilitate appropriate EHI access, exchange, or use that have been described to ONC include, but are not necessarily limited to:

- A certified EHR (certified health IT) currently in use by a health care provider that is, as implemented, capable only of "all or nothing" release of all EHI test results for all patients immediately to the patient portal, without offering the ordering clinicians or other healthcare professionals using the certified EHR any capability to flag or withhold individual EHI test results for an individual patient from the patient portal.
- A health care provider's current certified EHR is designed and implemented such that any test result the patient and health care provider want to have available to the patient in the portal must be manually pushed to the portal, result by result, by the ordering clinician.
- Existing segmentation tools or modalities (for example, implementation of segmentation capabilities only by broad data class rather than at the level of individual data point) not providing enough flexibility to address more complex use cases, such as honoring a patient's request to have immediate access to most of their EHI but to have electronic access to some EHI, such as test results, that are complicated to interpret or indicate a potential of a life-limiting diagnosis, only after such results have been explained to them in real time by an appropriately qualified healthcare professional.
- An existing certified EHR system does not have technical capacity to appropriately segment and share specific health information according to applicable laws, such as where a parent or legal guardian is legally permitted to obtain portions of a non-

emancipated minor child's EHI regardless of the child's consent but not legally permitted to obtain other portions of the child's EHI without the child's consent.[423]

- No health IT that a health care provider has or could implement includes the capability to automate the capture and execution of a patient's or patient's personal representative's unique individual preferences for when new EHI becomes available to them through electronic access.

In this proposed rule, we seek comment related to the capabilities of health IT products to segment data and support health care providers (and actors) in sharing information consistent with patient preferences and all laws applicable to the creation, collection, access, exchange, use and disclosure of EHI.

We also seek comment on experiences with the availability and utility of certified health IT products' capabilities to segment data in use cases including but not limited to the illustrative examples above. We also seek comment on how greater consistency in provider documentation practices could enhance the feasibility of technical segmentation solutions. Similarly, we seek comment on barriers to technical feasibility presented by local, state, and federal regulations. Further, we note our proposal in section III.C.10 and request comment on how else the Program could better support the other use cases described above either through functional or standards-based certification requirements.

V. Incorporation by Reference

The Office of the Federal Register has established requirements for materials (e.g., standards and implementation specifications) that agencies propose to incorporate by reference in the Code of Federal Regulations (79 FR 66267; 1 CFR 51.5(a)). Specifically, § 51.5(a) requires agencies to discuss, in the preamble of a proposed rule, the ways that the materials it proposes to incorporate by reference are reasonably available to interested parties or how it

[423] Examples of such applicable laws would include state or tribal laws restricting parental access to specific information within a non-emancipated minor's medical records. At the federal level, one example would be 42 CFR 59.10 confidentiality requirements applicable to Title X recipients, subrecipients, and service sites.

worked to make those materials reasonably available to interested parties; and summarize, in the preamble of the proposed rule, the material it proposes to incorporate by reference.

To make the materials we intend to incorporate by reference reasonably available, we provide a uniform resource locator (URL) for the standards and implementation specifications. In many cases, these standards and implementation specifications are directly accessible through the URLs provided. In most of these instances, access to the standard or implementation specification can be gained through no-cost (monetary) participation, subscription, or membership with the applicable standards developing organization (SDO) or custodial organization. Alternatively, a copy of the standards may be viewed for free at the U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, 330 C Street SW, Washington, DC 20201. Please call (202) 690-7171 in advance to arrange inspection.

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 et seq.) and the Office of Management and Budget (OMB) Circular A–119 require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A-119 provide exceptions to selecting only standards developed or adopted by voluntary consensus standards bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. As discussed in section III.B of this preamble, we have followed the NTTAA and OMB Circular A-119 in proposing standards and implementation specifications for adoption, including describing any exceptions in the proposed adoption of standards and implementation specifications. Over the years of adopting standards and implementation specifications for certification, we have worked with SDOs, such as HL7, to make the standards we propose to adopt, and subsequently adopt and incorporate by reference in the **Federal Register**, available to interested parties. As described above, this includes making

the standards and implementation specifications available through no-cost memberships and no-cost subscriptions.

As required by § 51.5(a), we provide summaries of the standards we propose to adopt and subsequently incorporate by reference in the Code of Federal Regulations. We also provide relevant information about these standards and implementation specifications throughout the preamble.

We have organized the following standards and implementation specifications that we propose to adopt through this rulemaking according to the sections of the Code of Federal Regulations (CFR) in which they would be codified and cross-referenced for associated certification criteria and requirements that we propose to adopt. We note, in certain instances, that we request comment in this proposed rule on multiple standards or implementation specifications that we are considering for adoption *and incorporation by reference* for particular use cases. We include all of these standards and implementation specifications in this section of the preamble.

Content exchange standards and implementation specifications for exchanging electronic health information – 45 CFR 170.205

- *Health Level 7 (HL7®) CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes STU Companion Guide, Release 3 - US Realm, May 12, 2022.*

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=447

Access requires a ‘‘user account’’ and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Companion Guide to Consolidated Clinical Document Architecture (C-CDA) R3, provides essential implementer guidance to continuously expand interoperability for clinical information shared via structured clinical notes. The guidance supplements specifications established in the Health Level Seven (HL7) CDA® R2.1 IG: C-CDA Templates for Clinical Notes. This additional guidance is intended to make implementers aware of expectations and best

practices for C-CDA document exchange. The objective is to increase consistency and expand interoperability across the community of data sharing partners who utilize C-CDA for information exchange.

- *HL7 FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.0 – STU 2 US (HL7 FHIR eCR IG), August 31, 2022.*

URL: https://build.fhir.org/ig/HL7/case-reporting/

Access requires a ‘‘user account’’ and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: With the adoption and maturing of Electronic Health Records (EHRs), there are opportunities to better support public health surveillance as well as to better support the delivery of relevant public health information to clinical care. Electronic Case Reporting (eCR) can provide more complete and timely case data, support disease/condition monitoring, and assist in outbreak management and control. It can also improve bidirectional communications through the delivery of public health information in the context of a patient’s condition and local disease trends and by facilitating ad hoc communications, as well as reduce health care provider burden by automating the completion of legal reporting requirements. The purpose of this FHIR IG is to offer opportunities to further enable automated triggering and reporting of cases from EHRs, to ease implementation and integration, to support the acquisition of public health investigation supplemental data, and to connect public health information (e.g., guidelines) with clinical workflows. Over time, FHIR may also support the distribution of reporting rules to clinical care to better align data authorities and make broader clinical data available to public health decision support services inside the clinical care environment.

- *HL7 CDA® R2 Implementation Guide: Public Health Case Report - the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1 - US Realm (HL7 CDA eICR IG), July 20, 2022.*

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=436

Access requires a ‘‘user account’’ and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The purpose of this implementation guide (IG) is to specify a standard for electronic submission of electronic initial public health case reports using HL7 Version 3 Clinical Document Architecture (CDA), Release 2 format. This implementation guide specifies a standard that will allow health care providers to electronically communicate the specific data needed in initial public health case reports (required by state laws/regulations) to jurisdictional public health agencies in CDA format—an interoperable, industry-standard format.

- *HL7 CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1 - US Realm (HL7 CDA RR IG), July 17, 2022.*

URL: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=470

Access requires a ‘‘user account’’ and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The purpose of this implementation guide (IG) is to specify a standard for a response document for a public health electronic Initial Case Report (HL7 eICR all releases) using HL7 Version 3 Clinical Document Architecture (CDA), Release 2 format. Through the Reportability Response, public health seeks to support bidirectional communication with clinical care for reportable conditions in CDA format, which is an interoperable, industry-standard format.

- *Reportable Conditions Trigger Codes Value Set for Electronic Case Reporting. RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022.*

URL: https://ecr.aimsplatform.org/ehr-implementers/triggering/

This is a direct access link.

Summary: The Reportable Condition Trigger Codes (RCTC) are a nation-wide set of standardized codes to be implemented within an electronic health record (EHR) that provide a preliminary identification of events that may be of interest to public health for electronic case reporting. The RCTC are the first step in a two-step process to determine reportability. The

RCTC are single factor codes that represent any event that may be reportable to any public health agency in the United States. A second level of evaluation still must be done against jurisdiction-specific reporting regulations, to confirm whether the event is reportable and to which public health agency or agencies. The RCTC currently includes ICD 10 CM, SNOMED CT, LOINC, RxNorm, CVX, and CPT, representing condition-specific diagnoses, resulted lab tests names, lab results, lab orders for conditions reportable upon suspicion, and medications for select conditions.

- *HL7 FHIR® Data Segmentation for Privacy Implementation Guide: Version 1.0.0 – current – ci-build, December 1, 2022.*

URL: https://build.fhir.org/ig/HL7/fhir-security-label-ds4p/index.html

This is a direct access link.

Summary: The HL7 FHIR Data Segmentation for Privacy IG provides guidance for applying security labels in FHIR. Security labels are used in access control systems governing the collection, access, use, and disclosure of health information to which they are assigned, such as FHIR resource(s), as required by applicable organizational, jurisdictional, or personal policies related to privacy, security, and trust. This IG is intended to complement the existing The HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (IG), which specifies the use of security labeling at the CDA Header, Section and Entry levels.

Vocabulary standards for representing electronic health information – 45 CFR 170.207

- *HL7 Standard Code Set CVX – Vaccines Administered, updates through June 15, 2022.*

URL: https://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=cvx

This is a direct access link.

Summary: The CDC's National Center of Immunization and Respiratory Diseases (NCIRD) developed and maintains the CVX (vaccine administered) code set. It includes both active and inactive vaccines available in the US. CVX codes for inactive vaccines allow transmission of historical immunization records. When a MVX (manufacturer) code is paired with a CVX

(vaccine administered) code, the specific trade named vaccine may be indicated. These codes should be used for immunization messages using either HL7 Version 2.3.1 or HL7 Version 2.5.1.

- *National Drug Code Directory (NDC) – Vaccine NDC Linker, updates through July 19, 2022.*

URL: https://www2.cdc.gov/vaccines/iis/iisstandards/ndc_tableaccess.asp

This is a direct access link.

Summary: The Drug Listing Act of 1972 requires registered drug establishments to provide the FDA with a current list of all drugs manufactured, prepared, propagated, compounded, or processed by it for commercial distribution. Drug products are identified and reported using a unique, three-segment number, called the National Drug Code (NDC), which serves as the universal product identifier for drugs. This standard is limited to the NDC vaccine codes identified by CDC.

- *CDC Race and Ethnicity Code Set version 1.2, July 15, 2021.*

URL: https://www.cdc.gov/phin/resources/vocabulary/index.html

The code set can be accessed through this link.

Summary: The U.S. Centers for Disease Control and Prevention (CDC) has prepared a code set for use in coding race and ethnicity data. This code set is based on current federal standards for classifying data on race and ethnicity, specifically the minimum race and ethnicity categories defined by the U.S. Office of Management and Budget (OMB) and a more detailed set of race and ethnicity categories maintained by the U.S. Bureau of the Census (BC). The main purpose of the code set is to facilitate use of federal standards for classifying data on race and ethnicity when these data are exchanged, stored, retrieved, or analyzed in electronic form. At the same time, the code set can be applied to paper-based record systems to the extent that these systems are used to collect, maintain, and report data on race and ethnicity in accordance with current federal standards.

- *Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy (October 29, 2021).*

URL: https://data.cms.gov/provider-characteristics/medicare-provider-supplier-enrollment/medicare-provider-and-supplier-taxonomy-crosswalk/data

This is a direct access link.

Summary: The Medicare Provider and Supplier Taxonomy Crosswalk dataset lists the providers and suppliers eligible to enroll in Medicare programs with the proper healthcare provider taxonomy code. This data includes the Medicare specialty codes, if available, provider/supplier type description, taxonomy code, and the taxonomy description. The Healthcare Provider Taxonomy Code Set is a hierarchical code set that consists of codes, descriptions, and definitions. Healthcare Provider Taxonomy Codes are designed to categorize the type, classification, and/or specialization of health care providers. The Code Set is available from the Washington Publishing Company (https://wpc-edi.com/). The Code Set is maintained by the National Uniform Claim Committee (https://www.nucc.org/).

- *Public Health Data Standards Consortium Source of Payment Typology Code Set, Version 9.2, December 2020.*

URL: https://nahdo.org/sites/default/files/2020-12/SourceofPaymentTypologyUsersGuideVersion9.2December2020.pdf

This is a direct access link.

Summary: The Source of Payment Typology was developed to create a standard for reporting payer type data that will enhance the payer data classification; it is also intended for use by those collecting data or analyzing healthcare claims information. Modeled loosely after the ICD typology for classifying medical conditions, the proposed typology identifies broad Payer categories with related subcategories that are more specific. This format provides analysts with flexibility to either use payer codes at a highly detailed level or to roll up codes to broader hierarchical categories for comparative analyses across payers and locations.

- *Logical Observation Identifiers Names and Codes (LOINC ®) Database Version 2.72, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc., February 16, 2022.*

URL: https://loinc.org/downloads/

Access requires registration, a user account, and license agreement. There is no monetary cost for registration, a user account, and license agreement.

Summary: Informed by tracking healthcare trends, evaluating concept requests, and listening to guidance from the community, this release contains new and edited concepts in Laboratory, Clinical, Survey, Document Type, and other domains. It also includes a newly streamlined release file structure for more efficient download and use.

- *The Unified Code of Units of Measure, Revision 2.1, November 21, 2017.*

URL: https://ucum.org/ucum.html

This is a direct access link.

Summary: The Unified Code for Units of Measure is a code system intended to include all units of measures being contemporarily used in international science, engineering, and business. The purpose is to facilitate unambiguous electronic communication of quantities together with their units. The focus is on electronic communication, as opposed to communication between humans. A typical application of The Unified Code for Units of Measure are electronic data interchange (EDI) protocols, but there is nothing that prevents it from being used in other types of machine communication.

- *International Health Terminology Standards Development Organization (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT ®) U.S. Edition, March 2022 Release.*

URL: https://www.nlm.nih.gov/healthit/snomedct/archive.html

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: In addition to the 279 new active concepts specific to the US Edition, the March 2022 SNOMED CT US Edition also includes the SNOMED CT COVID-19 Related Content published in the January 2022 SNOMED CT International Edition. This latest version of the US Edition also includes the SNOMED CT to ICD-10-CM reference set, with over 126,000 SNOMED CT source concepts mapped to ICD-10-CM targets.

- *RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, July 5, 2022 Release.*

URL: https://www.nlm.nih.gov/pubs/techbull/ja22/brief/ja22_rxnorm_july_release.html

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: RxNorm, a standardized nomenclature for clinical drugs, is produced by the National Library of Medicine. RxNorm's standard identifiers and names for clinical drugs are connected to the varying names of drugs present in many different controlled vocabularies within the Unified Medical Language System (UMLS) Metathesaurus, including those in commercially available drug information sources. These connections are intended to facilitate interoperability among the computerized systems that record or process data dealing with clinical drugs.

United States Core Data for Interoperability – 45 CFR 170.213

- *United States Core Data for Interoperability (USCDI), October 2022 Errata, Version 3 (v3).*

URL: https://www.healthit.gov/USCDI

This is a direct access link.

Summary: The United States Core Data for Interoperability (USCDI) establishes a minimum set of data classes that are required to be interoperable nationwide and is designed to be expanded in an iterative and predictable way over time. Data classes listed in the USCDI are represented in a technically agnostic manner to set a foundation for broader sharing of electronic health information. ONC has established a predictable, transparent, and collaborative expansion process

for USCDI based on public evaluation of previous versions and submissions by the health IT community and the public, including input from a federal advisory committee.

Application Programming Interface Standards – 45 CFR 170.215

- *HL7 FHIR US Core Implementation Guide STU 5.0.1, June 13, 2022*

URL: http://hl7.org/fhir/us/core/

This is a direct access link.

Summary: The US Core Implementation Guide is based on FHIR Version R4 and defines the minimum set of constraints on the FHIR resources to create the US Core Profiles. It also defines the minimum set of FHIR RESTful interactions for each of the US Core Profiles to access patient data. By establishing the "floor" of standards to promote interoperability and adoption through common implementation, it allows for further standards development evolution for specific uses cases.

- *HL7 FHIR® SMART Application Launch Framework Implementation Guide Release 2.0.0, November 26, 2021*

URL: http://hl7.org/fhir/smart-app-launch/

This is a direct access link.

Summary: This implementation guide describes a set of foundational patterns based on OAuth 2.0 for client applications to authorize, authenticate, and integrate with FHIR-based data systems.

VI. Response to Comments

Because of the large number of public comments normally received in response to **Federal Register** documents, we are not able to acknowledge or respond to them individually. We will consider all comments we receive by the date and time specified in the DATES section of this preamble, and when we proceed with a subsequent document, we will respond to the comments in the preamble of that document.

VII. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995 (PRA), codified as amended at 44 U.S.C. 3501 et seq., agencies are required to provide a 60-day notice in the **Federal Register** and solicit public comment on a proposed collection of information before it is submitted to the Office of Management and Budget for review and approval. In order to fairly evaluate whether an information collection should be approved by the OMB, section 3506(c)(2)(A) of the PRA requires that we solicit comment on the following issues:

1. Whether the information collection is necessary and useful to carry out the proper functions of the agency;

2. The accuracy of the agency's estimate of the information collection burden;

3. The quality, utility, and clarity of the information to be collected; and

4. Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Under the PRA, the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section are to be considered. We explicitly seek, and will consider, public comment on our assumptions as they relate to the PRA requirements summarized in this section. To comment on the collection of information or to obtain copies of the supporting statements and any related forms for the proposed paperwork collections referenced in this section, email your comment or request, including your address and phone number to sherrette.funn@hhs.gov, or call the Reports Clearance Office at (202) 690–6162. Written comments and recommendations for the proposed information collections must be directed to the OS Paperwork Clearance Officer at the above email address within 60 days.

A. Independent Entity

We propose that response submissions related to the Insights Condition and Maintenance of Certification requirements as discussed in section III.F of this preamble would be submitted to an independent entity on behalf of ONC. Specifically, we intend to award a grant, contract, or other agreement to an independent entity as part of the implementation of the Insights Condition

and Maintenance of Certification requirements and will provide additional details through subsequent information. We intend to make responses publicly available via an ONC website and intend to provide developers of certified health IT the opportunity to submit qualitative notes that would enable them to explain findings and provide additional context and feedback regarding their submissions.

For the purposes of estimating potential burden, we believe the independent entity would take approximately 5 minutes to review a response submission for completeness, and approximately 30 minutes to submit the completed response submission to ONC, based on how many products a health IT developer of certified health IT may be required to submit responses for. We also plan to minimize burden for the independent entity by automating parts of the response review and submission process via an online tool (estimated that ONC will spend approximately $1.5 million to develop and implement). We welcome comments if it is believed that more or less time should be included in our estimate.

Table 4. Estimated Annualized Burden Hours for Independent Entity to Review and Submit Developer Responses to ONC per Insights Condition Requirements

Code of Federal Regulations Section	Number of Independent Entity	Average Burden Hours	Total
45 CFR 170.407(a)	1	24	24
45 CFR 170.407(b)	1	143	143
Total Burden Hours			167

B. Health IT Developers

We propose in 45 CFR 170.407 that a health IT developer of certified health IT must submit responses associated with the Insights Condition and Maintenance of Certification requirements to an independent entity twice a year. We plan to minimize burden for health IT developers of certified health IT by providing a web-based submission form and method to simplify the process for response submission. For the purposes of estimating potential burden, we are estimating 52 health IT developers of certified health IT will be required to report on the

proposed measures within the Insights Condition and Maintenance of Certification requirements. We believe it will take approximately 21,136 to 44,900 hours on average for a health IT developer of certified health IT to collect and report on the proposed measures within the Insights Condition and Maintenance of Certification requirements. For the purposes of estimating the total potential burden for health IT developers of certified health IT, we estimate an average burden of 2,334,800 hours. However, this is a crude upper bound estimate as there are multiple measures with varying complexity associated with the Insights Condition and Maintenance of Certification, and the number of health IT developers of certified health IT required to report changes by each measure. For a more detailed discussion and the cost estimates of these new regulatory requirements associated with the Insights Condition and Maintenance of Certification, we refer readers to section VIII., Regulatory Impact Statement, of this proposed rule. We welcome comments if it is believed that more or less time should be included in our estimate.

Table 5: Estimated Annualized Total Burden Hours for Health IT Developers to Comply with the Insights Condition and Maintenance of Certification Requirements

Code of Federal Regulations Section	Number of Health IT Developers	Average Burden Hours - Lower Bound	Average Burden Hours - Upper Bound
45 CFR 170.407(a)	52	21,136	44,900
Total Burden Hours		1,099,072	2,334,800

We propose in § 170.315(b)(11)(vii)(B) that health IT developers compile documentation regarding the intervention risk management practices listed in § 170.315(b)(11)(vii)(A), and upon request from ONC, make available such detailed documentation for any predictive decision support intervention, as defined in § 170.102, that the certified Health IT Module enables or interfaces with. We believe ONC has the authority to conduct Direct Review consistent with § 170.580(a)(2) for any known non-conformity or where it has a reasonable belief that a non-conformity exists enabling ONC to have oversight of these requirements. The PRA, however,

exempts these information collections. Specifically, 44 U.S.C. 3518(c)(1)(B)(ii) excludes collection activities during the conduct of administrative actions or investigations involving the agency against specific individuals or entities.

C. ONC-ACBs

We propose in § 170.315(b)(11)(vii)(C) that a health IT developer that attests "yes" in § 170.315(b)(11)(v)(A) submit summary information of the intervention risk management practices listed in § 170.315(b)(11)(vii)(A)(*1*) through (*3*) to its ONC-ACB via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. To support submission of documentation, and consistent with other Principles of Proper Conduct in § 170.523(f)(1), we propose a new Principle of Proper Conduct for documentation related to § 170.315(b)(11)(vii)(C) in § 170.523(f)(1)(xxi). In the 2015 Edition Proposed Rule (80 FR 16894), we estimated fewer than ten annual respondents for all of the regulatory ''collection of information'' requirements that applied to the ONC-ACBs, including those previously approved by OMB. In the 2015 Edition Final Rule (80 FR 62733), we concluded that the regulatory ''collection of information'' requirements for the ONC-ACBs were not subject to the PRA under 5 CFR 1320.3(c). We continue to estimate fewer than 10 respondents for all of the regulatory "collection of information" requirements under Part 170 of Title 45. We welcome comments on this conclusion and our supporting rationale for this conclusion.

VIII. Regulatory Impact Statement

A. Statement of Need

This proposed rule is necessary to meet our statutory responsibilities under the Cures Act and to advance HHS policy goals to promote interoperability and mitigate burden for health IT developers and users. Proposals that could result in monetary costs for health IT developers and users include the: (1) proposals to update ONC Certification Criteria for Health IT; (2) proposal

for the Insights Condition and Maintenance of Certification requirements; and (3) proposals related to information blocking.

While much of the costs of this proposed rule will fall on health IT developers that seek to certify health IT under the Program, we believe the implementation and use of ONC Certification Criteria for Health IT, compliance with the Insights Condition and Maintenance of Certification requirements ("Insights Condition"), and the provisions related to information blocking proposed would ultimately result in significant benefits for health care providers and patients. We outline some of these benefits below. We emphasize in this regulatory impact analysis (RIA) that we believe this proposed rule would remove barriers to interoperability and EHI exchange, which would greatly benefit health care providers and patients.

We note in this RIA that there were instances in which we had difficulty quantifying certain benefits due to a lack of applicable studies, data, or both. However, in such instances, we highlight the significant non-quantified benefits of our proposals to advance an interoperable health system that empowers individuals to use their EHI to the fullest extent and enables health care providers and communities to deliver smarter, safer, and more efficient care.

B. Alternatives Considered

If there are alternatives to our proposals, we have described them within each of the sections within this RIA. In some cases, we have been unable to identify alternatives that would appropriately implement our responsibilities under the Cures Act and support interoperability. We believe our proposals take the necessary steps to fulfill the mandates specified in the Public Health Service Act (PHSA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Cures Act, in the least burdensome way. We are, however, open to less burdensome alternatives that meet statutory requirements and our goals. Accordingly, we welcome comments on our assessment and any alternatives we should consider.

C. Overall Impact

We have examined the impact of this proposed rule as required by Executive Order

12866 on Regulatory Planning and Review (September 30, 1993), Executive Order 13563 on Improving Regulation and Regulatory Review (February 2, 2011), section 202 of the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1532), and Executive Order 13132 on Federalism (August 4, 1999).

1. Executive Orders 12866 and 13563 – Regulatory Planning and Review Analysis

Executive Orders 12866 on Regulatory Planning and Review and 13563 on Improving Regulation and Regulatory Review direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). An RIA must be prepared for major rules with economically significant effects ($100 million or more in any one year). OMB has determined that this proposed rule is an economically significant rule as the potential costs associated with this proposed rule could be greater than $100 million per year. Accordingly, we have prepared an RIA that to the best of our ability presents the costs and benefits of this proposed rule.

a. Costs and Benefits

We have estimated the potential monetary costs and benefits of this proposed rule for health IT developers, health care providers, patients, and the Federal Government (*i.e.,* ONC), and have broken those costs and benefits out by section. In accordance with Executive Order 12866, we have included the RIA summary table as Table 35.

Our cost calculations quantify health IT developers' time and effort to implement these proposals through new development and administrative activities. We recognize that the costs developer incur as a result of these proposals may be passed on to certified technology end-users. These end-users include but are not limited to the nearly 5,000 non-federal hospitals who provide acute, inpatient care and over 1 million clinicians who provide outpatient care to all Americans. Official statistics show that nearly all U.S. non-federal acute care hospitals (https://www.healthit.gov/data/quickstats/national-trends-hospital-and-physician-adoption-

electronic-health-records) and the vast majority of outpatient physicians use certified health IT (https://www.healthit.gov/data/quickstats/office-based-physician-electronic-health-record-adoption). These proposals affect the technology all these health care providers use.

The benefits, both quantifiable and not quantifiable, articulated in this impact analysis have the potential to remove barriers to interoperability and EHI exchange for all these health care providers. Though these proposals first require effort by health IT developers to engineer them into their software, they must then be implemented by end-users to achieve the stated benefits – to healthcare delivery and the overall efficacy of the technology to document, transmit, and integrate EHI across multiple data systems.

To this end, we acknowledge that these estimated costs may not be borne solely by the health IT developers and could be passed on to end-users through health IT developers' licensing, maintenance, and other operating fees and costs. We assume health IT developers may pass on up to the estimated costs of these proposals, but not amounts above those estimated totals.

However, we have limited data on the fees and costs charged by health IT developers and how those fees and costs are distributed across various customer organizations. Given the ongoing nature of updates made by ONC to certified EHR technology, EHR developers may have already built in the costs associated with making these updates in their existing contracts. To the extent the costs associated with the updates we have proposed have not been taken into account, these costs may be passed on to end-users in different ways by health IT developers and across different health care provider organization types. Large integrated healthcare systems may face different fees and other pricing than different sized or structured health care provider organizations. The incredible diversity of the healthcare system also limits our ability to accurately model how these costs could be passed on even if there were data available to estimate how these proposals might alter the pricing models and fee rates of the nearly 400 health IT developers we estimate will be impacted by these proposals.

What we can say with more certainty is the overall impact of these proposals on the healthcare system as a whole. These proposals affect the certified technology used by the providers who give care to a vast majority of Americans. Nearly all emergency room visits, hospital stays, and regular check-ups are documented and managed using certified health IT. These proposals affect the interoperability of EHI for these care events and patients' electronic access to their health information. Certified health IT is now a nearly ubiquitous part of U.S. healthcare, and the costs and benefits estimated here encompass the far reach of these technologies and their impact on all facets of care.

Overall, it is highly speculative to quantify benefits associated with new technologies and standards we are proposing given their novelty and limited use. Emerging technologies may be used in ways not originally predicted. For example, ONC helped support the development of SMART on FHIR, which defines a process for an application to securely request access to data, and then receive and use that data. ONC would not have predicted that it would not only be used to support major EHR products, but also be used by Apple to connect its Health App to hundreds of healthcare systems, and used for apps launch on the Microsoft Azure product. It is also speculative to quantify benefits for specific stakeholders because benefits associated with many of ONC's proposals, which advance interoperability, don't necessarily accrue to stakeholders making the investments in developing and implementing the technologies. Benefits related to interoperability are spread across the healthcare ecosystem and can be considered a societal benefit. We have sought to describe benefits for each of the specific proposals and we welcome comments on how to quantify these benefits across a variety of stakeholders.

We note that we have rounded all estimates to the nearest dollar and that all estimates are expressed in 2021 dollars as it is the most recent data available to address all cost and benefit estimates consistently. The wages used to derive the cost estimates are from the May 2021 National Occupational Employment and Wage Estimates reported by the U.S. Bureau of Labor

Statistics.[424] We also note that estimates presented in the following "Employee Assumptions and Hourly Wage," "Quantifying the Estimated Number of Health IT Developers and Products," and "Number of End Users that Might Be Impacted by ONC's Proposed Regulations" sections are used throughout this RIA.

For proposals where research supported direct estimates of impact, we estimated the benefits. For proposals where no such research was identified to be available, we developed estimates based on a reasonable proxy.

We note that interoperability can positively impact patient safety, efficacy, care coordination, and improve healthcare processes and other health-related outcomes.[425] However, achieving interoperability is a function of a number of factors including the capability of the technology used by health care providers. Therefore, to assess the benefits of our proposals, we must first consider how to assess their respective effects on interoperability holding other factors constant.

Employee Assumptions and Hourly Wage

We have made employee assumptions about the level of expertise needed to complete the proposed requirements in this section. Unless indicated otherwise, for wage calculations for federal employees and ONC-ACBs, we have correlated the employee's expertise with the corresponding grade and step of an employee classified under the General Schedule (GS) Federal Salary Classification, relying on the associated employee hourly rates for the Washington, DC, locality pay area as published by the Office of Personnel Management for 2021.[426] We have assumed that other indirect costs (including benefits) are equal to 100% of pre-tax wages. Therefore, we have doubled the employee's hourly wage to account for other indirect costs. We

---

[424] May 2021 National Occupational Employment and Wage Estimates, United States. U.S. Bureau of Labor Statistics. https://www.bls.gov/oes/current/oes_nat.htm

[425] Nir Menachemi, Saurabh Rahurkar, Christopher A Harle, Joshua R Vest, The benefits of health information exchange: an updated systematic review, *Journal of the American Medical Informatics Association*, Volume 25, Issue 9, September 2018, Pages 1259–1265, https://doi.org/10.1093/jamia/ocy035

[426] Office of Personnel and Management. 2021 General Schedule (GS) Locality Pay Tables https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2021/general-schedule/

have concluded that a 100% expenditure on benefits and overhead is an appropriate estimate based on research conducted by HHS.[427] Unless otherwise noted, we have consistently used the May 2021 National Occupational Employment and Wage Estimates reported by the U.S. Bureau of Labor Statistics (BLS) to calculate private sector employee wage estimates (*e.g.,* health IT developers, health care providers, HINs, attorneys, etc.), as we believe BLS provides the most accurate and comprehensive wage data for private sector positions.[428] Just as with the General Schedule Federal Salary Classification calculations, we have assumed that other indirect costs (including benefits) are equal to 100% of pre-tax wages. We welcome comments on our methodology for estimating labor costs.

Quantifying the Estimated Number of Health IT Developers and Products

In this section, we describe the methodology used to assess the potential impact of new certification requirements on the availability of certified products in the health IT market. This analysis is based on the number of health IT developers that certified Health IT Modules for the 2015 Edition and the estimated number of developers that will participate in the future and the number of products these developers will certify.

These estimations are based on observed and expected conformance to 2015 Edition Cures Update requirements, market consolidation, and other voluntary and involuntary withdrawals from the Program. In Table 6 below, we quantify the number of participating developers and certified products for the 2011 Edition, 2014 Edition, and 2015 Edition. We found that the number of health IT developers certifying products between the 2011 Edition and 2014 Edition decreased by 22.1% and the number of products available decreased by 23.2%. Furthermore, we found that between the 2014 Edition and 2015 Edition the number of developers and products decreased by 38.3% and 33.9%.

Table 6. Number of Developers and Products for the 2011 Edition, 2014 Edition, and 2015 Edition

---

[427] *See* U.S. Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation (ASPE), *Guidelines for Regulatory Impact Analysis,* at 28-30 (2016), *available at https://aspe.hhs.gov/reports/guidelines-regulatory-impact-analysis.*

[428] May 2021 National Occupational Employment and Wage Estimates, United States. U.S. Bureau of Labor Statistics. https://www.bls.gov/oes/current/oes_nat.htm

	2011 Edition	2014 Edition	Change (%)	2015 Edition	Change (%)
Health IT Developers	1,017	792	-22.1	489	-38.3
Products Available	1,408	1,081	-23.2	714	-33.9

Note: Counts for 2015 Edition reflect all certificates through 2021. These counts include certificates that are active and withdrawn.

We recognize that certification for 2015 Edition is ongoing and the number of health IT developers certifying products to the 2015 Edition is subject to change. The figures for 2015 Edition in Table 6 reflect certifications through 2021 to provide a fixed point for analysis. We have found it prudent to use certification data that represent entire calendar years, and not to use certification stats mid-year. Therefore, 2015 Edition counts do not account for all certificates as of the publication of this proposed rulemaking.

These figures give us insight into how participation in the Program and certification for individual certification editions has changed over time – the effect of both market and regulatory forces. Given historical trends and the asymmetric costs faced by developers of certified technology with large and small client bases, we must consider the effect of certification requirements going into effect and proposed in this rulemaking on future participation in the Program to make our best estimates of the cost and benefits of this proposed rulemaking.

Our proposed estimates of health IT developers and certified products specifically factor in a reduction in Program participation due to non-conformance with the 2015 Edition Cures Update criterion, *Standardized API for Patient and Population Services* ("*Standardized API* criterion"). The criterion replaces the 2015 Edition criterion, *Application Access – Data Category Request*. The *Data Category Request* criterion required no content exchange standard, although ONC communicated its intent to support a standard for future rulemaking and did encourage the use of the FHIR standard to meet criterion requirements. The new *Standardized API* criterion does require FHIR as a content exchange standard. Products that certified the *Data Category Request* criterion must certify the *Standardized API* criterion by December 31, 2022.

In the RIA for the ONC Cures Act Final Rule, we estimated that certified API products that did not support FHIR and must do so to meet regulatory requirements may face up to $1.9 million in development and other labor and maintenance costs to develop this technology for the first time (85 FR 25921). In 2018[429] and 2021[430] analyses, we found that support for FHIR was not common among 2015 Edition certified API products, although health IT market leaders predominantly supported the standard and used it as the content exchange standard for their certified API technology. As of the end of 2021, our analysis of certification data found that approximately 60% of certified API developers did not support FHIR as part of their certified API technology. Considering this variation in support for the standard under the 2015 Edition and the costs faced by health IT developers to meet this requirement, we expect some attrition from the Program.

Our model assumes that 1 in 4 certified API developers that do not currently support FHIR will not certify the *Standardized API* criterion and withdraw their certificates. This is based on available market data and the historical trend of developers with small client bases to exit the Program as program requirements and their costs increase. Our estimates may change as health IT developers meet 2015 Edition Cures Update requirements and developers certify the *Standardized API* criterion. We will update our model with this new data and will update relevant cost and benefit calculations in this RIA accordingly.

Table 7. Estimated Number of Developers and Products

Scenario	Estimated number of health IT developers	Estimated number of products
All Products - End of 2021	414	569
All Products - Modeled Attrition	368	502

Note: End of 2021 counts reflect active products only.

At the end of 2021, 414 health IT developers certified 569 products with active certificates for the 2015 Edition or 2015 Edition Cures Update. This is a 15% decrease in the number of health IT developers and a 20% decrease in 2015 Edition certified products, overall.

[429] https://www.healthit.gov/buzz-blog/interoperability/heat-wave-the-u-s-is-poised-to-catch-fhir-in-2019
[430] https://www.healthit.gov/buzz-blog/health-it/the-heat-is-on-us-caught-fhir-in-2019

Using our model of certification for the *Standard API* criterion, we estimate an additional 11% decrease in the number of health IT developers and a 12% decrease in the number of certified products. For this RIA, we will use 368 as the number of health IT developers and 502 as the number of certified health IT products impacted by proposed rulemaking. As already stated, these estimates are subject to change as more data become available.

Number of End Users That Might Be Impacted by ONC's Proposed Regulations

For the purpose of this analysis, the population of end users impacted are the number of health care providers that possess certified health IT. Due to data limitations, our analysis is based on the number of hospitals and clinicians who participate in Medicare and who may be required to use certified health IT to participate in various Medicare programs, inclusive of those providers who received incentive payments to adopt certified health IT as part of the Medicare EHR Incentive Program.

One limitation of this approach is that we are unable to account for the impact of our provisions on users of health IT that were ineligible or did not participate in the CMS EHR Incentive Programs or current Medicare performance programs. For example, in 2017, 78 percent of home health agencies and 66 percent of skilled nursing facilities reported adopting an EHR (https://www.healthit.gov/data/data-briefs/electronic-health-record-adoption-and-interoperability-among-us-skilled-nursing). Nearly half of these facilities reported engaging aspects of health information exchange. However, we are unable to quantify, specifically the use of certified health IT products, among these provider types.

Despite these limitations, these Medicare program participants represent an adequate sample on which to base our estimates. An analysis of the CMS Provider of Services file for Hospitals (https://data.cms.gov/provider-characteristics/hospitals-and-other-facilities/provider-of-services-file-hospital-non-hospital-facilities) and CMS National Downloadable File of Doctors and Clinicians (https://data.cms.gov/provider-data/dataset/mj5m-pzi6) provides a current accounting of Medicare-participating hospitals and practice locations. In total, we estimated

about 4,800 non-federal acute care hospitals from the Provider of Services file and 1.25 million clinicians (including doctors and advanced nurse practitioners) across over 350,000 practice locations. If we assume that 96% of these hospitals and 80% of these practice locations use certified health IT, as survey data estimate, approximately 4,600 hospitals and 283,000 practice locations may face some passed on costs from these proposals.

We understand there will likely not be a proportional impact of these costs across all health care providers. We can assume a hospital would face different costs than a physician practice, and no two hospitals would face the same costs, as those costs may vary based upon various characteristics, including but not limited to: staff size, patient volume, and ownership. The same is true for individual clinical practices, for which costs may vary across the same characteristics as hospitals. However, given our limited data, our proposed approach to model pass-through costs onto health care providers assumes that hospitals face the same average costs and that they face a higher average cost per site than an individual clinical practice. Furthermore, we assume that clinical practices face the same average costs and lower average costs per site than the average hospital.

Based upon our prior modeling work for the Cures Act Final Rule (https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification), we assume that one-third of estimated costs will be passed on to hospitals and the remaining amount on to clinician practices. Table 8 shows an assumed distribution of the costs across technology users. The cost to any one hospital or practice is small compared to the cost as a whole. The average hospital user of certified health IT could be expected to face up to $53,250 in average additional costs associated with implementing technology that adopt these proposals. The average clinician practice site could be expected to face up to $1,755 in average additional costs associated with implementing technology that adopt these proposals. These are considered pass-through costs

incurred by the health IT developer to adopt these proposals and not additional costs exogenous to health IT developer efforts to adopt and engineer these proposals into their certified health IT.

Table 8: Model of Cost Distribution Based on Estimated Number of Hospitals and Clinical Practices with Certified Health IT

Health Care Provider	Est. Count	Est. $ Per Provider	Total $ Cost
Hospitals	4,600	53,250	245m
Clinical Practices	283,000	1,755	497m
All	287,600	2,580	742m

One issue to reiterate is that some of these costs may have already been incorporated within existing contracts and thus it is possible that the actual additional costs experienced by hospitals and clinicians may be lower than what is estimated. We do not have insights into proprietary contracts between EHR developers and their clients, and thus cannot speculate the extent to which the estimated additional costs would be passed on to their clients.

It's unknown if the estimated benefits would have the same distribution. A single clinician may not benefit the same as a single hospital, nor would one hospital benefit the same as another. However, given the same constraints to model costs across different provider types, we must assume a similar distribution for benefits as we propose for costs.

"The ONC Certification Criteria for Health IT" and Discontinuing Year Themed "Editions"

As discussed in section III.A of this preamble, we propose to rename § 170.315 as the "ONC Certification Criteria for Health IT" and replace all references throughout 45 CFR part 170 to the "2015 Edition" with this new description (this would impact §§ 170.102, 170.405, 170.406, 170.523, 170.524, and 170.550).

Costs

This proposal is not intended to place additional burden on health IT developers and does not require new development or implementation. We expect the costs associated with attesting to these criteria to be de minimis because we do not expect any additional effort on the part of health IT developers. We welcome comments on these expectations.

Benefits

Maintaining a single set of "ONC Certification Criteria for Health IT" will create more stability for the health IT community and Program partners and make it easier for health IT developers of certified health IT to maintain their product certificates over time. For example, when new rules are released, unchanged certification criteria will remain exactly as they are, rather than being placed in a new CFR section and requiring health IT developers to seek an updated certificate attributed to the new CFR section. We welcome comments on this expectation and any potential approaches to quantifying these benefits.

United States Core Data for Interoperability Version 3 (USCDI v3)

As discussed in section III.C.1 of this preamble, we propose to update the USCDI standard in § 170.213 by adding the newly released USCDI v3 and by establishing an expiration date for USCDI v1 (July 2020 Errata) on January 1, 2025, for purposes of the Program. We propose to add USCDI v3 in § 170.213(b) and incorporate it by reference in § 170.299. We propose to codify the existing reference to USCDI v1 (July 2020 Errata) in § 170.213(a). We propose that as of January 1, 2025, any Health IT Modules seeking certification for criteria referencing § 170.213 would need to be capable of exchanging the data classes and data elements that comprise USCDI v3. Additionally, once the USCDI standard in § 170.213 is updated to include USCDI v3, we propose that in order for previously certified Health IT Modules to maintain certification, health IT developers would be required to update their certified Health IT Modules to be capable of exchanging the data classes and data elements that comprise USCDI v3 for all certification criteria referencing § 170.213 by December 31, 2024. USCDI, via cross-reference to § 170.213, is currently referenced in the following criteria, each of which would refer to USCDI v1 and USCDI v3 until December 31, 2024, and only to USCDI v3 thereafter, if we finalize our proposal:

- "Care coordination - Transitions of care - Create" (§ 170.315(b)(1)(iii)(A)(*1*));
- "Care coordination - Clinical information reconciliation and incorporation - Reconciliation" (§ 170.315(b)(2)(iii)(D)(*1*) through (*3*));

- "Patient engagement - View, download, and transmit to 3rd party - View" (§ 170.315(e)(1)(i)(A)(*1*));
- "Design and performance - Consolidated CDA creation performance" (§ 170.315(g)(6)(i)(A));
- "Design and performance - Application access – all data request – Functional requirements" (§ 170.315(g)(9)(i)(A)(*1*)); and
- "Design and performance - Standardized API for patient and population services – Data response" (§ 170.315(g)(10)(i)(A) and (B)).

We note that § 170.315(f)(5) also currently references § 170.213. However, we propose to rely on specific implementation guides for this certification criterion, rather than referencing § 170.213. As such, we do not expect Health IT Modules certified to § 170.315(f)(5) to certify using either USCDI v1 or USCDI v3 (through December 31, 2024) and USCDI v3 only after this date, if we finalize our proposal, as we do the above listed criteria.

Costs

The USCDI v3 adds five new data classes and 46 new data elements that were not in USCDI v1. This will require updates to the Consolidated Clinical Document Architecture (C-CDA) standard, the FHIR US Core Implementation Guide, and updates to the criteria listed above. We have estimated the proposed cost to health IT developers to add support for the additional data classes and data elements in USCDI v3 in C-CDA, and to make the necessary updates to the affected certification criteria. These estimates are detailed in Table 9 below and are based on the following assumptions:

1. Health IT developers will experience the assumed average costs of labor and data model use. Table 9 shows the estimated labor costs per product for a health IT developer to develop support for the additional data elements and data classes in USCDI v3 for each affected certification criteria. We recognize that health IT developer costs will vary; however, our

estimates in this section assume all health IT developers will incur, on average, the costs noted in Table 9.

2. We estimate that 346 products certified by 269 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above.

We estimate that, in total, 368 health IT developers will certify 502 health IT products impacted by this proposal. However, not all these developers and products certify USCDI applicable criteria and need to meet the USCDI update requirements. As of the end of 2021, 73% of developers and 69% of products certified to one of the USCDI applicable criteria, listed above. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the USCDI updates. In Table 10, we also applied separate modifiers for individual criteria, calculated from an analysis of certificates through 2021. This allows us to more accurately assess USCDI update costs for individual criteria.

3. According to the May 2021 BLS occupational employment statistics, the mean hourly wage for a "Software Developer" is $58.17. As noted previously, we have assumed that other indirect costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including other indirect costs is $116.

Table 9. Costs to Health IT Developers to Develop Support for the Additional USCDI Data Elements in C-CDA Standard and Affected Certification Criteria

Tasks	Details	Lower Bound Hours	Upper Bound Hours	Remarks
Update C-CDA creation	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C-CDA and C-CDA 2.1 Companion Guide	1,800	3,600	(1) Lower bound assumes health IT product was voluntarily updated through the ONC Standards Version Advancement Process (SVAP) and USCDIv2 data elements are incorporated in the certified product.

				(2) Upper bound assumes certified product conforms only to USCDIv1 and needs to be updated to fully conform with USCDIv3.
§ 170.315(b)(1)(iii)(A)(*1*) Care coordination – Transitions of Care - Create	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C-CDA and C-CDA 2.1 Companion Guide	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the criteria requirements.
§ 170.315(b)(2)(iii)(D)(*1*) through (*3*) Care coordination - Clinical information reconciliation and incorporation - Reconciliation	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C-CDA and C-CDA 2.1 Companion Guide	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the criteria requirements.
§ 170.315(e)(1)(i)(A)(*1*) Patient engagement - View, download, and transmit to 3rd party - View	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C-CDA and C-CDA 2.1 Companion Guide	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the criteria requirements.
§ 170.315(g)(6)(i)(A) Design and performance - Consolidated CDA creation performance	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C-CDA and C-CDA 2.1 Companion Guide	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the criteria requirements.

§ 170.315(g)(9)(i)(A)(*1*) Design and performance - Application access – all data request – Functional requirements	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C-CDA and C-CDA 2.1 Companion Guide	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the criteria requirements.
§ 170.315(g)(10)(i)(A) and (B) Design and performance - Standardized API for patient and population services – Data response	New development to support USCDI v2 and v3 updates and changes to data classes and constituent data elements for C-CDA and C-CDA 2.1 Companion Guide	200	600	Necessary updates to health IT to support the new data classes and data elements to meet the requirements.

Table 10. Total Cost to Develop Support for the Additional USCDI Data Elements in C-CDA Standard and Affected Certification Criteria [2021 dollars]

Tasks	Estimated number of products	Estimated Cost	
		Lower Bound	Upper Bound
Update C-CDA creation	346	$72,244,800	$144,489,600
Updates to § 170.315(b)(1)	281	$6,519,200	$19,557,600
Updates to § 170.315(b)(2)	261	$6,055,200	$18,165,600
Updates to § 170.315(e)(1)	246	$5,707,200	$17,121,600
Updates to § 170.315(g)(6)	341	$7,911,200	$23,733,600
Updates to § 170.315(g)(9)	276	$6,403,200	$19,209,600
Updates to § 170.15(g)(10)	276	$6,403,200	$19,209,600
Total Cost	346	$111,244,000	$261,487,200

Notes: The number of estimated products that certify applicable criteria vary. We estimated separate modifiers for each certification criterion to estimate the number of products impacted by the USCDI updates. Estimates reflect the percent of all products that certify a criterion through 2021, except. Modifiers: (b)(1): 56%; (b)(2): 52%; (e)(1): 49%%; (g)(6): 68%; (g)(9): 55%. This estimate is subject to change.

The cost to a health IT developer to develop support for the additional USCDI data classes and elements vary by the number of applicable criteria certified for a Health IT Module. On average, the cost to update C-CDA creation to support the additional USCDI data elements range from $208,8000 to $417,600 per product. The cost to make updates to individual criteria to support the new data classes and elements range from $23,200 to $69,600 per product. Therefore, assuming 346 products overall and a labor rate of $116 per hour, we estimate that the total cost to all health IT developers would, on average, range from $111 million to $262 million. This would be a one-time cost to developers per product that is certified to the specified certification criteria and would not be perpetual.

Benefits

We believe this proposal would benefit health care providers, patients, and the industry as a whole. The USCDI comprises a core set of structured and unstructured data needed to support patient care and facilitate patient access using health IT; establishes a consistent baseline of harmonized data elements that can be broadly reused across use cases, including those outside of patient care and patient access; and will expand over time via a predictable, transparent, and collaborative process, weighing both anticipated benefits and industry-wide impacts. In Standards Bulletin 2022-2,[431] we noted that based on these principles and the established prioritization criteria, USCDI v3 contains data elements whose collection and exchange promote equity, reduce disparities, and support public health data interoperability as discussed in Standards Bulletin 2021-3,[432] where we highlighted that the collection, access, use, and reporting of SDOH as well as sexual orientation and gender identity data can help identify and address differences in health equity and improve health outcomes at an individual and population level. The additional data elements in USCDI v3 expand the baseline set of data available for health information exchange and thus provide more comprehensive health data for both providers and

[431] https://www.healthit.gov/sites/default/files/page/2022-07/Standards_Bulletin_2022-2.pdf
[432] https://www.healthit.gov/sites/default/files/page/2021-07/Standards_Bulletin_2021-3.pdf

patients. We expect the resulting improvements to interoperable exchange of health information to significantly benefit providers and patients and improve the quality healthcare provided. In addition, we believe the increased availability of the additional data elements in USCDI v3 as interoperable structured data will facilitate improvements in the efficiency, accuracy, and timeliness of public health reporting, quality measurement, health care operations, and clinical research. However, we are not aware of an approach for quantifying these benefits and welcome comments on potential approaches to quantifying these benefits.

Electronic Case Reporting

In section III.C.4 of this preamble, we propose updates to the 2015 Edition certification criterion for "*Transmission to public health agencies – electronic case reporting*" that would require health IT developers of certified health IT to adopt specific electronic standards to support functional requirements that were previously adopted as part of the § 170.315(f)(5) certification criterion. We propose that Health IT Modules certified to this criterion must enable a user to: (i) create an electronic initial case report (eICR) according to at least the Health Level Seven (HL7) Clinical Document Architecture (CDA) eICR implementation guide (IG) or the eICR profiles defined in the HL7 Fast Health Interoperability Resources (FHIR) eCR IG; (ii) consume and process a reportability response (RR) according to at least the HL7 CDA RR IG or the RR profiles defined in the HL7 FHIR eCR IG, and (iii) consume and process an electronic Reporting and Surveillance Distribution (eRSD) Bundle according to the eRSD profiles defined in the HL7 FHIR eCR IG. For the standards-based requirements in § 170.315(f)(5)(i) through (iii), we propose that Health IT Modules support all "mandatory" and "must support" data elements as applicable in the respective implementation guides (IGs). We also propose that Health IT Modules support the use of a version of the Reportable Conditions Trigger Code (RCTC) value set in § 170.315(f)(5)(1)(B) for determining potential case reportability.

Costs

This section describes the estimated costs of meeting the requirements in the updated "*Transmission to public health agencies – electronic case reporting*" criterion. The cost estimates are based on the following assumptions:

- *Health IT developers will experience the assumed average costs of labor and data model use.* Tables 11-12 show the estimated labor costs per product for a health IT developer to meet the requirements in the eCR certification criterion. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will, on average, incur the costs noted in the tables below.
- *The number of products that will update to the new eCR criterion is estimated based on the total number of currently certified products plus the number of new products we expect to certify to the eCR criterion.* Both estimates are adjusted for attrition. As of 2021, 54 developers certified 63 products to the eCR certification criterion or 13% of developers and 11% of products. Beginning in 2022, CMS required eligible hospitals and critical access hospitals in the Medicare Promoting Interoperability Program and eligible clinicians reporting on the Promoting Interoperability performance category in MIPS to report on use of eCR as part of the Public Health and Clinical Data Exchange Objective. The Electronic Case Reporting measure was optional in prior program years. Due to this new program requirement, we expect more Health IT Modules to certify the criterion in the coming year(s). As a proxy for possible future certification of eCR, we used the number of products that are currently certified to § 170.315(f)(1) (transmission to immunization registries) to estimate future certification of the eCR criterion. As of 2021, 31% of developers and 28% of products certified to the *Immunization* criterion, but not the eCR certification criterion. We used these rates to estimate future certification of the eCR criterion. We estimate that 368 developers will certify 502 products impacted by this rulemaking. We estimate updates to the eCR certification criterion will impact 141 products certified by 114 developers for the first time ("New") and 55 products already

certified by 48 developers ("Current") for an estimated total of 196 products certified by 162 developers.

- *Wages are determined using BLS estimates.* According to the May 2021 BLS occupational employment statistics, the mean hourly wage for a "Software Developer" is $58.05.[433] We assume that other indirect costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage, including other indirect costs, is $116.

Table 11. Estimated Labor Hours to Meet eCR Certification Requirements – New Products

Activity	Details	Estimated Labor Hours		Remarks
		Lower bound	Upper bound	
Task 1: Case Report Creation	(1) Enable a user to create a case report for electronic transmission according to (i) eICR profiles of HL7 FHIR eCR IG, or (ii) HL7 CDA eICR IG; (2) Support RCTC value set	1,000	1,500	(1) Lower bound assumes health IT product has begun to implement at least one of the two IGs. (2) Upper bound assumes health IT product does not support either IG and has not begun to implement.
Task 2: Case Report Response Receipt	Health IT Module must be able to consume and process a reportability response according to (1) RR profiles of HL7 FHIR eCR IG, or (2) HL7 CDA RR IG	1,000	1,500	(1) Lower bound assumes health IT product has begun to implement at least one of the two IGs. (2) Upper bound assumes health IT product does not support either IG and has not begun to implement.
Task 3: Support eRSD	Health IT Module must be able to consume and process an eRSD Bundle according to the eRSD profiles as specified in the HL7 FHIR eCR IG	0	1,500	(1) Lower bound assumes health IT product has begun to implement IG profile natively or is already using eCR Now to support this requirement. (2) Upper bound assumes health IT product is not using any solution (i.e., does not support IG profile and has not begun to implement the profile or use eCR Now).
Task 4: Support for Reporting	Health IT Module must be able to report to a system capable of receiving case reports electronically	0	160	(1) Lower bound assumes that health IT already has the technical pre-requisites for reporting but is not yet connected to platform or method to enable reporting. (2) Upper bound assumes health IT does not have

[433] https://www.bls.gov/oes/current/oes_nat.htm

				technical pre-requisites for reporting (e.g., no support for electronic connection and no support for available exchange methods).

Table 12. Estimated Labor Hours to Meet eCR Certification Requirements – Currently Certified Products

Activity	Details	Estimated Labor Hours		Remarks
		Lower bound	Upper bound	
Task 1: Case Report Creation	(1) Enable a user to create a case report for electronic transmission according to (i) eICR profiles of HL7 FHIR eCR IG, or (ii) HL7 CDA eICR IG; (2) Support RCTC value set	0	1,000	(1) Lower bound assumes health IT product has already implemented at least one of the two IGs. (2) Upper bound assumes health IT product has begun to implement at least one of the two IGs.
Task 2: Case Report Response Receipt	Health IT Module must be able to consume and process a reportability response according to (1) RR profiles of HL7 FHIR eCR IG, or (2) HL7 CDA RR IG	0	1,000	(1) Lower bound assumes health IT product has already implemented at least one of the two IGs. (2) Upper bound assumes health IT product has begun to implement at least one of the two IGs.
Task 3: Support eRSD	Health IT Module must be able to consume and process an eRSD Bundle according to the eRSD profiles as specified in the HL7 FHIR eCR IG	0	1,500	(1) Lower bound assumes health IT product has begun to implement IG profile natively or is already using eCR Now to support this requirement. (2) Upper bound assumes health IT product is not using any solution (i.e., does not support IG profile and has not begun to implement the profile or use eCR Now).
Task 4: Support for Reporting	Health IT Module must be able to report to a system capable of receiving case reports electronically	0	160	(1) Lower bound assumes health IT already supports at least one reporting option, such as to the AIMS platform, state-based registries or health information exchanges. (2) Upper bound assumes health IT does not have technical pre-requisites for reporting (e.g., no support for electronic connection and no support for available exchange methods).

Total Costs, *TC* can be represented by the following equation:

$$TC = p_c\left[\sum_{k=1}^{3} h_k w + h_r w\right] + p_n[\sum_{k=1}^{3} h_k w + h_r w]$$

Number of currently certified products, $p_c = 55$
Number of new certified products, $p_n = 141$
Fully loaded wage, $w = \$116$
Labor hours for IG implementation, h_k, for each profile or IG, k
Labor hours for reporting, h_r

Table 13. Example Calculation for the Lower Bound Estimated Cost to New Products to Perform Task 1 in Table 11 to Meet eCR Certification Requirements

Activity	Estimated labor hours	Developer Salary	Projected products
	Lower bound		
Task 1	1,000 hours	$116 per hour	141 products
Example Calculation: 1,000 hours * $116 * 141 products = $16,356,000			

Table 14. Costs to Meet eCR Certification Requirements – New Products

Activity	Estimated Labor Hours	
	Lower bound	Upper bound
Task 1 (141 products)	$16,356,000	$24,534,000
Task 2 (141 products)	$16,356,000	$24,534,000
Task 3 (141 products)	$0	$24,534,000
Task 4 (141 products)	$0	$2,616,960
Total Cost	$32,712,000.00	$76,218,960.00

Table 15. Costs to Meet eCR Certification Requirements – Currently Certified Products

Activity	Estimated Labor Hours	
	Lower bound	Upper bound
Task 1 (55 products)	$0	$6,380,000
Task 2 (55 products)	$0	$6,380,000
Task 3 (55 products)	$0	$9,570,000
Task 4 (55 products)	$0	$1,020,800

Total Cost	$0	$23,350,800.00

Table 16. Costs to Meet eCR Certification Requirements – All Products

Activity	Estimated Labor Hours	
	Lower bound	Upper bound
Task 1 (196 products)	$16,356,000	$30,914,000
Task 2 (196 products)	$16,356,000	$30,914,000
Task 3 (196 products)	$0	$34,104,000
Task 4 (196 products)	$0	$3,637,760
Total Cost	**$32,712,000**	**$99,569,760**

Based on the stated assumptions and costs outlined in Tables 14-16, the total estimated cost for certified health IT products to meet the proposed eCR certification criterion requirements will range from $32.7 million to $99.6 million. Assuming 162 health IT developers, there would be an average cost per developer ranging from $201,926 to $614,628, with an average cost per product ranging from $232,000 to $540,560 for new products and $0 to $424,560 for currently certified products.

Benefits

The primary benefit of adopting standards-based requirements for the eCR certification criterion is to improve consistency and promote interoperability over time. eCR is one of the pillars of ONC's and CMS' broader efforts to support effective healthcare data interoperability, which ensures that electronic health information is shared appropriately between healthcare organizations and public health agencies (PHAs) in the right format, through the right channel at the right time.[434] Adopting a standards-based approach to eCR facilitates the exchange of health information between healthcare and public health by requiring the use of a common format for the creation of case reports and processing of a reportability response.

[434] https://www.cdc.gov/datainteroperability/index.html

Potential benefits of a centralized approach to eCR have been assessed in an Association of State and Territorial Health Officials (ASTHO)-sponsored economic analysis of the efficiencies gained at PHAs by using centralized eCR services through the Association of Public Health Laboratories (APHL) Informatics Messaging Services (AIMS) platform, rather than using localized eCR solutions or manual, paper-based methods.[435] A key component of this service is the inclusion of the CDC supported Council of State and Territorial Epidemiologists' (CSTE) developed decision support tool, Reportable Condition Knowledge Management System (RCKMS), which helps determine whether initial case reports are reportable in specific public health jurisdictions and eliminates confusion regarding where reports should be sent.[436,437] According to the analysis, centralized eCR components could provide, "$2.5 million in increased efficiency per jurisdiction over 15 years" compared to manual reporting and "$310,000 of net benefits over 15 years" compared to localized eCR solutions.[438]

Benefits of eCR to the healthcare sector and public health that would be promoted through standards adoption:

- Automatic, complete, accurate data reported in real-time (faster and more complete than manual entry) facilitates evidence-based decision-making for public health.
- Directly benefits public health response efforts by supporting situational awareness, case management, contract tracing, and efforts to coordinate isolation.
- Helps improve public health efficiency for evaluation and follow-up by providing PHAs with higher quality patient and clinical data in a timely manner.
- Reduces reporting burden for health care providers without disrupting clinical workflow, which can result in time and cost savings for the healthcare sector.

---

[435] https://www.aphl.org/programs/informatics/Pages/aims_platform.aspx
[436] CSTE Surveillance/Informatics: Reportable Conditions Knowledge Management Systems. CSTE Web site. http://www.cste.org/
group/RCKMS.
[437] https://ecr.aimsplatform.org/cms/resources/blocks/digital-bridge-ecr-evaluation-report-12-32019.pdf
[438] Cooney MA, Iademarco MF, Huang M, MacKenzie WR, Davidson AJ. The public health community platform, electronic case reporting, and the digital bridge. Journal of Public Health Management and Practice. 2018 Mar 1;24(2):185-9.

- Fulfills legal reporting requirements as well as CMS PI Program requirements for eCR, meaning benefits to public health would not come at an additional cost to health care providers who are already required to report.
- Streamlines reporting to multiple jurisdictions.

Benefits of certification criterion update:

- Adoption of standards for eCR will improve consistency and interoperability over time.
- Consistency in the reporting of specific data elements will increase the efficiency of exchange (e.g., by facilitating automated reporting, enabling RCKMS and PHA processing of eICRs and bi-directional communication between providers and public health).
- RCTC value set establishes a baseline for use in the Program and enables health IT developers of certified health IT to support newer or updated versions of RCTC value sets as soon as new releases are available.

Decision Support Interventions and Predictive Models

We propose, in section III.C.5 of this preamble, a new certification criterion for "*decisions support interventions*" in § 170.315(b)(11). The intent of this certification criterion is to ensure the availability of sufficient information on decision support interventions based on predictive models, including machine learning and artificial intelligence, through a more comprehensive list of source attributes and through the conduct and documentation of risk management activities. That information is intended to enable selection and use of fair (i.e., unbiased), appropriate, valid, and effective interventions. The certification criterion also would provide additional transparency into evidence-based decision support interventions by requiring that products allow CDS to be enabled based on specific data classes.

Without such a certification criterion we are concerned that limited and asymmetric information will lead to the use of inaccurate, harmful, and biased models, and current evidence

indicates that such undesirable use is already occurring widely.[439] We are further concerned that without requirements for more complete information on predictive models, the market for such models will not develop adequately.

Alternatives Considered

We considered several alternative regulatory approaches but believe this approach implies the lowest burden of available options while having a high likelihood of impacting decision-making. Because we seek to address a market failure related to inadequate and asymmetric information, we propose an informational intervention. The approach is market-oriented and aimed at ensuring that model purchasers and users have sufficient information to select and use models responsibly. We believe that several alternative approaches, such as performance or design standards would imply substantially higher regulatory burden and are inappropriate given the ongoing research and development in this area and uncertainty inherent in predictive model development.

Rather than mandatory reporting, we considered the potential for a voluntary database to which model developers might report information on the quality of their models. However, we are concerned that such a database would achieve relatively low participation because of disincentives for some developers to make the performance of their models public. We believe that the current approach in which we have required reporting of a set of core source attributes that we strongly believe should be available for all models (e.g., intended use) and reporting of other attributes (e.g., external validation results) as required if available but otherwise providing the option to clearly label as missing, is a more effective balance between prescriptive requirements and voluntary participation. We request public comment on the burden associated with the required source attributes and risk management information.

---

[439] See, for instance, Ziad Obermeyer, et al., *Dissecting racial bias in an algorithm used to manage the health of populations*, 366 SCIENCE (2019). And Wong et al. External Validation of a Widely Implemented Proprietary Sepsis Prediction Model in Hospitalized Patients. *JAMA Intern Med.* 2021;181(8):1065–1070. doi:10.1001/jamainternmed.2021.2626. And Murray, Sara G., Robert M. Wachter, and Russell J. Cucina. "Discrimination by artificial intelligence in a commercial electronic health record—a case study." Health Affairs Blog 10 (2020).

Given the national availability of many models, Federal regulation is beneficial to set a common set of expectations across the national market.

Costs

This section describes the estimated costs of the "Predictive Decision Support" certification criterion. The cost estimates are based on the following assumptions:

- *Health IT developers will experience the assumed average costs of labor and data model use.* Table 17 shows the estimated labor costs per product for a health IT developer to develop support for the predictive decision support certification criterion. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will, on average, incur the costs noted in Table 17.
- *The number of health IT developers and products certified will closely align with certification of the 2015 Edition clinical decision support (CDS) criterion.* We estimate that 301 products certified by 243 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above. We estimate that, in total, 368 health IT developers will certify 502 health IT products impacted by this rulemaking. However, we estimate not all these developers and products will certify the new *Predictive Decision Support* criterion. As of the end of 2021, 66% of developers and 60% of products certified to the *CDS* criterion. We assume that all products certified to the *CDS* criterion will certify the new *Predictive Decision Support* criterion. We, therefore, use certification of the *CDS* criterion as a proxy for the percent of developers and products that will certify the *Predictive Decision Support* criterion in the future. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products that will certify this criterion and be impacted by the costs of this new criterion. We further estimate that not all products certified to *CDS* criterion will attest to the portion of the new criterion supporting predictive decision support interventions and therefore will not

be required to complete some tasks associated with the new criterion. We estimate that 75% of developers will attest to supporting predictive decision support interventions and request comment on this estimate.

- *Wages are determined using BLS estimates.* According to the Bureau of Labor and Statistics,[440] the median hourly wage for a "Software Developer" is $58.17. As noted previously, we have assumed that other indirect costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including other indirect costs is $116.

Table 17. Estimated Labor Hours to Develop and Maintain Updated Decision Support Functionality.

Activity	Lower bound hours	Upper bound hours	Remarks
Task 1: Update CDS tools to enable interventions based on additional data classes and report on use of specific data classes	1,000	2,000	(1) Lower bound assumes health IT already has developed CDS modules that only need to be updated for new data classes. (2) Upper bound assumes further data-structure related work is necessary to facilitate CDS based no additional classes.
Task 2: Enable end-users to provide feedback on CDS and reports on that feedback.	200	1,000	(1) Lower bound assumes that developers have already developed feedback capabilities and will need to make limited updates to the reporting of that information. (2) Upper bound assumes that developer's current capability to support feedback on CDS needs to be significantly enhanced to support enabling end-users to provide effective feedback and to create reports from that feedback.
Task 3: Provide users the ability to review, revise and author additional source attributes.	1,000	2,000	(1) Lower bound assumes that existing tools used to create similar forms or documents can be adapted to this purpose. (2) Upper bound assumes a higher burden due to more novel development.
Task 4: Provide information for additional source attributes related to predictive decision support intervention.	200	6,000	We expect a wide range of effort based on the extent to which EHR developers currently make CDS available and whether they make predictive decision support interventions available. For those that do enable predictive decision support interventions and do not currently evaluate the models on

[440] https://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm

			the attributes included, we believe doing so will imply substantial costs.
Task 5: Describe risk management information	230	570	The total hours estimated to conduct real-world testing per developer were 1,140 and that accounted for numerous criteria included as eligible for real world testing. We believe that conducting intervention risk management for (b)(11), including the provision of risk management documentation, would require a fraction of that time equivalent to between one fifth and one half the time.

We request comment on the estimated number of hours associated with each task. In particular, we request comment on the range of hours associated with Task 4 and Task 5, which we believe will vary greatly depending on the number and types of models that developers include or interface with their products. Estimating the relevant time for these tasks is a challenge because there is limited information regarding the extent to which developers' current practices fall short of the proposed requirements.

Table 18. Total Cost to Developers to Develop and Maintain Updated Decision Support Functionality.

	Projected Products	Notes	Estimated Total Cost (10 year) (Assuming Software Developer pay of $58.17 per hour Software Developers (bls.gov))	
			Lower bound	Upper bound
Task 1	301	Developers certified to (a)(9) as of 4/15/2022	$ 35,018,340	$ 70,036,680
Task 2	301	Developers certified to (a)(9) as of 4/15/2022	$ 6,381,200	$ 35,018,340
Task 3	226	Assuming approximately 75% enable predictive decision support interventions	$ 23,956,000	$ 52,585,680
Task 4	226	Assuming approximately 75% enable predictive decision support interventions	$ 5,258,568	$ 157,757,040
Task 5	301	Developers certified to (a)(9) as of 4/15/2022	$ 8,054,218	$ 19,960,454
Total			$ 81,627,634	$ 335,358,194

We request comment on the estimate included above that 75% of developers of products that are currently certified to § 170.315(a)(9) and will be certified to § 170.315(b)(11) include predictive decision support interventions.

Benefits

Predictive decision support interventions are common, with some individual interventions being applied to tens or hundreds of millions of individuals despite, in some cases, crucial insufficiencies in the performance of those models.[441] However, there are a wide range of potential applications of predictive decision support interventions, and we believe that the healthcare delivery field is far from fully adopting these interventions in the circumstances where they would be beneficial. Because predictive decision support interventions are being and potentially could be applied to a wide range of contexts, comprehensively estimating quantitative benefits from improved interventions and underlying models is challenging and, for some types of benefits, infeasible. However, we have generated some quantitative benefits related to the scope of potential cost savings and have identified additional benefits, characterized qualitatively, to the proposed certification criterion.

We believe that the most directly quantifiable benefits of the proposed changes to predictive decision support relate to increased use of more accurate and effective predictive decision support interventions.[442] We believe that increased transparency into the performance of models and risk management practices related to their development would result in (1) wider uptake of predictive decisions support interventions overall due to greater certainty about the intervention's performance, and (2) selection of fairer, more appropriate, more accurate, more effective and safer models through greater information on the available choices. However, we

---

[441] Ziad Obermeyer, et al., *Dissecting racial bias in an algorithm used to manage the health of populations*, 366 SCIENCE (2019).
Andrew Wong, et al., *External validation of a widely implemented proprietary sepsis prediction model in hospitalized patients*, 181 JAMA INTERNAL MEDICINE (2021).
THE JOHNS HOPKINS ACG® SYSTEM, *available at* https://www.johnshopkinssolutions.com/wp-content/uploads/2016/08/ACG-System-Brochure.pdf.
[442] https://www.healthit.gov/buzz-blog/health-innovation/back-to-the-future-what-predictive-decision-support-can-learn-from-deloreans-and-the-big-short

acknowledge that there is substantial uncertainty in the degree to which the proposal would result in wider uptake and use of more effective interventions.

Given the sheer number of algorithms and applicable conditions and uses, we have selected two relevant scenarios—sepsis onset and ambulatory care sensitive admission--which have a fair amount of supporting research, to show the potential benefits of our proposal. First, in patient populations in whom the risk of sepsis is moderate to high, risk-assessments based on patient factors and characteristics (i.e., data elements) are (or should be) made for implementing rapid risk-based patient care. The potential impact of using predictive decision support interventions to more effectively conduct these risk-assessments can illustrate the benefits. Admissions for sepsis cost $24 billion per year;[443] and early detection of sepsis can lead to interventions that dramatically reduce those costs. However, advanced predictive decisions support interventions for the identification of sepsis are not widely used and instead older models, such as Sequential Organ Failure Assessment (SOFA), are dominant.[444]

Existing evidence indicates that more advanced predictive models can provide substantial performance improvements over simpler, widely used models.[445] The potential benefits of more advanced models are large. A prospectively evaluated sepsis predictive decision support intervention decreased in-hospital mortality related to sepsis by 39.5%, decreased length of stay by 32.3% and decreased readmission by 22.7% in one clinical trial.[446] However, there is also substantial uncertainty about whether models will offer that benefit when implemented on a broad scale. Performance of the same model evaluated in that clinical trial was substantially

---

[443] Epidemiology and Costs of Sepsis in the United States—An Analysis Based on Timing of Diagnosis and Severity Level* - PMC (nih.gov)
[444] J-L Vincent, et al., The SOFA (Sepsis-related Organ Failure Assessment) score to describe organ dysfunction/failure (Springer-Verlag 1996).
[445] As one example of a study demonstrating clear accuracy improvements over widely used, simpler models see Ryan J Delahanty, et al., *Development and evaluation of a machine learning model for the early identification of patients at risk for sepsis*, 73 ANNALS OF EMERGENCY MEDICINE (2019).
[446] Burdick, Hoyt, et al. "Effect of a sepsis prediction algorithm on patient mortality, length of stay and readmission: a prospective multicentre clinical outcomes evaluation of real-world patient data from US hospitals." BMJ health & care informatics 27.1 (2020).

lower in a separate evaluation,[447] and that difference may be attributable to difference in performance in varied deployments and locations.

Transparency has the potential to shed light on the variation in performance across models and to drive uptake of higher performing models. A systematic review of predictive models designed to detect early onset of sepsis found that published evaluations demonstrated sensitivities ranging from 64% to 98%.[448] One sepsis model that was recently widely adopted was found in subsequent validation to have relatively poor performance with a sensitivity of 33%. This again highlights the potential value of greater information to evaluate these models.[449]

Given the heterogeneity in the literature, it is challenging to estimate the extent to which the availability of information that would be facilitated by our proposal would impact the average quality of predictive models used or how that average quality will evolve over time. Because models often perform less effectively in real-world implementation than in test environments, we believe the likely impact would be smaller than that implied by the literature but believe an impact on the average sensitivity of models used of 5 percentage points is reasonable. We note that in the cited systematic review, the median sensitivity of included models was 81% so that our assumption is that with the rule in place median sensitivity of available models would increase by 5 percentage points to 86%. Based on cost savings indicated in the available literature, we estimate that early detection of onset would result in cost savings of 50% for the incrementally more commonly detected patient event. We request comment on these estimates.

Beyond increases in the accuracy and effectiveness of models used, it is also challenging to estimate the extent to which the proposed certification criterion would result in increased use

---

[447] Topiwala, Raj, et al. "Retrospective observational study of the clinical performance characteristics of a machine learning approach to early sepsis identification." *Critical Care Explorations* 1.9 (2019).
[448] Hassan, Nehal, et al. "Preventing sepsis; how can artificial intelligence inform the clinical decision-making process? A systematic review." *International Journal of Medical Informatics* 150 (2021): 104457.
Makam, Anil N., Oanh K. Nguyen, and Andrew D. Auerbach. "Diagnostic accuracy and effectiveness of automated electronic sepsis alert systems: a systematic review." *Journal of hospital medicine* 10.6 (2015): 396-402.
[449] Wong, Andrew, et al. "External validation of a widely implemented proprietary sepsis prediction model in hospitalized patients." *JAMA Internal Medicine* 181.8 (2021): 1065-1070.

of more accurate decision support interventions. Findings on other transparency related public policies, such as nutrition labels, indicate that use of labels can have substantial impacts on consumers choices.[450] While these findings indicate a likely increase in use of interventions from transparency related policies, we believe it is difficult to transfer these findings to the specific case of predictive decision support interventions. For the purpose of this proposal, we are assuming that the proposal would relate to application of improved models (with an average increased sensitivity of 5%) by 2% a year beginning in the year that requirements commenced.

Another example we wish to highlight besides sepsis is the use of models to identify patients at risk for ambulatory sensitive conditions. Such conditions result in costs of $33.7 billion (bn) per year.[451] As in the sepsis example, there are several existing predictive models, and they exhibit a wide range accuracy.[452] We therefore believe it is reasonable to apply the estimates used in the prior example related to sepsis onset to estimate potential benefits related to ambulatory care sensitive admissions. Given substantial differences in the sensitivity of models intended to identify patients at risk of ambulatory sensitive admissions, we believe this assumption is reasonable.[453]

We estimate all benefits on a 10-year time horizon. Because health IT developers of certified health IT with Health IT Modules certified to the existing certification criterion in § 170.315(a)(9) would not be required to certify to the proposed criterion in § 170.315(b)(11) until 2024, we note that benefits would not commence until the third year. We believe that time period allows sufficient time for the full impact of the proposal to take effect, including developer certification to the criterion, publication of risk management information, and hospital resorting

---

[450] For examples, see Joanne F Guthrie, et al., *Who uses nutrition labeling, and what effects does label use have on diet quality?*, 27 JOURNAL OF NUTRITION EDUCATION (1995);Marian L Neuhouser, et al., *Use of food nutrition labels is associated with lower fat intake*, 99 JOURNAL OF THE AMERICAN DIETETIC ASSOCIATION (1999).
[451] https://www.hcup-us.ahrq.gov/reports/statbriefs/sb259-Potentially-Preventable-Hospitalizations-2017.jsp
[452] Emma Wallace, et al., *Risk prediction models to predict emergency hospital admission in community-dwelling adults: a systematic review*, 52 MEDICAL CARE (2014).
Seung Eun Yi, et al., *Predicting hospitalisations related to ambulatory care sensitive conditions with machine learning for population health planning: derivation and validation cohort study*, 12 BMJ OPEN (2022).
[453] Garcia-Arce, Andres, Florentino Rico, and José L. Zayas-Castro. "Comparison of machine learning algorithms for the prediction of preventable hospital readmissions." *The Journal for Healthcare Quality (JHQ)* 40.3 (2018): 129-138.

into improved predictive models. We expect that the use of predictive models in healthcare will continue to evolve well beyond that time horizon; however, given the dynamic and uncertain nature of this area, we do not believe it would be appropriate to provide estimates beyond that period.

We examined the sensitivity of our estimated benefits based on uncertainty in the underlying rates. We varied two rates: the average increase in the sensitivity of models used and the increased rate at which more accurate models were used. Specifically, we recalculated benefits with an assumed sensitivity increase of 2.5%, 5% or 10% (with 5% representing our primary estimate) and an assumed increase in application of models of 1%, 2% and 3% (with 2% representing our primary estimate). In these analyses, we estimated that the 10-year undiscounted incremental impacts ranged from $259,650,000 to $3,115,800,000. We also estimated the annualized benefits of the incremental impacts using alternative modeling assumptions and present them in Table 20.

Table 19. Select Benefits to Patients and Payers from Updated Decision Support Functionality.

Year Impacts are Incurred	Cost of Sepsis Admission	Proportion of admissions for which more sensitive model used	Increased Sensitivity of Models Used	Assumed Costs Saved for Impacted Admissions	Incremental Impacts (undiscounted)*	Incremental Impacts (7% discount)	Incremental Impacts (3% discount)	
1						$0.00	$0.00	
2						$0.00	$0.00	
3	$24bn	**0.02**	**0.05**	**0.5**	$12,000,000	$9,795,575	$10,981,670	
4	$24bn	**0.04**	**0.05**	**0.5**	$24,000,000	$18,309,485	$21,323,689	
5	$24bn	**0.06**	**0.05**	**0.5**	$36,000,000	$25,667,502	$31,053,916	
6	$24bn	**0.08**	**0.05**	**0.5**	$48,000,000	$31,984,427	$40,199,244	
7	$24bn	**0.1**	**0.05**	**0.5**	$60,000,000	$37,364,985	$48,785,491	
8	$24bn	**0.12**	**0.05**	**0.5**	$72,000,000	$41,904,656	$56,837,465	
9	$24bn	**0.14**	**0.05**	**0.5**	$84,000,000	$45,690,434	$64,379,006	
10	$24bn	**0.16**	**0.05**	**0.5**	$96,000,000	$48,801,532	$71,433,016	
Total					$432,000,000.00	**$259,518,595**	**$344,993,527**	**PV**
						$36,949,610	**$40,443,766**	**Ann**

Year Impacts are Incurred	Cost of Ambulatory Sensitive Admission	Proportion of admissions for which more sensitive model used	Increased Sensitivity of Models Used	Assumed Costs Saved for Impacted Admissions	Incremental Impacts (undiscounted)*	Incremental Impacts (7% discount)	Incremental Impacts (3% discount)	
1								
2								
3	33.7bn	**0.02**	**0.05**	**0.5**	$16,850,000	$13,754,619	$15,420,136	
4	$33.7bn	**0.04**	**0.05**	**0.5**	$33,700,000	$25,709,569	$29,942,014	
5	$33.7bn	**0.06**	**0.05**	**0.5**	$50,550,000	$36,041,451	$43,604,874	
6	$33.7bn	**0.08**	**0.05**	**0.5**	$67,400,000	$44,911,466	$56,446,439	
7	$33.7bn	**0.1**	**0.05**	**0.5**	$84,250,000	$52,466,666	$68,502,960	
8	$33.7bn	**0.12**	**0.05**	**0.5**	$101,100,000	$58,841,120	$79,809,274	
9	$33.7bn	**0.14**	**0.05**	**0.5**	$117,950,000	$64,156,985	$90,398,854	
10	$33.7bn	**0.16**	**0.05**	**0.5**	$134,800,000	$68,525,485	$100,303,860	
Total					$606,600,000	**$364,407,361**	**$484,428,410**	**PV**
						$51,883,410	**$56,789,788**	**Ann**

Table 20. Select Benefits from Updated Decision Support Functionality Under Alternative Assumptions, $ Millions, Annualized, 3% Discount Rate

		Impact on Model Sensitivity		
		2.50%	5%	10%
Impact on Annual Model Application	1%	$24.3	$48.6	$97.2
	2%	$48.6	$97.2	$194.5
	3%	$72.9	$145.9	$291.7

We have highlighted one condition and one event that would benefit from the more widespread use of more accurate predictive models under the proposed rule. There are numerous other conditions and events in which increased sensitivity could offer substantial cost savings. However, given uncertainty in the estimates around the included estimates, and important differences across various conditions and the extent to which predictive decision support interventions might impact care, we are not confident that the assumptions generated here are transferable to other contexts.

We invite public comment on the extent to which these two use cases might relate to other use cases. We further invite public comment on additional benefits for which commenters believe there is an existing literature suitable to estimate potential benefits.

In addition to benefits associated with more sensitive models, we believe that there are numerous other potential benefits related to the more widespread use of more accurate predictive decisions support. However, many of the benefits associated with greater accuracy, and in particular more specific models, such as reduced inappropriate treatment or reduced burdens on providers are difficult to quantify and have, to date, been targeted by fewer predictive models. As salient examples, we note that false-positives for screening for breast cancer alone is associated with $4 bn per year and that more specific interventions could reduce the rates of false positive.[454] We further note that provider burnout and fatigue are important and costly issues, we believe these benefits may be large.[455] However, since we are aware of fewer estimates around the potential impact of predictive decision support interventions to address these issues, we have not attempted to quantify the potential benefits associated with their use.

Beyond the benefits associated with greater use of accurate models, we believe there would be several other important benefits associated with the proposed transparency requirements. We believe that increased transparency into the intended use of models would increase the appropriate use of models. There is concern that models will be applied to populations, contexts or decisions for which they are not well suited to provide accurate information.[456] Effective, transparent display of the intended and out of scope use could reduce incidence of treatment decisions resulting in harm. However, we are not aware of efforts to quantify harm from misapplied models today.

We believe increased transparency into models and practices would result in the selection and use of fairer models. Biased models are likely to deprioritize treatment for certain groups while also being more likely to recommend inappropriate treatment for those groups resulting in limited benefit and potential harm to some groups relative to those for whom models perform

---

[454] Ong, Mei-Sing, and Kenneth D. Mandl. "National expenditure for false-positive mammograms and breast cancer overdiagnoses estimated at $4 billion a year." *Health affairs* 34.4 (2015): 576-583.
[455] Gregory, Megan E., Elise Russo, and Hardeep Singh. "Electronic health record alert-related workload as a predictor of burnout in primary care providers." *Applied clinical informatics* 8.03 (2017): 686-697.
[456] Richard Ribón Fletcher, et al., *Addressing fairness, bias, and appropriate use of artificial intelligence and machine learning in global health*, 3 FRONTIERS IN ARTIFICIAL INTELLIGENCE (2021).

well. Greater transparency into the fairness of models would enable model users to select fairer models and reward producers of fairer models. This would lead to the selection of models that further rather than hinder the equitable delivery of healthcare to groups that have been marginalized. We request comment on the feasibility of quantitating benefits associated with increased model fairness, which may be identifiable through increased benefits to groups that have been marginalized.

We believe that increased transparency would lead to a better functioning market for predictive models that adequately incentivizes and rewards high quality models. In the current state, model developers have an information advantage relative to consumers, and consumers of models act under considerable uncertainty regarding the quality of the product they are acquiring. This market dynamic can lead to harmful choices by consumers and inadequate reward for high quality developers, potentially leading to a feedback loop through adverse selection that encourages market exit by high quality, high-cost model developers. However, adequately characterizing the benefits of a higher information market to the overall quality of models developed and sold is not feasible.

We request comment on approaches or additional data that would enhance the precision of our estimates of benefits, refine assumptions made related to benefits from more accurate models, and that would allow for quantitative reporting of benefits that we have described in a qualitative manner.

Synchronized Clocks Standard

We propose in section III.C.6 of this preamble to remove the current named specification for clock synchronization, which is Network Time Protocol (NTP v4 of RFC 5905), in 45 CFR 170.210(g). However, we propose to maintain an expectation that Health IT Modules certified to applicable certification criteria continue to utilize any network time protocol (NTP) standard that can ensure a system clock has been synchronized and meets the time accuracy requirements as

defined in the applicable certification criteria in § 170.315(d)(2), § 170.315(d)(3), § 170.315(d)(10), and § 170.315(e)(1).

Costs

This proposal is not intended to place additional burden on health IT developers as it does not require new development or implementation. Rather, a health IT developer's costs would be de minimis because we are providing flexibility to allow health IT developers to use any network time protocol standard that exists. We welcome comments on these expectations.

Benefits

We believe leveraging existing network time protocol standards and not requiring a specific standard allows for more flexibility. We have heard from health IT developers that the current required functionality is in place but not fully used. This proposal allows for additional flexibility to meet the time accuracy requirements as defined in applicable certification criteria. For example, under this proposal, Microsoft-based certified health IT using Operating System to synchronize network time, may use Microsoft's version of Network Time Protocol (MS NTP) as an alternative to Network Time Protocol Version 4 (NTP v4) of RFC 5905 as specified in § 170.210(g), and must meet the time accuracy requirement as defined in the certification criteria. We welcome comments regarding potential approaches for quantifying these benefits.

Standardized API for Patient and Population Services

As discussed in section III.C.7 of this preamble, we propose to update the certification criterion, "*standardized API for patient and population services*," to align with updated standards and new requirements. We propose to adopt the SMART Application Launch Framework Implementation Guide Release 2.0.0 in § 170.215(c)(2), which would replace SMART Application Launch Framework Implementation Guide Release 1.0.0 in § 170.215(a)(3) (proposed in this rule as § 170.215(c)(1)) as the standard on December 31, 2024.

We also propose to revise the requirement in § 170.315(g)(10)(vi) to specify that Health IT Modules presented for certification that allow short-lived access tokens to expire, in lieu of

immediate access token revocation, must be able to revoke an authorized application's access at a patient's direction within one hour of the request.

Additionally, we propose to amend the API Condition and Maintenance of Certification requirements by adding the requirement that Certified API Developers with patient-facing APIs must publish their service base URLs for all customers regardless of whether the certified Health IT Modules are centrally managed by the Certified API Developer or locally deployed by an API Information Source. We propose that these service base URLs must conform to a specific data format.

Finally, we propose to adopt the FHIR US Core Implementation Guide version 5.0.1 in § 170.215(b)(1)(ii). However, based on the annual US Core release cycle, we believe US Core IG v6.0.0 will be published before ONC issues a final rule. Therefore, it is our intent to consider adopting the updated US Core IG v6.0.0 that supports the data elements and data classes in USCDI v3 since we propose to adopt USCDI v3 in this rule. Health IT systems that adopt this version of US Core can provide the latest consensus-based capabilities for providing access to USCDI data classes and elements using a FHIR API.

Costs

We have estimated the proposed cost to health IT developers to make these updates. These estimates are detailed in Table 23 below and are based on the following assumptions:

- *Health IT developers will experience the assumed average costs of labor and data model use*. Table 21 shows the estimated labor costs per product for a health IT developer to implement these updates to the criterion. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will, on average, incur the costs noted in Table 21.
- *We estimate that 276 products certified by 228 developers will be affected by our proposal*. These estimates are a subset of the total estimated health IT developers and certified products we estimated above. We estimate that, in total, 368 health

IT developers will certify 502 health IT products impacted by this rulemaking. However, not all these developers and products will certify the *Standardized API* criterion and need to meet these proposed requirements. As of the end of 2021, 62% of developers and 55% of products certified the *Application Access – Data Category Request* criterion. By December 31, 2022, all products that certify this criterion must certify the new *Standardized AP*I criterion. We, therefore, use current certification of the *Data Category Request* criterion as a proxy for the percent of developers and products certified to the *Standardized API* criterion in the future. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by these updates to the *Standardized API* criterion.

- *Wages are determined using BLS estimates.* According to the May 2021 BLS occupational employment statistics, the mean hourly wage for a "Software Developer" is $58.17. As noted previously, we have assumed that other indirect costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including other indirect costs is $116.

Table 21. Estimated Labor Hours to Update Standardized API for Patient and Population Services

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Implementation to the FHIR US Core IG 5.0.1 (per product)	Implement FHIR US Core IG 5.0.1 to update API to conform to US Core v6, which adopts the USCDIv3 data classes and elements	500	1,000	(1) Lower bound assumes health IT product voluntarily updated to USCDIv3 through SVAP. (2) Upper bound assumes health IT product only supports USCDIv1 and needs to update API to support resources aligned with data elements in USCDIv3.
Task 2: Service-base URL Publication (per developer)	(1) Publish service-base URL in FHIR Endpoint resource format (2) Publish API Information Source	250	1,000	(1) Lower bound assumes API Technology Supplier met the ONC Cures

	organization information in Organization resource format (3) Make both available as FHIR bundle			Act Final Rule service-base URL maintenance of certification requirement and published endpoint and organization data in these standard formats. (2) Upper bound assumes API Technology Supplier met the Cures Final Rule service-base URL maintenance of certification requirement but did not publish in the standard format.
Task 3: Develop support of 60-minute access revocation (per product)	Develop support for patients to revoke access to authorized app and for revocation to be fulfilled by server within 60 minutes of request.	50	100	(1) Lower bound assumes developer needs to modify current revocation process and not rebuild is necessary. (2) Upper bound assumes revocation process exists, as required by ONC Cures Act Final Rule, but needs to be reprogrammed to accommodate new revocation step.
Task 4: Update security via SMART App Launch Framework to IG 2.0 (per product)	Update API from SMART App Launch Framework IG 1.0 to IG 2.0.	500	1,000	(1) Lower bound assumes update to SMART App Launch Framework IG 2.0 underway. (2) Upper bound assumes update to Framework IG 2.0 not underway.

Table 22. Example Calculation for the Lower Bound Estimated Cost to Products to Perform Task 1 in Table 21 To Update API [2021 dollars]

Activity	Estimated labor hours	Developer salary	Projected products
	Lower bound		
Task 1	500	$116 per hour	276
Example calculation: 500 * $116 * 276 products = $16,008,000			

Table 23. Total Cost to Update Standardized API for Patient and Population Services [2021 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Task 1 (276 products)	$16,008,000	$32,016,000
Task 2 (228 developers)	$6,612,000	$26,448,000
Task 3 (276 products)	$1,600,800	$3,201,600
Task 4 (276 products)	$16,008,000	$32,016,000
Total (276 products and 228 developers)	$40,228,800	$93,681,600

The cost to a health IT developer to update the *Standardized API* criterion for their certified Health IT Modules would range from $146,000 to $340,000 per product, on average. Therefore, assuming 276 products overall and a labor rate of $116 per hour, we estimate that the total cost to all health IT developers would, on average, range from $40 million to $94 million. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

We believe this proposal would benefit health care providers, patients, and the industry as a whole. The adoption of the US Core 5.0.1 IG would, with the additional data elements in USCDI v3, expand the baseline set of data available and provide more comprehensive health data for both providers and patients. Updates to the SMART App Launch Framework IG 2.0 would align the certified API functionality with current adopted standards-based methods to connect patients' health information to the app of their choice. Furthermore, updated requirements to the service-base URL publication API maintenance of certification requirement would provide a standard format for all published FHIR endpoints to be securely discovered and consumed by authorized applications. The standard publication format will reduce the burden on patients, app developers, and other third parties to find and connect to the appropriate FHIR endpoint to initiate data access. This would directly benefit the speed and efficiency of making these connections and reduce the level of effort on third parties to access and use these standards-based APIs.

We expect the resulting improvements to interoperable exchange of health information to significantly benefit providers and patients and improve the quality of healthcare provided. In the

ONC Cures Act Final Rule (85 FR 25925), we estimated the total annual benefit of APIs, on average, to range from $0.34 billion to $1.43 billion. These proposed updates to the criterion ensure the benefits of APIs are maintained and the annual benefit due to improved health outcomes and patients having access to their online medical record is realized.

As described in previously, there are additional potential future benefits to the expanded availability of an interoperable API for patient and population services that are not quantifiable at this time. For some use cases there is a clear indication of future technical direction, but at this time, there is insufficient implementation to clearly quantify the scope. For example, CMS has identified an intent to leverage APIs for population services to modernize quality measurement and quality reporting under value-based payment programs.[457] In 2016, a report found that quality measurement reporting bears an estimate $15.4 billion cost on clinicians for chart abstraction, data validation, and measure reporting.[458] The potential future use of FHIR-based APIs for quality measurement could provide greater ability to implement real time data for quality purposes and drastically reduce the costs of manual quality reporting workflows. We seek comment on potential means to estimate these benefits and future cost savings.

Patient Demographics and Observations Certification Criterion

As discussed in section III.C.8 of this preamble, we propose to rename the "*Demographics*" certification criterion (§ 170.315(a)(5)) to "*Patient Demographics and Observations.*" We propose to add the data elements "Sex for Clinical Use" in § 170.315(a)(5)(i)(F), "Name to Use" in § 170.315(a)(5)(i)(G), and "Pronouns" in § 170.315(a)(5)(i)(H) to the "Patient Demographics and Observations" certification criterion (§ 170.315(a)(5)). Additionally, we propose to replace the terminology standards specified for "Sex" in § 170.315(a)(5)(i)(C), "Sexual Orientation" in § 170.315(a)(5)(i)(D), and "Gender

---

[457] CMS Digital Quality Roadmap, March 2022: https://ecqi.healthit.gov/sites/default/files/CMSdQMStrategicRoadmap_032822.pdf.

[458] Health Aff (Millwood), March 2016. *US Physician Practices Spend More Than $15.4 Billion Annually To Report Quality Measures.* https://pubmed.ncbi.nlm.nih.gov/26953292/.

Identity" in § 170.315(a)(5)(i)(E). As such, ONC proposes to remove the fixed list of terms for "Sex" in § 170.315(a)(5)(i)(C), "Sexual Orientation" in § 170.315(a)(5)(i)(D), and "Gender Identity" in § 170.315(a)(5)(i)(E) which are represented by SNOMED CT and HL7® Value Sets for AdministrativeGender and NullFlavor in § 170.207(o)(1) and (2)), and replace it with the SNOMED CT code sets specified in § 170.207(n)(2) and (o)(3).

The proposed modifications to the "Patient Demographics and Observations" criterion would provide greater clarity and standardization to how a patient's sexual orientation and gender identity are recorded electronically in the electronic health record. The USCDI v3 standard includes new data elements for Sexual Orientation and Gender Identity. These data elements are required to be included as part of a patient's electronic health information and included in any record shared with the patient, the patient's caregiver, or health care provider.

Costs

The proposed modifications to the "Patient Demographics and Observations" criterion include 6 tasks: (1) Modify Sex, (2) Modify Sexual Orientation, (3) Modify Gender Identity, (4) Add Sex for Clinical Use, (5) Add Pronouns, and (6) Add Name to Use. These tasks have their own level of effort, and these estimates are detailed in Table 24 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 24 shows the estimated labor costs per product to modify the "Patient Demographics and Observations" Criterion. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur the costs noted in Table 24.

2. We estimate that 321 products certified by 261 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above.

The estimate of 321 products certified by 261 developers is derived as follows. We estimate that, in total, 368 health IT developers would certify 502 health IT products impacted by

this rulemaking. However, not all these developers and products certify the "Patient Demographics and Observations" criterion and need to meet the proposed requirements. As of the end of 2021, 71% of developers and 64% of products certified to the criterion. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the criterion.

3. According to the May 2021 BLS occupational employment statistics, the mean hourly wage for a "Software Developer" is $58.17. As noted previously, we have assumed that other indirect costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including other indirect costs is $116.

Table 24. Estimated Labor Hours to Modify § 170.315(a)(5) Demographics Criterion

Task	Details	Lower bound hours	Upper bound hours
Task 1: Modify Sex [§ 170.315(a)(5)(i)(C)]	Value set for Sex removed and now references SNOMED CT.	0	40
Task 2: Modify Sexual Orientation [§ 170.315 (a)(5)(i)(D)]	Value set for Sexual Orientation removed and now references SNOMED CT.	0	40
Task 3: Modify Gender Identity [§ 170.315 (a)(5)(i)(E)]	Value set for Gender Identity removed and now references SNOMED CT.	0	40
Task 4: Add Sex for Clinical Use [§ 170.315 (a)(5)(i)(F)]	Add "Sex for Clinical Use" using LOINC.	240	580
Task 5: Add Pronouns [§ 170.315 (a)(5)(i)(H)]	Add "Pronouns" using LOINC.	240	580
Task 6: Add Name to Use [§ 170.315 (a)(5)(i)(G)]	Add "Name to Use" as a kind of name field.	240	580

Table 25. Example Calculation for the Lower Bound Estimated Cost to Products to Perform Task 1 in Table 24 To Modify Demographics [2021 dollars]

Activity	Estimated labor hours	Developer salary	Projected products
	Lower bound		
Task 1	200	$116 per hour	321
Example calculation: 200 * $116 * 321 products = $7,447,200			

Table 26. Total Cost to Modify Demographics [2021 dollars]

Activity	Estimated Cost

	Lower bound	Upper bound
Task 1 (321 products)	$0	$1,489,440
Task 2 (321 products)	$0	$1,489,440
Task 3 (321 products)	$0	$1,489,440
Task 4 (321 products)	$8,936,640	$21,596,880
Task 5 (321 products)	$8,936,640	$21,596,880
Task 6 (321 products)	$8,936,640	$21,596,880
Total (321 products and 261 developers)	$26,809,920	$69,258,960

The cost to a health IT developer to make the proposed modifications to the "Patient Demographics and Observations" criterion for their certified Health IT Modules would range from $83,520 to $215,760 per product, on average. Therefore, assuming 321 products overall and a labor rate of $116 per hour, we estimate that the total cost to all health IT developers would, on average, range from $27 million to $69 million. This would be a one-time cost to developers per product that is certified to the specified certification criterion.

Benefits

Improved recording of sexual orientation and gender identity in the medical record has multiple benefits. This has clinical benefits for patients in the immediate term as information related to gender identity and sexual orientation is critical for informing treatment. Additionally, advances in treatment may result from researchers having more reliable and accurate sexual orientation and gender identity data available. Not only would this benefit clinical care teams who are treating patients within a particular clinical setting, this will improve the interoperability of this data when shared electronically with the patient or the patient's authorized representative through the technology of their choosing or when shared electronically with a third-party elected by the patient, such as an application developer, health care provider, or other entity.

The benefits of these modifications are not quantifiable at this time, but we expect the resulting improvements to interoperable exchange of health information to significantly benefit providers and patients and improve the quality of healthcare provided. Furthermore, having a patient's information recorded uniformly and available across their medical records would

improve the patient's access to their information and ensure the information is available uniformly across technologies.

Updates to Transitions of Care Certification Criterion in § 170.315(b)(1)

As discussed in section III.C.9 of this preamble, we propose to modify the "*transitions of care*" certification criterion in § 170.315(b)(1). We propose to replace the fixed value set for the USCDI data element Sex and instead enable health IT developers to represent sex with the standard adopted in § 170.207(n)(1) for the time period up to and including December 31, 2025; or § 170.207(n)(2).

Costs

1. IT developers will use the same labor costs and data models. Table 27 shows the estimated labor costs per product to modify the transitions of care criterion. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur the costs noted in Table 27.

2. We estimate that 281 products certified by 236 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above.

The estimate of 281 products certified by 236 developers is derived as follows. We estimate that, in total, 368 health IT developers will certify 502 health IT products impacted by this rulemaking. However, not all these developers and products certify the transitions of care criterion and need to meet the proposed requirements. As of the end of 2021, 64% of developers and 56% of products certified to the transitions of care criterion. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the criterion.

3. According to the May 2021 BLS occupational employment statistics, the mean hourly wage for a "Software Developer" is $58.17. As noted previously, we have assumed that

overhead costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including overhead costs is $116.

Table 27 Estimated Labor Hours to Modify § 170.315(b)(1) Transitions of Care Criterion

Task	Details	Lower bound hours	Upper bound hours
Task 1: Modify Sex [§ 170.315(a)(5)(i)(C)]	Value set for Sex removed and now references SNOMED CT.	0	40

Table 28. Total Cost to Modify Transitions of Care [2021 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Modify Sex (281 products)	$0	$1,489,440

The cost to a health IT developer to make the proposed modifications to the transitions of care criterion for their certified Health IT Modules would range from $0 to $5,300 per product, on average. Therefore, assuming 281 products overall and a labor rate of $116 per hour, we estimate that the total cost to all health IT developers would, on average, range from $0 to $1.5 million. This would be a one-time cost to developers per product that is certified to the specified certification criterion.

Benefits

There are multiple benefits associated with having more granular information available related to improved recording of sexual orientation and gender identity. This has clinical benefits for patients in the immediate term as information related to gender identity and sexual orientation is critical for informing treatment. Additionally, advances in treatment may result from researchers having more reliable and accurate sexual orientation and gender identity data available. Not only would this benefit clinical care teams who are treating patients within a particular clinical setting, this would improve the interoperability of this data when shared electronically with the patient or the patient's caregiver through the technology of their choosing or when shared electronically with a third-party elected by the patient, such as an application developer, health care provider, or other entity.

The benefits of these modifications are not quantifiable at this time, but we expect the resulting improvements to interoperable exchange of health information to significantly benefit providers and patients and improve the quality of healthcare provided. Furthermore, having a patient's information recorded uniformly and available across their medical records would improve the patient's access to their information and ensure the information is available uniformly across technologies.

Patient Requested Restrictions Certification Criterion

As discussed in section III.C.10 of this preamble, we propose to adopt a new certification criterion in § 170.315(d)(14), to update the existing criterion in § 170.315(e)(1), and to add references for these criteria into the Privacy and Security Framework in § 170.550(h). These proposals are standards agnostic for the implementation of functional requirements supporting HIPAA workflows for a patient to request a right for restrictions on certain uses and disclosures of their EHI for a clinician or other covered entity -to honor such request.

Alternatives

In section III.C.10.b, we discuss a series of alternate proposals related to the primary proposals described for a new certification criterion in § 170.315(d)(14) and to update the existing criterion in § 170.315(e)(1). These alternate proposals would add standards and implementation specifications for the purposes of specifying security labels and related applicable actions to restrict the use or disclosure of EHI. We believe these options may address concerns associated with these criteria as described in our primary proposal. However, we do not believe it is appropriate to propose these options as the primary proposal, as the scope of the current specifications is beyond the core goal of the proposed functionality and additional constraints may be preferable to health IT developers and users. We further considered additional alternatives, such as proposing only a patient-directed workflow, but such an approach would be inadequate to address the needs of the responsible covered entity under the HIPAA Privacy

Rules because it would not include capabilities for the covered entity to review the patient request and implement appropriate privacy workflows.

Costs

It is difficult to estimate or quantify the burden of this proposal because data segmentation for privacy is not widely implemented and has not generally been implemented for this use case. Specifically, while there are standards for security labels for document-based exchange, which ONC adopted in full in 2020 for the criteria in § 170.315(b)(7) and (b)(8), there are not standards which define the technical requirements for the actions described by the security label vocabularies. In other words, the standards exist to describe the policy and action that should be accomplished by a Health IT Module, but not how that action is implemented.

For these reasons, in our proposal, we did not specify how, or at what level of granularity that segmentation must occur. There is also not general industry consensus on what approach will be most cost-effective or how many types of actions would represent the minimum set. This means that in our proposal, we were also unable to define one specific option – or set of options – as a required or a minimum set of actions.

In the ONC Cures Act Final Rule, we estimated a cost of the certification criteria and standards adopted for security labels in § 170.315(b)(7) and (b)(8). We estimated developers would need 400 to 600 hours per criterion to make upgrades on systems that had previously been certified to a prior version of the criteria, or 720 to 1220 hours per criterion for systems that are implementing these criteria for the first time. We estimated the total cost to developers could range from $2,910,400 to $6,933,600. We noted that this would be a one-time cost (85 FR 25926). While this may be perceived to provide some context for an estimate of the scope of these standards if applied under our alternate proposal, these estimates are not readily applicable to the new criterion proposed in § 170.315(d)(14). Not only are the existing criteria lacking the implementation of technical specifications as described, the scope of the HL7 CDA DS4P IG referenced for the criteria in § 170.315(b)(7) and (b)(8) includes a wide range of additional use

cases beyond the patient right to request a restriction under HIPAA Privacy Rules. In the ONC Cures Act Final Rule, we specifically noted our intent in adopting these voluntary certification criteria was to support known high priority use cases defined by state and federal privacy laws for specific privacy constraints for pediatric care and opioid use and substance disorder, including actions related to 42 CFR part 2 restrictions. We note that even in comparison to these high-priority and highly complex use cases, data segmentation workflows supporting patient preferences for data sharing are particularly challenging because of the significant range of potential variables based not only on the types of data but also on applicable law.

In section III.C.10.a, we specifically request public comment to assist in defining the scope of development and helping ONC better understand the potential cost of implementation. Specifically, we seek comment on clear methods by which we might quantify the development burden and costs for the new criterion in § 170.315(d)(14), the new functionality in the existing criterion in § 170.315(e)(1), and the addition to the Privacy and Security Framework in § 170.550(h). In our alternate proposals and request for information in section III.C.10.b and c, we seek comment on clear methods by which we might quantify the development burden and costs that could be associated with a standards-based approach as compared to adopting only a functional requirement. Finally, we seek comment on clear methods by which we might quantify the development burden and costs for this proposed alternative to constrain the USCDI referenced in the new proposed criterion in § 170.315(d)(14) and the proposed revisions to the existing criterion in § 170.315(e)(1).

Benefits

In the ONC Cures Act Final Rule, we noted that the updated criteria in § 170.315(b)(7) and (b)(8) (Security tags—Summary of Care—send and Security tags—Summary of Care—receive) would benefit providers, patients, and ONC because it would support more complete records, contribute to patient safety, and enhance care coordination. We stated that implementing security tags enables providers to more effectively share patient records with sensitive

information, thereby protecting patient privacy while still delivering actionable clinical content. We emphasized that health care providers already have processes and workflows to address their existing compliance obligations, which could be made more efficient and cost effective through the use of health IT. We were, however, unable to quantify these benefits at the time because we did not have adequate information to support quantitative estimates (85 FR 25927).

Since we issued the ONC Cures Act Final Rule, the number of developers certified to the voluntary criteria in § 170.315(b)(7) and (b)(8) has increased, but it remains a small percentage of the total products certified. While we believe there would be similar benefits to patients and other covered entities from our proposals in this rule to support privacy workflows, we similarly are limited in our ability to estimate such impact at this time.

Insights Condition and Maintenance of Certification Requirements

As discussed in section III.F of this preamble, the "*Insights Condition*" calls for health IT developers of certified health IT to report for each applicable product on measures which focus on interoperability. For the initial requirements of the Insights Condition, ONC has proposed nine measures that relate to individual access to electronic health information, clinical care information exchange, public health information exchange, and standards adoption and conformance.

Alternatives

Section 4002(c) of the Cures Act requires the creation of an Electronic Health Record (EHR) Reporting Program. We have chosen to implement the developer reporting through ONC's Health IT Certification Program to integrate this legislative mandate with other reporting requirements for health IT developers of certified health IT as a Condition and Maintenance of Certification requirement. This approach is aligned with how we have interpreted other similar provisions of the Cures Act, and it is intended to maximize participation among health IT developers of certified health IT while aligning participation with other requirements of the Program. Other alternatives to implementing this provision of the Cures Act could be to conduct

a survey of health IT developers of certified health IT to report on measures; however, such an effort would reflect only those developers who participated in the survey, thus limiting the generalizability of the results. A survey approach would also complicate ONC's ability to standardize developer results reporting and thus the quality and the rigor of the data would be affected. Thus, in order to be consistent with ONC's implementation of other Cures Act condition and maintenance of certification requirements, to maximize the generalizability and accuracy of the data gathered through this effort, and to align it with other activities, we have chosen to implement the condition through ONC's Health IT Certification Program.

Costs

In calculating the cost of reporting each measure *m* we applied the following expression:

$$Cm = \#Hours \times Wage \times \#\ of\ Developers$$

The data for each of the elements (e.g., #hours, wages, #developers) were extracted from various sources and there are assumptions associated with each element, which are described in this section.

The *#Hours* represents the labor hours it takes to produce measure *m*. The health IT developers of certified health IT were asked the average number of hours they would need to develop and report a measure. Based on their reporting, we created a lower bound that represents 25% less than the reported number and an upper bound that represents 35% more than the reported number. We adjusted the number of hours required for developing each measure according to the difficulty level as ranked by health IT developers of certified health IT.[459] We attributed more hours to skillful labor categories (from administrators to programmers and managers) than what was provided by developers as we believe these will be more accurate estimates.

[459] Blavin F., et al. 2020. Urban Institute. Electronic Health Record (EHR) Reporting Program: Developer-Reported Measures. Available at https://www.urban.org/sites/default/files/publication/105427/electronic-health-record-ehr-reporting-program-developer-reported-measures.pdf. Accessed March16, 2023.

The *Wage* represents hourly wage of a particular occupation needed to produce a measure. The wage estimates were extracted from the 2021 Bureau of Labor Statistics data and multiplied by two to account for administrative other indirect costs, representing the median hourly wage of a software developer ($116) and a management analyst ($97) (the numbers incorporate other indirect cost of labor).[460] We assumed that the time used only by these occupations was sufficient for completing the task. The number of health IT developers is a function of the proposed small developer threshold and certified criteria requirements, which are described in more detail in section III.F.3 of this preamble under *Associated Thresholds for Health IT Developers*. We used data from the 2019 CMS Promoting Interoperability (PI) program and the Certified Health IT Product List to estimate the number of developers that would be reporting measures to the program. Per the proposed small developer threshold, developers whose certified health IT products were used by at least 50 hospitals, or 500 clinicians would have to report measures to the program. In addition to having these minimum number of users across their certified health IT products, per the proposal, we limited developers to those with products that certify to at least one of the following criteria associated with the proposed measures (see Table 29):

- Transitions of care § 170.315(b)(1)
- Clinical information reconciliation § 170.315 (b)(2)
- Data export § 170.315(b)(6), *where applicable as a proxy for* electronic health information export § 170.315(b)(10)
- Transmission to immunization registry § 170.315(f)(1)
- View, download, and transmit to 3rd party § 170.315(e)(1)
- Application access – data category request § 170.315(g)(8), *where applicable as a proxy for* Standardized API for patient and population services § 170.315 (g)(10)

[460] See BLS at https://www.bls.gov/oes/current/oes_nat.htm. Accessed March 16, 2023.

For each measure, the estimated the number of health IT developers of certified health IT depended on whether developers' products certified to criteria associated with a particular measure (as shown in Table 29) and whether they meet the threshold requirement for a small developer. We note that given that both § 170.315(b)(10) and § 170.315(g)(10) won't be required until after the publication of this NPRM, § 170.315(b)(6) and § 170.315(g)(8), respectively, were used as proxies for the purposes of determining the threshold and related calculations, where the newer criteria were not yet certified to. We assumed developers who have certified to § 170.315(b)(6) and § 170.315(g)(8) shall also certify to § 170.315(b)(10) and § 170.315(g)(10), respectively.

Table 29. Estimated Number of Hours and Developers associated for each measure (per developer)

Measure	Related Criterion	Estimated number of applicable developers of certified health IT (no threshold)	Estimated number of applicable developers of certified health IT (threshold applied)	Management Analyst Estimated Hours (per developer)		Software Developer Estimated Hours (per developer)	
				Lower Bound	Upper Bound	Lower Bound	Upper Bound
Individuals' Use to Access their EHI	§ 170.315(e)(1); § 170.315(g)(10)	157	53	308	770	1540	3080
Immunization Submission to IIS	§ 170.315(f)(1)	115	37	480	1200	2400	4800
Immunization Forecast Query Reporting	§ 170.315(f)(1)	115	37	480	1200	2400	4800
C-CDAs Obtained by Exchange Mechanism	§ 170.315(b)(1)	175	54	400	1000	2000	4000
C-CDAs Received and Incorporated	§ 170.315(b)(1); § 170.315(b)(2)	171	56	400	1400	2800	5600
Availability of apps	§ 170.315(g)(10)	176	59	308	770	1540	3080
Use of FHIR by type of endpoint	§ 170.315(g)(10)	176	59	400	1000	2000	4000
Volume of Bulk FHIR requests by type	§ 170.315(g)(10)	176	59	400	1000	2000	4000

EHI export	§ 170.315(b)(10)	169	53	320	640	960	2560

Data Source: ONC analysis of 2019 CMS Promoting Interoperability Program Data & CHPL

We decided the small developer thresholds based upon analyses we conducted of the 2019 CMS PI Program and Certified Health IT Product List. We examined the various alternatives for setting user thresholds based on the percentage of users and developers that would be represented and reporting measures, respectively in the Program (*see* Table 30 below). The thresholds we decided upon maximize coverage and while not unduly disadvantaging smaller developers. The thresholds were determined based upon analysis of 2019 CMS PI program data and the CHPL data. The data from the CMS PI program included 4,209 non-federal acute hospitals and 691,381 clinicians who attested to the program. After limiting hospitals and clinicians to those using existing 2015 Edition certification criteria, the 2015 Edition Cures Update criteria, or a combination of the two; and to those products of developers who had certified to at least one of the criteria associated with the measures proposed in the Program (*see* Table 29), we ended up with 3,863 hospitals and 689,801 clinicians. For example, based upon a threshold of 50 hospitals, we would be able to include approximately 99% of all hospital users and the top 18 developers (based upon market share) while excluding the bottom 33 developers (based upon market share). This 99% value is based upon the percentage of users who are *not* exclusively using products from developers who meet the small developer threshold. Thus, in the case of a 50-hospital threshold, only 1.4% of hospital users are exclusively using products from small developers, and thus about 99% of the inpatient market is covered.

Table 30. Thresholds options at the developer level

	Est. Number of Users Only Using Small Developers	**Est. % of Users Only Using Small Developers**	**Est. Number of Small Developers**	**Est. Number of Remaining Developers**
Hospitals				
Option (a) 100 Threshold	142	3.7%	39	12

Option (b) 50 Threshold	56	1.4%	33	18
Clinicians				
Option (a) 2,000 Threshold	21,075	3.1%	176	31
Option (b) 1,000 Threshold	11,251	1.6%	160	47
Option (b) 500 Threshold	7,828	1.1%	146	61

In calculating the aggregate cost of developing all measures we applied the concept of economies of scope, where the total cost of production is not incrementally increasing in the number of measures, but it is rather attenuating. Specifically, the aggregate cost in this application is governed by the following expression: The total cost (TC) of producing measures 1 and 2 is the sum of producing the two measures separately minus the cost of producing them together.

To calculate the cost of producing measures together, health IT developers of certified health IT were asked during discussions to provide an estimate on the extent to which there would be an overlap in developing infrastructure between the measures published by the Urban Institute and level of difficulty by measure.[461] While some measures we propose differ from those the Urban Institute published, there is significant overlap across many of the measures, which would retain the validity of these estimates. The weighted average for selected measures suggested that there would be considerable overlap on the immunization measures and somewhat overlap on the bulk FHIR and EHI export measures (*see* Table 31). We note that for the incorporation measure, there is overlap between the proposed measure and the CMS PI Program Measure. We welcome comments that provide us information on the level of perceived overlap so that we can adjust the estimates accordingly for the costs associated with that measure.

Table 31. Percent overlap in developing the following combination of measures.

[461] Blavin F., et al. 2020. Urban Institute. Electronic Health Record (EHR) Reporting Program: Developer-Reported Measures. Available at https://www.urban.org/sites/default/files/publication/105427/electronic-health-record-ehr-reporting-program-developer-reported-measures.pdf. Accessed March 16, 2023.

	Percent
Immunization Submission to IIS and Immunization Forecast Query Reporting	50%
Volume of Bulk FHIR requests by type and EHI Export	27%

Additionally, we assumed that there will be a 10% overlap of developing infrastructure across all measures. We applied these rates accordingly when calculating the total cost of developing measures for the Insights Condition.

Following this approach, the aggregate cost estimates are presented by different alternatives associated with thresholds in Table 32. The first row shows the total cost assuming developers have at least 50 hospital or 500 clinician users, which generates the cost between $103 and $218 million. In addition to estimating the costs associated with the 50 hospitals or 500 clinician user thresholds, we also present the cost for two alternatives where the number of users for hospitals is 100 and for clinicians ranges from 1000 to 2000. The total cost would be reduced by about a half compared to the previous specification because smaller number of developers would qualify for the program.

Table 32. Aggregate Cost Estimates for the Insights Condition by Threshold Alternatives

Options	Lower Bound	Upper Bound
50 Hospitals and 500 Clinicians Threshold (Proposed Approach)	$99,601,742.40	$210,384,572.40
100 Hospitals and 1000 Clinicians Threshold (Alternative 1)	$ 73,276,507	$ 154,529,829
100 Hospitals and 2000 Clinicians Threshold (Alternative 2)	$51,262,462	$107,930,521
No Threshold Applied	$304,434,902.40	$643,349,743.20

In Table 29, we present the estimated number of labor hours to develop and report by measure for each individual developer. This table served as the basis for the cost estimates, prior to adjusting as described above.

In Table 33, we present cost estimates for each individual measure by developer and across all developers. The measures vary in cost because we made adjustments based on synergies discussed above (e.g., similar measures, common infrastructure) and the level of

expected burden to develop each measure. We welcome comments on the approach and data sources we leveraged to calculate these estimates.

Table 33. Estimated costs by measure per health IT developer of certified health IT and across all eligible health IT developers of certified health IT (no threshold)

		Estimated costs (per developer)		Total Estimated Costs (all eligible developers)	
Measure	#Eligible Developers	Lower Bound	Upper Bound	Lower Bound	Upper Bound
Methods Patient Use to Access their EHI	157	$298,352.00	$411,180.00	$31,141,264.00	$64,555,260.00
Immunization Submission to IIS	115	$278,208.00	$576,720.00	$31,993,920.00	$66,322,800.00
Immunization Forecast Query Reporting	115	$154,560.00	$320,400.00	$17,774,400.00	$36,846,000.00
C-CDAs Obtained by Exchange Mechanism	175	$231,840.00	$480,600.00	$40,572,000.00	$84,105,000.00
C-CDAs Received and Incorporated	171	$311,040.00	$672,840.00	$53,187,840.00	$115,055,640.00
Availability of apps	176	$178,516.80	$370,062.00	$31,418,956.80	$65,130,912.00
Use of FHIR by type of endpoint	176	$231,840.00	$480,600.00	$40,803,840.00	$84,585,600.00
Volume of Bulk FHIR requests by type	176	$231,840.00	$480,600.00	$40,803,840.00	$84,585,600.00
EHI export	169	$99,046.40	$249,484.80	$16,738,841.60	$42,162,931.20
All Measures	Total Cost	$1,915,243.20	$4,042,486.80	$304,434,902.40	$643,349,743.20

Table 34. Estimated costs by measure per health IT developer of certified health IT and across all eligible health IT developers of certified health IT (threshold applied)

		Estimated costs (per developer)		Total Estimated Costs (all eligible developers)	
Measure	#Eligible Developers	Lower Bound	Upper Bound	Lower Bound	Upper Bound
Methods Patient Use to	53	$298,352.00	$411,180.00	$10,512,656.00	$21,791,540.00

Access their EHI					
Immunization Submission to IIS	37	$278,208.00	$576,720.00	$10,293,696.00	$21,338,640.00
Immunization Forecast Query Reporting	37	$154,560.00	$320,400.00	$5,718,720.00	$11,854,800.00
C-CDAs Obtained by Exchange Mechanism	54	$231,840.00	$480,600.00	$12,519,360.00	$25,952,400.00
C-CDAs Received and Incorporated	56	$311,040.00	$672,840.00	$17,418,240.00	$37,679,040.00
Availability of apps	59	$178,516.80	$370,062.00	$10,532,491.20	$21,833,658.00
Use of FHIR by type of endpoint	59	$231,840.00	$480,600.00	$13,678,560.00	$28,355,400.00
Volume of Bulk FHIR requests by type	59	$231,840.00	$480,600.00	$13,678,560.00	$28,355,400.00
EHI export	53	$99,046.40	$249,484.80	$5,249,459.20	$13,222,694.40
All Measures	Total Cost	$1,915,243.20	$4,042,486.80	$99,601,742.40	$210,384,572.40

Benefits

The ONC Cures Act Final Rule seeks to advance interoperability and support the access, exchange, and use of electronic health information. There is currently limited transparency and information regarding interoperability; this not only stymies informed decision-making by ONC but also others in the industry, including health care providers, and entities that enable exchange, including various types of health information networks and health app developers. ONC's measurement of interoperability is currently reliant primarily on self-reported survey data from end users of health information technology. While this information does provide some insights on interoperability from end-user perspectives, the insights derived are limited. The proposed measures will provide system-generated metrics on interoperability that will complement self-reported, user perspective data sources, such as surveys. Through the Insights Condition section

of this proposed rule, we have identified where surveys have been limited in providing a clear picture of certain aspects of interoperability that these measures will elucidate. In addition, they will reach a greater number of health care providers than surveys, giving a more complete and representative national perspective. Greater transparency and information on interoperability of health IT products has the potential to benefit a number of interested parties, including ONC and other entities that enable exchange, including health app developers and health information networks. The proposed measures are also designed to identify areas that are working well and problems that we can monitor over time. This will help identify the need for technical and policy solutions as well as spur innovation that builds on successes and addresses gaps. While we currently do not have a means to quantify these benefits, we welcome any feedback on methods to better quantify the impact these measures can have for healthcare and health IT.

The proposed rule's measures for the Insights Condition would help improve and inform ONC programmatic and regulatory decision-making. ONC's programs and policies are designed to make direct and positive impacts on health IT use, care delivery, and patient health. ONC does this primarily through supporting standards development and the Program. The proposed measures would help ONC and others better understand the use, progress, and value of health IT standards. This has practical implications for improving the work ONC leads that increases the use of standards. For example, ONC has limited empirical information to provide guidance on the usage of standards associated with the Interoperability Standards Advisory. With the addition of the proposed measures, ONC can provide guidance to industry that is grounded in data from health IT developers rather than anecdotes. This has the potential to move industry to adopt standards more quickly, which has downstream impacts on improved interoperability. In addition, the proposed measures will increase transparency regarding the capability and usage of certified products. Through these measures ONC and other interested parties will be able to identify areas that are problematic and in need of further investigation, such as cross-cutting

policy and technical issues. They will also provide needed data to develop solutions to these complex problems.

The proposed measures from the Insights Condition will focus on four key priority areas: individual access to electronic health information, clinical care information exchange, standards adoption and conformance, and public health information exchange. Under the individual access to electronic health information domain, the measures will inform on the ONC Cures Act Final Rule goal of increasing access of electronic health information to individuals, particularly through the use of third-party apps. Increased patient engagement has been associated with improved health outcomes, and improved ease of access to their own medical records can improve patient engagement.[462] Thus, a better understanding of how patients are using apps with Certified API Technology will help inform ONC and other interested parties on the progress to reaching this goal. In addition, this measure will help inform app developers and health IT developers of certified health IT, who are supporting apps on what individual's needs are to access their EHI. It will also inform health care provider organizations regarding action they may need to consider in supporting EHI and the need for outreach to patients and caregivers.

The clinical care information exchange measures will help ONC and other interested parties better understand the effectiveness of current C-CDA document exchange mechanisms. By collecting data on the volume of exchange by patient encounters by exchange mechanism, ONC will be able to use that information to inform key policies that support exchange and interoperability, such as TEFCA, which seeks to facilitate exchange between transport mechanisms, such as health information networks. Understanding the volume of exchange flowing through these mechanisms will provide entities enabling exchange, in addition to ONC, with information on which mechanisms are the most frequently and least frequently used. Understand the rates of C-CDA document incorporation is valuable for interested parties

[462] Health Affairs. (2013). Health Policy Brief: Patient Engagement. Accessed March 16, 2023, at: http://healthaffairs.org/healthpolicybriefs/brief_pdfs/healthpolicybrief_86.pdf.

supporting C-CDA document exchange (e.g., is it incorporated and used). This measure can also support further development in the incorporation of C-CDA documents.

Currently, ONC has limited data on the use of Certified API Technology in the app market. The ONC Cures Act Final Rule established the rules for the use of Certified API Technology in such a way to increase access to health information for both patients and health care providers. By understanding which apps are using FHIR-based APIs and the volume of transfer of FHIR resources, ONC and standards development organizations (SDOs) will be able to prioritize their work toward high use data elements as well as explore why some data elements may not have as much use as anticipated. This will not only benefit ONC and SDOs, but in the long-term this will benefit patient care as exchange at the data element level is likely to be less cumbersome than document-based exchange. In addition, these measures are expected to increase transparency in the health IT app market which should lead to improved efficiencies, more competition, and better use of data. Greater transparency will inform decision-making among app developers, patients, health care providers, and other key parties (e.g., CARIN Alliance). Through better insights into the intersections of health IT and the app market, gaps as well as areas of strength can be identified that may spur further innovations in the market.

The ONC Cures Act Final Rule also introduced certification criteria and policies for the exchange of bulk patient health information. The goal of these functionalities is to make patient data requests easier and less expensive as well as allowing health care providers a greater choice of health IT applications. Understanding how these functionalities are being used will allow ONC and others to assess the progress toward those goals and identify where there may be areas in need of refinement. It will provide interested parties, such as accountable care organizations (ACO), researchers, and others with interest in secondary use of certified health IT data with insights as to whether such data is easily moved out of health IT products to support a variety of use cases to advance patient care.

Finally, because of the COVID-19 epidemic, there has been increased attention on the capabilities of health care providers to share public health information with public health agencies (PHA).[463] There has been a focus on the electronic exchange of immunization data to an immunization information system (IIS) via certified health IT. The proposed measures will identify trends and patterns in IIS registries' ability to receive immunization data to enable innovative solutions and improve the utility of IISs and IIS data. Thus, this data would be beneficial to IIS registries to help make improvements to their systems and policies to better support exchange of immunization data. In addition, these measures can help support the numerous HHS efforts aimed at improving the flow of information between health care providers and PHAs, such as ONC's STAR HIE Program and the CDC's ongoing Data Modernization Initiative.

Information Blocking Enhancements

We propose in section IV of this preamble several enhancements with respect to the information blocking provisions in the ONC Cures Act Final Rule. These include defining in regulation text what it means, and what it does not mean, to "offer" health IT. The enhancements also include updating the Infeasibility (45 CFR 171.204) and Manner (45 CFR 171.301, formerly known as the "Content and Manner") Exceptions for clarity and to add more ways for actors' practices to satisfy these exceptions and thus not be considered "information blocking" for purposes of 45 CFR part 171.

Costs

We expect ONC to incur an annual cost for issuing educational resources related to the proposed information blocking enhancements. We estimate that ONC would issue educational resources each quarter, or at least four times per year. We assume that the resources would be provided by ONC staff with the expertise of a GS-15, Step 1 federal employee(s). The hourly

[463] Dixon BE, Caine VA, Halverson PK. Deficient Response to COVID-19 Makes the Case for Evolving the Public Health System. American Journal of Preventive Medicine. 2020;59(6):887-891. https://doi.org/10.1016/j.amepre.2020.07.024.

wage with benefits for a GS-15, Step 1 employee located in Washington, DC is approximately $155.[464] We estimate it would take ONC staff between 100 and 200 hours to develop resources each quarter, or 400 to 800 hours annually. Therefore, we estimate the annual cost to ONC would, on average, range from $62,000 to $124,000.

Benefits

Currently, ONC has limited data and research available to reasonably estimate the benefits of how often an actor may avail itself of one of the permitted exceptions or the costs for an actor to meet a condition to an exception.

We anticipate that the proposed information blocking enhancements will enable actors to determine more easily and with greater certainty whether their practices (acts or omissions) that may or do interfere with access, exchange, or use of EHI (as defined in 45 CFR 171.102) meet the conditions to be considered a "reasonable and necessary" activity under an information blocking exception. As such, we expect these proposals will further ease the burden and costs of complying with the information blocking regulations, while providing increased predictability. This predictability will permit regulated entities to more effectively plan and invest resources in developing and using interoperable technologies and services to improve healthcare efficiency and value. Additionally, we anticipate as a result of the proposed revised definitions and exceptions, there will be reduced interference with the access, exchange, and use of electronic health information because of the added clarity the proposals will provide the market regarding certain practices. Thus, we anticipate an increase in the overall benefits derived from reducing the prevalence of information blocking. We welcome comment on these conclusions and the supporting rationale.

Total Annual Cost Estimate

[464] Office of Personnel and Management. https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2022/DCB.pdf. Accessed March 16, 2023.

We estimate that the total annual cost for this proposed rule for the first year after it is finalized (including one-time costs), based on the cost estimates outlined above and throughout this RIA, would result in $742 million. The total undiscounted perpetual cost over a 10-year period for this proposed rule (starting in year three), based on the cost estimates outlined above, would result in $712 million. We estimate the total costs to health IT developers to be $742 million while the government (ONC) costs to be between $62,000 to $124,000.

Total Annual Benefit Estimate

We estimate the total annual benefit for this proposed rule, based on the benefit estimates outlined above, would be on average $1.0 billion.

Total Annual Net Benefit

We estimate the total undiscounted perpetual annual net benefit for this proposed rule (starting in year three), based on the estimates outlined above, would result in a net benefit of $326 million.

b. Accounting Statement and Table

When a rule is considered an economically significant rule under Executive Order 12866, we are required to develop an accounting statement indicating the classification of the expenditures associated with the provisions of the proposed rule. Monetary annual effects are presented as discounted flows using 3% and 7% factors in Table 35 below. We are not able to explicitly define the universe of all costs but have provided an average of likely costs of this proposed rule as well as a high and low range of likely costs.

Table 35. EO 12866 Summary Table. **(in $ millions, 2021 Dollars)**

	Primary (3%)	Primary (7%)
Present Value of Quantified Costs	$1,436,076,554	$1,322,854,511
Present Value of Quantified Benefits	$829,421,908	$623,925,957
Present Value of Net Benefits	$222,254,535	$126,747,175
	Primary (3%)	Primary (7%)

Annualized Quantified Costs	$168,351,982	$188,344,721
Annualized Quantified Benefits	$97,233,550	$88,833,019
Annualized Net Quantified Benefits	$26,055,011	$18,045,946

Table 36: EO 12866 Summary Table Non-Discounted Flows. (2021 Dollars)

	Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**
Costs	$742,414,31	$89,089,717	$89,089,717	$89,089,717	$89,089,717
Benefits			$28,850,000	$57,700,000	$86,550,000
-	**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
Costs	$89,089,717	$89,089,717	$89,089,717	$89,089,717	$89,089,717
Benefits	$115,400,000	$144,250,000	$173,100,000	$201,950,000	$230,800,000

D. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) requires agencies to analyze options for regulatory relief of small businesses if a rule has a significant impact on a substantial number of small entities. The Small Business Administration (SBA) establishes the size of small businesses for Federal Government programs based on average annual receipts or the average employment of a firm.[465] The entities that are likely to be directly affected by the requirements in this proposed rule requirements are health IT developers. We note that the proposed updates and clarifications

[465] The SBA references that annual receipts mean "total income" (or in the case of a sole proprietorship, "gross income") plus "cost of goods sold" as these terms are defined and reported on Internal Revenue Service tax return forms.

to the reasonable and necessary activities that do not constitute information blocking would provide flexibilities and relief for health IT developers of certified health IT, health information networks, health information exchanges, and health care providers in relation to the information blocking provision of the Cures Act. We refer readers to section IV for our information blocking-related proposals and welcome comments on their impacts on small entities.

While health IT developers that pursue certification of their health IT under the Program represent a small segment of the overall information technology industry, we believe that many health IT developers impacted by the requirements proposed in this proposed rule most likely fall under the North American Industry Classification System (NAICS) code 541511 "Custom Computer Programming Services."[466] OMB advised that the Federal statistical establishment data published for reference years beginning on or after January 1, 2022, should be published using the 2022 NAICS United States codes.[467] The SBA size standard associated with this NAICS code is set at $30 million annual receipts or less. There is enough data generally available to establish that between 75% and 90% of entities that are categorized under the NAICS code 541511 are under the SBA size standard. We also note that with the exception of aggregate business information available through the U.S. Census Bureau and the SBA related to NAICS code 541511, it appears that many health IT developers that pursue certification of their health IT under the Program are privately held or owned and do not regularly, if at all, make their specific annual receipts publicly available. As a result, it is difficult to locate empirical data related to many of these health IT developers to correlate to the SBA size standard. However, although not perfectly correlated to the size standard for NAICS code 541511, we do have information indicating that over 60% of health IT developers that have had Complete EHRs and/or Health IT Modules certified to the 2011 Edition have less than 51 employees.

---

[466] https://www.sba.gov/sites/default/files/2022-05/Table%20of%20Size%20Standards_Effective%20May%202%202022_Final.pdf
[467] https://www.sba.gov/article/2022/feb/01/guidance-using-naics-2022-procurement.

We estimate that the proposed requirements in this proposed rule would have effects on health IT developers, some of which may be small entities, that have certified health IT or are likely to pursue certification of their health IT under the Program. We believe, however, that we have proposed the minimum amount of requirements necessary to accomplish our primary policy goal of enhancing interoperability. Further, as discussed in this RIA above, there are very few appropriate regulatory or non-regulatory alternatives that could be developed to lessen the compliance burden associated with this proposed rule because at least a few of the proposals are derived directly from legislative mandates in the Cures Act.

We do not believe that the proposed requirements of this proposed rule would create a significant impact on a substantial number of small entities, but request comment on whether there are small entities that we have not identified that may be affected in a significant way by this proposed rule. Additionally, the Secretary proposes to certify that this proposed rule would not have a significant impact on a substantial number of small entities.

E. Executive Order 13132 – Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications. Nothing in this proposed rule imposes substantial direct compliance costs on state and local governments, preempts state law, or otherwise has federalism implications. We are not aware of any state laws or regulations that are contradicted or impeded by any of the proposals in this proposed rule. We welcome comments on this assessment.

F. Unfunded Mandates Reform Act of 1995

Section 202 of the Unfunded Mandates Reform Act of 1995 requires that agencies assess anticipated costs and benefits before issuing any rule that imposes unfunded mandates on state, local, and tribal governments or the private sector requiring spending in any one year of $100 million in 1995 dollars, updated annually for inflation. The current inflation-adjusted statutory

threshold is approximately $165 million in 2022. While the estimated potential cost effects of this proposed rule reach the statutory threshold, we do not believe this proposed rule imposes unfunded mandates on state, local, and tribal governments, or the private sector. We welcome comments on these conclusions.

OMB reviewed this proposed rule.

List of Subjects

45 CFR Part 170

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Healthcare, Health information technology, Health insurance, Health records, Hospitals, Incorporation by reference, Laboratories, Medicaid, Medicare, Privacy, Reporting and record keeping requirements, Public health, Security.

45 CFR Part 171

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Healthcare, Health care provider, Health information exchange, Health information technology, Health information network, Health insurance, Health records, Hospitals, Privacy, Reporting and recordkeeping requirements, Public health, Security.

For the reasons set forth in the preamble HHS proposes to amend, 45 CFR subtitle A, subchapter D, as follows:

PART 170 – HEALTH INFORMATION TECHNOLOGY STANDARDS, IMPLEMENTATION SPECIFICATIONS, AND CERTIFICATION CRITERIA AND CERTIFICATION PROGRAMS FOR HEALTH INFORMATION TECHNOLOGY

1. The authority citation for part 170 continues to read as follows:

Authority: 42 U.S.C. 300jj–11; 42 U.S.C 300jj–14; 5 U.S.C. 553

2. Amend § 170.102 by:

a. Removing the terms “2015 Edition Base EHR” and “2015 Edition health IT certification criteria”;

b. Adding the definitions of “Base EHR,” “ONC certification criteria for health IT,” “Predictive decision support intervention,” “Provide,” and “Revised certification criterion (or criteria)” in alphabetical order.

The additions read as follows:

§ 170.102 Definitions.

Base EHR means an electronic record of health-related information on an individual that:

(1) Includes patient demographic and clinical health information, such as medical history and problem lists;

(2) Has the capacity:

(i) To provide clinical decision support;

(ii) To support physician order entry;

(iii) To capture and query information relevant to health care quality;

(iv) To exchange electronic health information with, and integrate such information from other sources; and

(3) Has been certified to the certification criteria adopted by the Secretary in—

(i) Section 170.315(a)(1), (2), or (3); (a)(5), (a)(14), (b)(1), (c)(1), (g)(7), (9), (10), and (h)(1) or (2);

(ii) Section 170.315(a)(9) or (b)(11) for the period up to and including December 31, 2024; and

(iii) Section 170.315(b)(11) on and after January 1, 2025.

ONC certification criteria for health IT means the certification criteria in § 170.315.

* * * * *

Predictive decision support intervention means technology intended to support decision-making based on algorithms or models that derive relationships from training or example data and then

are used to produce an output or outputs related to, but not limited to, prediction, classification, recommendation, evaluation, or analysis.

* * * * *

Provide means the action or actions taken by a health IT developer of certified Health IT Modules to make the certified health IT available to its customers.

* * * * *

Revised certification criterion (or criteria) means a certification criterion that meets at least one of the following:

(1) Has added or changed the capabilities described in the existing criterion in 45 CFR part 170;

(2) Has an added or changed standard or implementation specification referenced in the existing criterion in 45 CFR part 170; or

(3) Is specified through notice and comment rulemaking as an iterative or replacement version of an existing criterion in 45 CFR part 170.

* * * * *

3. Amend § 170.205 by:

a. Revising paragraph (a)(5);

b. Adding paragraph (a)(6);

c. Adding paragraphs (o)(2) and (t)

The revision and additions read as follows:

§ 170.205 Content exchange standards and implementation specifications for exchanging electronic health information.

(a)* * *

(5) *Standard.* HL7 CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2 (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2025.

(6) *Standard.* HL7® CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes STU Companion Guide, Release 3 - US Realm (incorporated by reference, see § 170.299).

* * * * *

(o) * * *

(2) *Standard*. HL7 FHIR® Data Segmentation for Privacy Implementation Guide: Version 1.0.0 – current – ci-build, December 1, 2022 (incorporated by reference, see § 170.299).

* * * * *

(t) *Public health – electronic case reporting* –(1) *Standard.* HL7 FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.0 – STU 2 US (HL7 FHIR eCR IG) (incorporated by reference, see § 170.299).

(2) *Standard.* HL7 CDA® R2 Implementation Guide: Public Health Case Report - the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1 - US Realm (HL7 CDA eICR IG) (incorporated by reference, see § 170.299).

(3) *Standard.* HL7 CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1 - US Realm (HL7 CDA RR IG) (incorporated by reference, see § 170.299).

(4) *Standard*. Reportable Conditions Trigger Codes Value Set for Electronic Case Reporting. RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022 (incorporated by reference, see § 170.299).

4. Amend § 170.207 by:

a. Revising paragraph (a)(1) and removing and reserving paragraph (a)(3);

b. Revising paragraph (c)(1) and removing and reserving paragraph (c)(2);

c. Adding paragraphs (d)(1) and (4);

d. Adding paragraphs (e)(1) and (2);

e. Adding paragraphs (f)(3) and (m)(2);

f. Revising paragraph (n)(1) and adding paragraphs (n)(2) and (3);

g. Revising paragraphs (o) and (p)(1) through (p)(8);

h. Adding paragraphs (r)(2) and (s)(2).

The revisions and additions read as follows:

§ 170.207 Vocabulary standards for representing electronic health information.

(a)* * *

(1) *Standard*. IHTSDO SNOMED CT®, U.S. Edition, March 2022 Release (incorporated by reference, see § 170.299).

* * * * *

(c)* * *

(1) *Standard*. Logical Observation Identifiers Names and Codes (LOINC®) Database Version 2.72, February 16, 2022, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (incorporated by reference, see § 170.299).

* * * * *

(d)* * *

(1) *Standard*. RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, July 5, 2022 Full Monthly Release (incorporated by reference, see § 170.299).

* * *

(4) *Standard.* The code set specified at 45 CFR 162.1002(b)(2).

* * * * *

(e)* * *

(1) *Standard*. HL7 Standard Code Set CVX - Vaccines Administered, updates through June 15, 2022 (incorporated by reference, see § 170.299).

(2) *Standard*. National Drug Code Directory (NDC) - Vaccine NDC Linker, updates through July 19, 2022 (incorporated by reference, see § 170.299).

* * * * *

(f)* * *

(3) *Standard*. CDC Race and Ethnicity Code Set Version 1.2 (July 15, 2021) (incorporated by reference, see § 170.299).

* * * * *

(m)* * *

(1)* * *

(2) *Standard*. The Unified Code of Units of Measure, Revision 2.1, November 21, 2017 (incorporated by reference, see § 170.299).

(n)* * *

(1) *Standard.* Birth sex must be coded in accordance with HL7 Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference, see § 170.299), up until the adoption of this standard expires January 1, 2026, attributed as follows:

(i) Male. M; (ii) Female. F; (iii) Unknown. nullFlavor UNK.

(2) *Standard*. Sex must be coded in accordance with, at a minimum, the version of SNOMED CT ® codes specified in § 170.207(a)(1).

(3) *Standard.* Sex for Clinical Use must be coded in accordance with, at a minimum, the version of LOINC ® codes specified in § 170.207(c)(1).

(o) *Sexual orientation and gender information*--(1) *Standard*. Sexual orientation must be coded in accordance with, at a minimum, the version of SNOMED-CT® codes specified in paragraph (a)(4) of this section for paragraphs (o)(1)(i) through (iii) of this section and HL7 Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference, see § 170.299), up until the adoption of this standard expires on January 1, 2026, for paragraphs (o)(1)(iv) through (vi) of this section, attributed as follows:

(i) *Lesbian, gay or homosexual.* 38628009

(ii) *Straight or heterosexual.* 20430005

(iii) *Bisexual.* 42035005

(iv) *Something else, please describe.* nullFlavor OTH

(v) *Don't know.* nullFlavor UNK

(vi) *Choose not to disclose.* nullFlavor ASKU

(2) *Standard*. Gender identity must be coded in accordance with, at a minimum, the version of SNOMED-CT® codes specified in paragraph (a)(4) of this section for paragraphs (o)(2)(i) through (v) of this section and HL7 Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference in § 170.299), up until the adoption of this standard expires January 1, 2026, for paragraphs (o)(2)(vi) and (vii) of this section, attributed as follows:

(i) *Male.* 446151000124109

(ii) *Female.* 446141000124107

(iii) *Female-to-Male (FTM)/Transgender Male/Trans Man.* 407377005

(iv) *Male-to-Female (MTF)/Transgender Female/Trans Woman.* 407376001

(v) *Genderqueer, neither exclusively male nor female.* 446131000124102

(vi) *Additional gender category or other, please specify.* nullFlavor OTH

(vii) *Choose not to disclose.* nullFlavor ASKU

(3) *Standard*. Sexual Orientation and Gender Identity must be coded in accordance with, at a minimum, the version of SNOMED CT® codes specified in § 170.207(a)(1).

(4) *Standard.* Pronouns must be coded in accordance with, at a minimum, the version of LOINC codes specified in 170.207(c)(1).

(p)* * *

(1) *Financial resource strain.* Financial resource strain must be coded in accordance with, at a minimum, the version of LOINC ® codes specified in § 170.207(c)(1) of this section and attributed with the LOINC ® code 76513-1 and LOINC ® answer list ID LL3266-5.

(2) *Education*. Education must be coded in accordance with, at a minimum, the version of LOINC® codes specified in § 170.207(c)(1) of this section and attributed with LOINC® code 63504-5 and LOINC® answer list ID LL1069-5.

(3) *Stress.* Stress must be coded in accordance with, at a minimum, the version of LOINC® codes specified in § 170.207(c)(1) of this section and attributed with the LOINC® code 76542-0 and LOINC® answer list LL3267-3.

(4) *Depression*. Depression must be coded in accordance with, at a minimum, the version of LOINC® codes specified in § 170.207(c)(1) of this section and attributed with LOINC® codes 55757-9, 44250-9 (with LOINC® answer list ID LL361-7), 44255-8 (with LOINC® answer list ID LL361-7), and 55758-7 (with the answer coded with the associated applicable unit of measure in the standard specified in § 170.207(m)(2)).

(5) *Physical activity.* Physical activity must be coded in accordance with, at a minimum, the version of LOINC® codes specified in § 170.207(c)(1) of this section and attributed with LOINC® codes 68515-6 and 68516-4. The answers must be coded with the associated applicable unit of measure in the standard specified in § 170.207(m)(2).

(6) *Alcohol use.* Alcohol use must be coded in accordance with, at a minimum, the version of LOINC® codes specified in § 170.207(c)(1) of this section and attributed with LOINC® codes 72109-2, 68518-0 (with LOINC® answer list ID LL2179-1), 68519-8 (with LOINC® answer list ID LL2180-9), 68520-6 (with LOINC® answer list ID LL2181-7), and 75626-2 (with the answer coded with the associated applicable unit of measure in the standard specified in § 170.207(m)(2)).

(7) *Social connection and isolation.* Social connection and isolation must be coded in accordance with, at a minimum, the version of LOINC® codes specified in § 170.207(c)(1) of this section and attributed with the LOINC® codes 76506-5, 63503-7 (with LOINC answer list ID LL1068-7), 76508-1 (with the associated applicable unit of measure in the standard specified in § 170.207(m)(2)), 76509-9 (with the associated applicable unit of measure in the standard specified in § 170.207(m)(2)), 76510-7 (with the associated applicable unit of measure in the standard specified in § 170.207(m)(2)), 76511-5 (with LOINC answer list ID LL963-0), and

76512-3 (with the associated applicable unit of measure in the standard specified in § 170.207(m)(2)).

(8) *Exposure to violence (intimate partner violence)*. Exposure to violence: Intimate partner violence must be coded in accordance with, at a minimum, the version of LOINC® codes specified in § 170.207(c)(1) of this section and attributed with the LOINC® code 76499-3, 76500-8 (with LOINC® answer list ID LL963-0), 76501-6 (with LOINC® answer list ID LL963-0), 76502-4 (with LOINC® answer list ID LL963-0), 76503-2 (with LOINC® answer list ID LL963-0), and 76504-0 (with the associated applicable unit of measure in the standard specified in § 170.207(m)(2)).

* * * * *

(r)* * *

(2) *Standard*. Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy, October 29, 2021 (incorporated by reference, see § 170.299).

(s)* * *

(2) *Standard*. Public Health Data Standards Consortium Source of Payment Typology Code Set Version 9.2 (December 2020) (incorporated by reference, see § 170.299).

5. Amend § 170.210 by revising paragraph (g) to read as follows:

§ 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.

* * * * *

(g) *Synchronized clocks.* The date and time recorded utilize a system clock that has been synchronized using any Network Time Protocol (NTP) standard.

* * * * *

6. Revise § 170.213 to read as follows:

§ 170.213 United States Core Data for Interoperability.

The Secretary adopts the following versions of the United States Core Data for Interoperability standard:

(a) *Standard*. United States Core Data for Interoperability (USCDI), July 2020 Errata, Version 1 (v1) (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2025.

(b) *Standard.* United States Core Data for Interoperability (USCDI), October 2022 Errata, Version 3 (v3) (incorporated by reference, see § 170.299).

7. Revise § 170.215 to read as follows:

§ 170.215 Application Programming Interface Standards.

The Secretary adopts the following standards and associated implementation specifications as the available standards for application programming interfaces (API):

(a) *API base standard.* The following are applicable for purposes of standards-based APIs.

(1) *Standard*. HL7® Fast Healthcare Interoperability Resources (FHIR ®) Release 4.0.1 (incorporated by reference, see § 170.299).

(2) [Reserved]

(b) *API constraints and profiles.* The following are applicable for purposes of constraining and profiling data standards.

(1) *United States Core Data Implementation Guides.*

(i) *Implementation specification.* HL7 FHIR® US Core Implementation Guide STU 3.1.1 (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2025.

(ii) *Implementation Specification.* HL7 FHIR® US Core Implementation Guide STU 5.0.1 (incorporated by reference, see § 170.299).

(2) [Reserved]

(c) *Application access and launch.* The following are applicable for purposes of enabling client applications to access and integrate with data systems.

(1) *Implementation specification.* HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0, including mandatory support for the "SMART Core Capabilities" (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2025.

(2) *Implementation specification.* HL7 SMART Application Launch Framework Implementation Guide Release 2.0.0, including mandatory support for the "Capability Sets" of "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch"; all "Capabilities" as defined in "8.1.2 Capabilities;" "Token Introspection" as defined in "7 Token Introspection" (incorporated by reference, see § 170.299).

(d) *Bulk export and data transfer standards*. The following are applicable for purposes of enabling access to large volumes of information on a group of individuals.

(1) *Implementation specification.* FHIR Bulk Data Access (Flat FHIR) (v1.0.0: STU 1), including mandatory support for the "group-export" "OperationDefinition" (incorporated by reference, see § 170.299).

(2) [Reserved]

(e) *API authentication, security, and privacy*. The following are applicable for purposes of authorizing and authenticating client applications.

(1) *Standard.* OpenID Connect Core 1.0, incorporating errata set 1 (incorporated by reference, see § 170.299).

(2) [Reserved]

8. Amend § 170.299 by:

a. Revising paragraph (a);

b. Adding paragraphs (d)(17) through (19);

c. Adding paragraph (e)(6);

d. Redesignating paragraphs (f) through (s) as paragraphs (g) through (t) respectively;

e. Adding new paragraph (f);

f. Amending newly redesignated paragraphs (g), (n), (q), and (s) by adding paragraphs (g)(35) through (41), (n)(6), (q)(5) and (6), (s)(8) and (9);

g. Revising newly redesignated paragraph (p)(2).

The revisions and additions read as follows:

§ 170.299 Incorporation by reference.

(a) Certain material is incorporated by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. All approved incorporation by reference (IBR) material is available for inspection at the U.S. Department of Health and Human Services (HHS) and at the National Archives and Records Administration (NARA). Contact HHS at: U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, 330 C Street SW., Washington, DC 20201, call ahead to arrange for inspection at 202–690–7151. For information on the availability of this material at NARA, visit www.archives.gov/federal-register/cfr/ibr-locations.html or email fr.inspection@nara.gov. The material may be obtained from the sources in the following paragraphs of this section.

* * * * *

(d)* * *

(17) HL7 Standard Code Set CVX – Vaccines Administered, updates through June 15, 2022, IBR approved for § 170.207(e).

(18) National Drug Code Directory (NDC) – Vaccine NDC Linker, updates through July 19, 2022, IBR approved for § 170.207(e)

(19) CDC Race and Ethnicity Code Set version 1.2 (July 15, 2021), IBR approved for § 170.207(f).

(e)* * *

(6) Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy, October 29, 2021 IBR approved for § 170.207(r).

(f) Council of State and Territorial Epidemiologists, 2635 Century Parkway NE, Suite 700, Atlanta, GA 30345, 770-458-3811, https://www.cste.org/

(1) Reportable Conditions Trigger Codes Value Set for Electronic Case Reporting. RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022, IBR approved for § 170.205(t).

(2) [Reserved]

* * * * *

(g)* * *

(35) HL7 CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes STU Companion Guide, Release 3 - US Realm, May 12, 2022, IBR approved for § 170.205(a).

(36) HL7 FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.0 – STU 2 US (HL7 FHIR eCR IG), August 31, 2022. IBR approved for § 170.205(t).

(37) HL7 CDA® R2 Implementation Guide: Public Health Case Report - the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1 - US Realm (HL7 CDA eICR IG), July 20, 2022, IBR approved for § 170.205(t).

(38) HL7 CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1 - US Realm (HL7 CDA RR IG), July 17, 2022, IBR approved for § 170.205(t).

(39) HL7 FHIR® US Core Implementation Guide STU 5.0.1, June 13, 2022, IBR approved for § 170.215(b).

(40) HL7 FHIR® SMART Application Launch Framework Implementation Guide, Release 2.0.0, November 26, 2021, IBR approved for § 170.215(c).

(41) HL7 FHIR® Data Segmentation for Privacy Implementation Guide: Version 1.0.0 – current – ci-build, December 1, 2022, IBR approved for § 170.205(o).

* * * * *

(n)* * *

(6) United States Core Data for Interoperability (USCDI), October 2022 Errata, Version 3 (v3) IBR approved for § 170.213(b).

* * * * *

(p)* * *

(2) Public Health Data Standards Consortium Source of Payment Typology Code Set, Version 9.2 (December 2020), IBR approved for § 170.207(s).

(q)* * *

(5) Logical Observation Identifiers Names and Codes (LOINC ®) Database Version 2.72, February 16, 2022, IBR approved for § 170.207(c).

(6) The Unified Code of Units of Measure, Revision 2.1, November 21, 2017, IBR approved for § 170.207(m).

* * * * *

(s)* * *

(8) International Health Terminology Standards Development Organization (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT ®) U.S. Edition, Release March 2022, IBR approved for § 170.207(a).

(9) RxNorm, July 5, 2022, Release, IBR approved for § 170.207(d).

* * * * *

9. Amend § 170.315 by:

a. Revising the section heading;

b. Revising the introductory text;

c. Revising paragraphs (a)(5)(i), (a)(5)(i)(A)(*1*) and (*2*), (a)(5)(i)(C), (D), and (E),

d. Adding paragraphs (a)(5)(i)(F), (G), and (H) and (a)(9)(vi);

e. Revising paragraphs (a)(12), (b)(1)(iii)(A)(*1*) and (*2*); (b)(1)(iii)(B)(*2*), (b)(1)(iii)(G) introductory text, (b)(1)(iii)(G)(*3*), (b)(2)(i) and (ii), (b)(2)(iii)(D), and (b)(2)(iv), (b)(6)(ii)(B)(*2*), (b)(9)(ii);

f. Adding paragraph (b)(11);

g. Revising paragraphs (c)(4)(iii)(C), (E), (G), (H), and (I);

h Adding paragraph (d)(14);

i. Revising paragraphs (e)(1)(i)(A)(*1*) and (*2*), (e)(1)(i)(B)(*1*) and (*2*), and adding paragraph (e)(1)(iii);

j. Revising paragraphs (f)(1)(i)(B) and (C), (f)(3)(ii), (f)(4)(ii), (f)(5);

k. Revising paragraphs (g)(3) introductory text, (g)(6)(i)(A) and (B), (g)(9)(i)(A)(*1*) and (*2*), (g)(10)(i)(A) and (B), (g)(10)(ii)(A), (g)(10)(iv)(A), (g)(10)(v)(A)(*1*)(*ii*) and (*2*)(*ii*), (g)(10)(vi), and (g)(10)(vii).

The revisions and additions read as follows:

§ 170.315 ONC Certification Criteria for Health IT.

The Secretary adopts the following certification criteria for health IT. Health IT must be able to electronically perform the following capabilities in accordance with applicable standards and implementation specifications adopted in this part. For all criteria in this section, a health IT developer with a Health IT Module certified to any revised certification criterion, as defined in § 170.102, shall update the Health IT Module and shall provide such update to their customers in accordance with the dates identified for each revised certification criterion and for each applicable standard in 45 CFR part 170 subpart B.

(a)* * *

(5) *Patient demographics and observations*. (i) Enable a user to record, change, and access patient demographic and observations data including race, ethnicity, preferred language, sex, sex for clinical use, sexual orientation, gender identity, name to use, pronouns, and date of birth.

(A)* * *

(*1*) Enable each one of a patient's races to be recorded in accordance with, at a minimum, the standard specified in § 170.207(f)(3) and whether a patient declines to specify race.

(*2*) Enable each one of a patient's ethnicities to be recorded in accordance with, at a minimum, the standard specified in § 170.207(f)(3) and whether a patient declines to specify ethnicity.

* * * * *

(C) *Sex.* Enable sex to be recorded in accordance with the standard specified in § 170.207(n)(1) for the time period up to and including December 31, 2025; or § 170.207(n)(2).

(D) *Sexual orientation.* Enable sexual orientation to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(o)(1) for the time period up to and including December 31, 2025; or § 170.207(o)(3), as well as whether a patient declines to specify sexual orientation.

(E) *Gender identity.* Enable gender identity to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(o)(2) for the time period up to and including December 31, 2025; or § 170.207(o)(3), as well as whether a patient declines to specify gender identity.

(F) *Sex for Clinical Use.* Enable a patient's sex for clinical use to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(n)(3). Conformance with this paragraph is required by January 1, 2026.

(G) *Name to Use.* Enable a patient's preferred name to use to be recorded. Conformance with this paragraph is required by January 1, 2026.

(H) *Pronouns*. Enable a patient's preferred pronouns to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(o)(4). Conformance with this paragraph is required by January 1, 2026.

* * * * *

(9)* * *

(vi) *Expiration of Criterion.* The adoption of this criterion for purposes of the ONC Health IT Certification Program expires on January 1, 2025.

* * * * *

(12) *Family health history***.** Enable a user to record, change, and access a patient's family health history in accordance with the familial concepts or expressions included in, at a minimum, the version of the standard in § 170.207(a)(1).

* * * * *

(b)* * *

(1)* * *

(iii)* * *

(A)* * *

(*1*) The data classes expressed in the standards in § 170.213 and in accordance with § 170.205(a)(4), (5), and paragraphs (b)(1)(iii)(A)(*3*)(*i*) through (*iii*) of this section for the time period up to and including December 31, 2024, or

(*2*) The data classes expressed in the standards in § 170.213 and in accordance with § 170.205(a)(4), (6), and paragraphs (b)(1)(iii)(A)(*3*)(*i*) through (*iii*) of this section, and

* * * * *

(B)* * *

(*2*) At a minimum, the version of the standard specified in § 170.207(a)(1).

* * * * *

(G) *Patient matching data*. First name, last name, previous name, middle name (including middle initial), suffix, date of birth, current address, phone number, and sex. The following constraints apply:

* * * * *

(*3*) *Sex Constraint*: Represent sex with the standards adopted in § 170.213.

(2)* * *

(i) *General Requirements*. Paragraphs (b)(2)(ii) and (iii) of this section must be completed based on the receipt of a transition of care/referral summary formatted in accordance with the standards adopted in § 170.205(a)(3) through (5) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates, for time period up to and including December 31, 2024; or in accordance with the standards adopted in § 170.205(a)(3), (4), (6).

(ii) *Correct patient*. Upon receipt of a transition of care/referral summary formatted according to the standards adopted § 170.205(a)(3) through (5) for the time period up to and including December 31, 2024; or according to the standards adopted § 170.205(a)(3), (4), and (6), technology must be able to demonstrate that the transition of care/referral summary received can be properly matched to the correct patient.

(iii)* * *

(D) Upon a user's confirmation, automatically update the list, and incorporate the following data expressed according to the specified standards:

* * * * *

(iv) *System verification.* Based on the data reconciled and incorporated, the technology must be able to create a file formatted according to the standard specified in § 170.205(a)(4) using the Continuity of Care Document template and the standard specified in paragraph (a)(5) of this section for the time period up to and including December 31, 2024; or according to the standard specified in § 170.205(a)(4) using the Continuity of Care Document template and the standard specified in paragraph (a)(6) of this section.

* * * * *

(6)* * *

(ii)* * *

(B)* * *

(*2*) At a minimum, the version of the standard specified in § 170.207(a)(1).

* * * * *

(9)* * *

(ii) The standard in § 170.205(a)(5) for the time period up to and including December 31, 2024; or § 170.205(a)(6).

* * * * *

(11) *Decision support interventions*--(i) *Decision support intervention interaction.* Interventions provided to a user must occur when a user is interacting with technology.

(ii) *Decision support configuration.* (A) Enable interventions and reference resources specified in paragraphs (b)(11)(iii) and (iv) of this section to be configured by a limited set of identified users (e.g., system administrator) based on a user's role.

(B) Enable interventions:

(*1*) Based on the following data expressed in the standards in § 170.213, at a minimum:

(*i*) Problems;

(*ii*) Medications;

(*iii*) Allergies and Intolerances;

(*iv*) At least one demographic specified in paragraph (a)(5)(i) of this section;

(*v*) Laboratory;

(*vi*) Vital Signs;

(*vii*) Unique Device Identifier(s) for a Patient's Implantable Device(s); and

(*viii*) Procedures.

(*2*) When a patient's medications, allergies and intolerance, and problems are incorporated from a transition of care or referral summary received and pursuant to paragraph (b)(2)(iii)(D) of this section.

(C) Enable end users to provide electronic feedback data based on information displayed through the intervention and make available such feedback data for export, in a computable format, including but not limited to the intervention, action taken, user feedback provided (if applicable), user, date, and location.

(iii) *Evidence-based decision support interventions.* Enable a limited set of identified users to select (i.e., activate) electronic decision support interventions (in addition to drug-drug and drug-allergy contraindication checking) based on any of the data referenced in paragraphs (b)(11)(ii)(B)(*1*)(*i*) through (*vii*) of this section.

(iv) *Linked referential DSI.* (A) Identify for a user diagnostic and therapeutic reference information in accordance with at least one of the following standards and implementation specifications:

(*1*) The standard and implementation specifications specified in § 170.204(b)(3).

(*2*) The standard and implementation specifications specified in § 170.204(b)(4).

(B) For paragraph (b)(11)(iv)(A) of this section, technology must be able to identify for a user diagnostic or therapeutic reference information based on each one and at least one combination of the data referenced in paragraphs (b)(11)(ii)(B)(*1*)(*i*), (*ii*), and (*iv*) of this section.

(v) *Predictive decision support interventions attestation.* Health IT developers must make one of the following attestations:

(A) Yes – the Health IT Module enables or interfaces with one or more predictive decision support interventions as defined in § 170.102 based on any of the data expressed in the standards in § 170.213.

(B) No – the Health IT Module does not enable or interface with one or more predictive decision support interventions as defined in § 170.102 based on any of the data expressed in the standards in § 170.213.

(vi) *Source attributes.* Enable a user to review a plain language description of source attribute information as indicated and at a minimum via direct display, drill down, or link out from a Health IT Module:

(A) For evidence-based decision support interventions under paragraph (b)(11)(iii) of this section:

(*1*) Bibliographic citation of the intervention (clinical research or guideline);

(*2*) Developer of the intervention (translation from clinical research or guideline);

(*3*) Funding source of the intervention development technical implementation; and

(*4*) Release and, if applicable, revision dates of the intervention or reference source;

(*5*) Use of the patient demographics and observations data specified in paragraph (a)(5)(i) of this section;

(*6*) Use of Social Determinants of Health data as expressed in the standards in § 170.213; and

(*7*) Use of Health Status Assessments data as expressed in the standards in § 170.213.

(B) For linked referential DSI in paragraph (b)(11)(iv) of this section and drug-drug, drug-allergy interaction checks in paragraph (a)(4) of this section, the developer of the intervention, and where clinically indicated, the bibliographic citation of the intervention (clinical research or guideline).

(C) For Health IT Modules that enable or interface with one or more predictive decision support interventions, as described in paragraph (b)(11)(v)(A) of this section, source attributes in paragraph (b)(11)(vi)(A) of this section and the following:

(*1*) Intervention details:

(*i*) Output of the intervention;

(*ii*) Intended use of the intervention;

(*iii*) Cautioned out-of-scope use of the intervention;

(*2*) Intervention development:

(*i*) Input features of the intervention including description of training and test data;

(*ii*) Process used to ensure fairness in development of the intervention;

(*iii*) External validation process, if available;

(*3*) Quantitative measures of intervention performance:

(*i*) Validity of prediction in test data;

(*ii*) Fairness of prediction in test data;

(*iii*) Validity of prediction in external data, if available;

(*iv*) Fairness of prediction in external data, if available;

(*v*) References to evaluation of use of the model on outcomes, if available;

(*4*) Ongoing maintenance of intervention implementation and use:

(*i*) Update and continued validation or fairness assessment schedule;

(*ii*) Validity of prediction in local data, if available;

(*iii*) Fairness of prediction in local data, if available.

(D) A Health IT Module must clearly indicate when a source attribute listed in paragraphs (b)(11)(vi)(A), (B), or (C) of this section, as applicable, is not available for the user to review, including when:

(*1*) The source attribute includes the "if available" phrase; or

(*2*) The decision support intervention, enabled by or interfaced with the Health IT Module, is developed by other parties that are not developers of certified health IT.

(E) Enable a limited set of identified users to author and revise source attributes and information beyond source attributes listed in paragraphs (b)(11)(vi)(A) and (b)(11)(vi)(C) of this section, as applicable.

(vii) *Intervention Risk Management.* By December 31, 2024, a health IT developer that attests "yes" in § 170.315(b)(11)(v)(A) must:

(A) Employ or engage in the following intervention risk management practices for all predictive decision support interventions, as defined in § 170.102, that the Health IT Module enables or interfaces with:

(*1*) *Risk analysis*. Analyze potential risks and adverse impacts associated with a predictive decision support intervention for the following characteristics: validity, reliability, robustness, fairness, intelligibility, safety, security, and privacy.

(*2*) *Risk mitigation*. Implement practices to mitigate risks, identified in accordance with § 170.315(b)(11)(vii)(A)(*1*), associated with a predictive decision support intervention; and

(*3*) *Governance*. Establish policies and implement controls for predictive decision support intervention governance, including how data are acquired, managed, and used in a predictive decision support intervention.

(B) Compile detailed documentation regarding the intervention risk management practices listed in paragraph (b)(11)(vii)(A) of this section and upon request from ONC, make available such detailed documentation for any predictive decision support intervention, as defined in § 170.102, that the Health IT Module enables or interfaces with.

(C) Submit summary information of the intervention risk management practices listed in paragraph (b)(11)(vii)(A) of this section to its ONC-ACB via publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

(D) Review annually and, as necessary, update documentation described in paragraphs (b)(11)(vii)(B) and (b)(11)(vii)(C) of this section.

(c)* * *

(4)* * *

(iii)* * *

(C) Provider type in accordance with, at a minimum, the standard specified in § 170.207(r)(2).

* * * * *

(E) Patient insurance in accordance with the standard specified in § 170.207(s)(2).

* * * * *

(G) Patient sex in accordance with the version of the standard specified in § 170.207(n)(2).

(H) Patient race and ethnicity in accordance with, at a minimum, the version of the standard specified in § 170.207(f)(3).

(I) Patient problem list data in accordance with, at a minimum, the version of the standard specified in § 170.207(a)(1).

(d)* * *

(14) Patient requested restrictions.

(i) For any data expressed in the standards in § 170.213, enable a user to flag whether such data needs to be restricted from being subsequently used or disclosed as set forth in 45 CFR § 164.522; and

(ii) Prevent any data flagged pursuant to paragraph (d)(14)(i) of this section from being included in a use or disclosure.

(e)* * *

(1)* * *

(i)* * *

(A)* * *

(*1*) The data classes expressed in the standards in § 170.213 (which should be in their English (*i.e.,* non-coded) representation if they associate with a vocabulary/code set), and in accordance with § 170.205(a)(4) and (a)(5), and paragraphs (e)(1)(i)(A)(*3*)(*i*) through (*iii*) of this section for the time period up to and including December 31, 2024, or

(*2*) The data classes expressed in the standards in § 170.213 (which should be in their English (*i.e.*, non-coded) representation if they associate with a vocabulary/code set), and in accordance with § 170.205(a)(4) and (a)(6), and paragraphs (e)(1)(i)(A)(*3*)(*i*) through (*iii*) of this section.

* * * * *

(B)* * *

(*1*) Patients (and their authorized representatives) must be able to use technology to download an ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) in the following formats:

(*i*) Human readable format; and

(*ii*) The format specified in accordance to the standard specified in § 170.205(a)(4) and (5) for the time period up to and including December 31, 2024 or § 170.205(a)(4) and (6), and following the CCD document template.

(*2*) When downloaded according to the standard specified in § 170.205(a)(4) through (6) following the CCD document template, the ambulatory summary or inpatient summary must include, at a minimum, the following data (which, for the human readable version, should be in their English representation if they associate with a vocabulary/code set):

* * * * *

(iii) *Request for restrictions* – Patients (and their authorized representatives) must be able to use an internet-based method to request a restriction to be applied for any data expressed in the standards in § 170.213. Conformance with this paragraph is required by January 1, 2026.

(f)* * *

(1)* * *

(i)* * *

(B) At a minimum, the version of the standard specified in § 170.207(e)(1) for historical vaccines.

(C) At a minimum, the version of the standard specified in § 170.207(e)(2) for administered vaccines.

(3)* * *

(ii) At a minimum, the versions of the standards specified in § 170.207(a)(1) and (c)(1).

(4)* * *

(ii) At a minimum, the versions of the standards specified in § 170.207(a)(1) and (c)(1).

(5) *Transmission to public health agencies – electronic case reporting.* (i) Enable a user to create an electronic case report for transmission meeting the requirements described in paragraphs (f)(5)(i)(A) through (C) of this section for the time period up to and including December 31, 2024; or meet the requirements described in paragraph (f)(5)(ii) of this section.

(A) Consume and maintain a table of trigger codes to determine which encounters may be reportable.

(B) Match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.

(C) Create a case report for electronic transmission based on a matched trigger from paragraph (f)(5)(i)(B) of this section and including at a minimum:

(*1*) The data classes expressed in the standards in § 170.213.

(*2*) Encounter diagnoses information formatted according to the standard specified in § 170.207(i) or the version of the standard specified in § 170.207(a)(1).

(*3*) The provider's name, office contact information, and reason for visit.

(*4*) An identifier representing the row and version of the trigger table that triggered the case report.

(ii) Enable a user to create a case report for electronic transmission in accordance with the following:

(A) Consume and process electronic case reporting trigger codes and parameters and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code value set in § 170.205(t)(4) received from the eRSD profiles as specified in the HL7 FHIR eCR IG in § 170.205(t)(1).

(B) Create a case report consistent with at least one of the following standards:

(*1*) The eICR profile of the HL7 FHIR eCR IG in § 170.205(t)(1), or

(*2*) The eICR profile of the HL7 CDA eICR IG § 170.205(t)(2).

(C) Receive, consume, and process a case report response that is formatted to either the reportability response profile of the HL7 FHIR eCR IG in § 170.205(t)(1) or the HL7 CDA RR IG in § 170.205(t)(3).

(D) Transmit a case report electronically to a system capable of receiving an electronic case report.

* * * * *

(g)* * *

(3) Safety-enhanced design. User-centered design processes must be applied to each capability technology includes that is specified in the following certification criteria: paragraphs (a)(1) through (5), (9), and (14), and (b)(2), (3), and (11) of this section.

* * * * *

(6)* * *

(i)* * *

(A) The data classes expressed in the standards in § 170.213 in accordance with § 170.205(a)(4) and (a)(5) and paragraphs (g)(6)(i)(C)(*1*) through (*4*) of this section for the time period up to and including December 31, 2024; or

(B) The data classes expressed in the standards in § 170.213, and in accordance with § 170.205(a)(4) and (6) and paragraphs (g)(6)(i)(C)(*1*) through (*3*) of this section.

* * * * *

(9)* * *

(i)* * *

(A)* * *

(*1*) Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (5) following the CCD document template, and as specified in paragraphs (g)(9)(i)(A)(*3*)(*i*) through (*iv*) of this section for the time period up to and including December 31, 2024; or

(*2*) Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (6) following the CCD document template, and as specified in paragraphs (g)(9)(i)(A)(*3*)(*i*) through (*iv*) of this section.

* * * * *

(10)* * *

(i)* * *

(A) Respond to requests for a single patient's data according to the standards and implementation specifications adopted in 170.215(a) and in § 170.215(b)(1), including the mandatory capabilities described in “US Core Server CapabilityStatement,” for each of the data included in the standards adopted in § 170.213. All data elements indicated as “mandatory” and “must support” by the standards and implementation specifications must be supported.

(B) Respond to requests for multiple patients' data as a group according to the standards and implementation specifications adopted in § 170.215(a), (b)(1), and (d), for each of the data included in the standards adopted in § 170.213. All data elements indicated as “mandatory” and “must support” by the standards and implementation specifications must be supported.

(ii)* * *

(A) Respond to search requests for a single patient's data consistent with the search criteria included in the implementation specifications adopted in § 170.215(b)(1), specifically the mandatory capabilities described in “US Core Server CapabilityStatement.”

* * * * *

(iv)* * *

(A) Establish a secure and trusted connection with an application that requests data for patient and user scopes in accordance with the implementation specifications adopted in § 170.215(b)(1) and (c).

* * * * *

(v)* * *

(A)* * *

(*1*)* * *

(*ii*) A Health IT Module's authorization server must issue a refresh token valid for a period of no less than three months to applications using the “confidential app” profile according to an implementation specification adopted in § 170.215(c).

* * * * *

(*2*)* * *

(*ii*) A Health IT Module's authorization server must issue a refresh token valid for a new period of no less than three months to applications using the “confidential app” profile according to an implementation specification adopted in § 170.215(c).

* * * * *

(vi) *Patient authorization revocation*. A Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a patient's direction within 1 hour of the request.

(vii) *Token introspection*. A Health IT Module's authorization server must be able to receive and validate tokens it has issued in accordance with an implementation specification in § 170.215(c).

* * * * *

10. Amend § 170.402 by adding paragraphs (a)(5) and (b)(3) to read as follows:

§ 170.402 Assurances.

(a)* * *

(5) A health IT developer must not inhibit its customer’s timely access to interoperable health IT certified under the Program.

(b)* * *

(3)(i) *Update*. A health IT developer must update a Health IT Module, once certified to a certification criterion adopted in § 170.315, to all applicable revised certification criteria, including the most recently adopted capabilities and standards included in the revised certification criterion.

(ii) *Provide*. A health IT developer must provide all Health IT Modules certified to a revised certification criterion, including the most recently adopted capabilities and standards included in the revised certification criterion, to its customers of such certified health IT.

(iii) *Timeliness*. Unless expressly stated otherwise in this part, a health IT developer must complete the actions specified in paragraphs (b)(3)(i) and (ii) of this section:

(A) By no later than December 31 of the calendar year that falls 24 months after the effective date of the final rule adopting the revised criterion or criteria; or

(B) If the developer obtains new customers of health IT certified to the revised criterion after the effective date of the final rule adopting the revised criterion or criteria, then the health IT developer must provide the health IT certified to the revised criterion to such customers within whichever of the following timeframes that expires last:

(*1*) The timeframe provided in paragraph (b)(3)(iii)(A) of this section; or

(*2*) No later than 12 months after the purchasing or licensing relationship has been established between the health IT developer and the new customer for the health IT certified to the revised criterion.

11. Amend § 170.404 by revising paragraph (b)(2) to read as follows:

§ 170.404 Application programming interfaces.

* * * * *

(b)* * *

(2) *Service base URL publication*. For all Health IT Modules certified to § 170.315(g)(10), a Certified API Developer must publish, at no charge, the service base URLs and related organizational details that can be used by patients to access their electronic health information, by December 31, 2024. This includes all customers regardless of whether the Health IT Modules certified to § 170.315(g)(10) are centrally managed by the Certified API Developer or locally deployed by an API Information Source. These service base URLs and organizational details must conform to the following:

(i) Service base URLs must be publicly published in Endpoint resource format according to the standard adopted in § 170.215(a).

(ii) Organization details for each service base URL must be publicly published in Organization resource format according to the implementation specifications adopted in § 170.215(b)(1)). Each Organization resource must contain:

(A) A reference, in the Organization.endpoint element, to the Endpoint resources containing service base URLs managed by this organization.

(B) The organization's name, location, and provider identifier.

(iii) Endpoint and Organization resources must be:

(A) Collected into a Bundle resource formatted according to the standard adopted in § 170.215(a) for publication; and

(B) Reviewed quarterly and, as necessary, updated.

* * * * *

12. Amend § 170.405 by:

a. Revising paragraph (a) and paragraph (b)(2)(ii); and

b. Removing and reserving paragraphs (b)(3) through (7) and (b)(10).

The revisions read as follows:

§ 170.405 Real world testing.

(a) *Condition of Certification requirement.* A health IT developer with one or more Health IT Module(s) certified to any one or more of the ONC Certification Criteria for Health IT in § 170.315(a)(9), (b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10), and (h) must successfully test the real world use of those Health IT Module(s) for interoperability (as defined in 42 U.S.C. 300jj(9) and § 170.102) in the type of setting in which such Health IT Module(s) would be/is marketed.

(b)* * *

(2)* * *

(ii) For real world testing activities conducted during the immediately preceding calendar year, a health IT developer must submit to its ONC-ACB an annual real world testing results report addressing each of its certified Health IT Modules that include certification criteria referenced in paragraph (a) of this section by a date determined by the ONC-ACB that enables the ONC-ACB to publish a publicly available hyperlink to the results report on CHPL no later than March 15 of each calendar year, beginning in 2023. For certified Health IT Modules included in paragraph (a) of this section that are updated using Inherited Certified Status after August 31 of the year in which the plan is submitted, a health IT developer must include the newer version of the certified Health IT Module(s) in its annual real world testing results report. The real world testing results must report the following for each of the certification criteria identified in paragraph (a) of this section that are included in the Health IT Module's scope of certification:

* * * * *

13. Amend § 170.406 by revising paragraph (a)(5) to read as follows:

§ 170.406 Attestations.

(a)* * *

(5) Section 170.405 if a health IT developer has one or more Health IT Modules certified to any one or more ONC Certification Criteria for Health IT in § 170.315(a)(9), (b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10), and (h).

* * * * *

14. Add § 170.407 to read as follows:

§ 170.407 Insights Condition and Maintenance of Certification.

(a) *Condition of Certification.* A health IT developer must submit responses in accordance with the established Insights Condition of Certification requirements with respect to all applicable certified health technology a health IT developer offers under the ONC Health IT Certification Program. A health IT developer must provide responses to an independent entity on behalf of the Secretary with the following Insights Condition measures requirements**:**

(1) *Individuals' access to electronic health information measure*. (i) A health IT developer must submit responses for the individuals' access to electronic health information measure if the health IT developer has:

(A) Any Health IT Module certified to sections 170.315(e)(1) or (g)(10); and

(B) Has at least 50 hospital users or 500 clinician users across its certified health IT products.

(ii) A health IT developer must submit a response that it does not meet the minimum reporting qualifications for this measure if:

(A) The health IT developer does not have at least one product that is certified to one or more of the applicable certification criteria specified in the measure requirements;

(B) The health IT developer does not have at least 50 hospital users or 500 clinician users across its certified health IT; or

(C) If the health IT developer's product does not have any users using the functionality specified by the certification criteria specified in the measure during the reporting period.

(2) *C-CDA documents obtained using certified health IT by exchange mechanism measure.* (i) A health IT developer must submit responses for the C-CDA documents obtained using certified health IT by exchange mechanism measure if the developer has:

(A) Any Health IT Module certified to section 170.315(b)(2); and

(B) Has at least 50 hospital users or 500 clinician users across its certified health IT products.

(ii) A health IT developer must submit a response that it does not meet the minimum reporting qualifications for this measure if:

(A) The health IT developer does not have at least one product that is certified to the certification criterion specified in the measure requirements;

(B) The health IT developer does not have at least 50 hospital users or 500 clinician users across its certified health IT; or

(C) If the health IT developer's product does not have any users using the functionality specified by the certification criterion specified in the measure during the reporting period.

(3) *C-CDA medications, allergies, and problems reconciliation and incorporation using certified health IT measure.* (i) A health IT developer must submit responses for the C-CDA medications, allergies, and problems reconciliation and incorporation using certified health IT measure if the health IT developer has:

(A) Any Health IT Module certified to sections 170.315(b)(2); and

(B) Has at least 50 hospital users or 500 clinician users across their certified health IT products.

(ii) A health IT developer must submit a response that it does not meet the minimum reporting qualifications for this measure if:

(A) The health IT developer does not have at least one product that is certified to the certification criterion specified in the measure requirements;

(B) The health IT developer does not have at least 50 hospital users or 500 clinician users across its certified health IT; or

(C) If the health IT developer's product does not have any users using the functionality specified by the certification criterion specified in the measure during the reporting period.

(4) *Applications supported through certified health IT measure*. (i) A health IT developer must submit responses for the applications support through certified health IT measure if the health IT developer has:

(A) Any Heath IT Module certified to section 170.315(g)(10); and

(B) Has at least 50 hospital users or 500 clinician users across its certified health IT products.

(ii) A health IT developer must submit a response that it does not meet the minimum reporting qualifications for this measure if:

(A) The health IT developer does not have at least one product that is certified to the certification criterion specified in the measure requirements;

(B) The health IT developer does not have at least 50 hospital users or 500 clinician users across its certified health IT; or

(C) If the health IT developer's product does not have any users using the functionality specified by the certification criterion specified in the applicable measure during the reporting period.

(5) *Use of FHIR in apps supported by certified API technology measure*. (i) A health IT developer must submit responses for the use of FHIR in apps supported by certified API technology measure if the health IT developer has:

(A) Any Health IT Module certified to section 170.315(g)(10); and

(B) Has at least 50 hospital users or 500 clinician users across its certified health IT products.

(ii) A health IT developer must submit a response that it does not meet the minimum reporting qualifications for this measure if:

(A) The health IT developer does not have at least one product that is certified to the certification criterion specified in the measure requirements;

(B) The health IT developer does not have at least 50 hospital users or 500 clinician users across its certified health IT; or

(C) If the health IT developer's product does not have any users using the functionality specified by the certification criterion specified in the applicable measure during the reporting period.

(6) *Use of FHIR bulk data access through certified health IT measure*. (i) A health IT developer must submit responses for the use of FHIR bulk data access through certified health IT measure if the health IT developer has:

(A) Any Health IT Module certified to section 170.315(g)(10); and

(B) Has at least 50 hospital users or 500 clinician users across its certified health IT products.

(ii) A health IT developer must submit a response that it does not meet the minimum reporting qualifications for this measure if:

(A) The health IT developer does not have at least one product that is certified to the certification criterion specified in the measure requirements;

(B) The health IT developer does not have at least 50 hospital users or 500 clinician users across its certified health IT; or

(C) If the health IT developer's product does not have any users using the functionality specified by the certification criterion specified in the applicable measure during the reporting period.

(7) *Electronic health information export through certified health IT measure*. (i) A health IT developer must submit responses for the electronic health information export through certified health IT measure if the health IT developer has:

(A) Any Health IT Module certified to section 170.315(b)(10); and

(B) Has at least 50 hospital users or 500 clinician users across its certified health IT products.

(ii) A health IT developer must submit a response that it does not meet the minimum reporting qualifications for this measure if:

(A) The health IT developer does not have at least one product that is certified to the certification criterion specified in the measure requirements;

(B) The health IT developer does not have at least 50 hospital users or 500 clinician users across its certified health IT; or

(C) If the health IT developer's product does not have any users using the functionality specified by the certification criterion specified in the applicable measure during the reporting period.

(8) *Immunization administrations electronically submitted to an immunization information system through certified health IT measure*. (i) A health IT developer must submit responses for immunization administrations electronically submitted to an immunization information system through certified health IT measure if the health IT developer has:

(A) Any Health IT Module certified to section 170.315(f)(1); and

(B) Has at least 50 hospital users or 500 clinician users across its certified health IT products.

(ii) A health IT developer must submit a response that it does not meet the minimum reporting qualifications for this measure if:

(A) The health IT developer does not have at least one product that is certified to the certification criterion specified in the measure requirements;

(B) The health IT developer does not have at least 50 hospital users or 500 clinician users across its certified health IT; or

(C) If the health IT developer's product does not have any users using the functionality specified by the certification criterion specified in the applicable measure during the reporting period.

(9) *Immunization history and forecasts measure.* (i) A health IT developer must submit responses for Immunization history and forecasts measure if the health IT developer has:

(A) Any Health IT Module certified to section 170.315(f)(1); and

(B) Has at least 50 hospital users or 500 clinician users across its certified health IT products.

(ii) A health IT developer must submit a response that it does not meet the minimum reporting qualifications for this measure if:

(A) The health IT developer does not have at least one product that is certified to the certification criterion specified in the measure requirements;

(B) The health IT developer does not have at least 50 hospital users or 500 clinician users across its certified health IT; or

(C) If the health IT developer's product does not have any users using the functionality specified by the certification criterion specified in the applicable measure during the reporting period.

(b) *Maintenance of Certification*. (1) A health IT developer must provide responses to the Insights Condition of Certification specified in paragraph (a) of this section semiannually for any Health IT Module that has or has had an active certification at any time under the ONC Health IT Certification Program during the prior six months:

(i) A health IT developer must provide responses for measures specified in paragraphs (a)(1), (4), (8), and (9) of this section beginning April 2025;

(ii) A health IT developer must provide responses for measures specified in paragraphs (a)(2), (3), and (5) through (7) of this section beginning April 2026.

(2) [Reserved]

15. Amend § 170.523 by:

a. Revising paragraphs (f)(1) introductory text, (f)(1)(xxi), (g)(1), (k)(1)(i) and (ii); and

b. Adding paragraph (u).

The revisions and addition read as follows:

§ 170.523 Principles of proper conduct for ONC-ACBs.

* * * * *

(f)* * *

(1) For the ONC Certification Criteria for Health IT:

* * * * *

(xxi) Where applicable, all of the information required to be submitted by the health IT developer to meet intervention risk management requirements in § 170.315(b)(11)(vii)(C).

* * * * *

(g)* * *

(1) Retain all records related to the certification of Complete EHRs and Health IT Modules to the ONC Certification Criteria for Health IT beginning with the codification of those certification criteria in the Code of Federal Regulations through a minimum of 3 years from the effective date of the removal of those certification criteria from the Code of Federal Regulations; and

* * * * *

(k)* * *

(1)* * *

(i) The disclaimer "This Health IT Module is compliant with the ONC Certification Criteria for Health IT and has been certified by an ONC-ACB in accordance with the applicable certification criteria adopted by the Secretary of Health and Human Services. This certification does not represent an endorsement by the U.S. Department of Health and Human Services."

(ii) For a Health IT Module certified to the ONC Certification Criteria for Health IT, the information specified by paragraphs (f)(1)(i), (vi) through (viii), (xv), and (xvi) of this section as applicable for the specific Health IT Module.

* * * * *

(u) *Insights*. Confirm that developers of certified health IT submit responses for Insights Conditions and Maintenance of Certification requirements in accordance with § 170.407.

16. Amend § 170.524 by revising paragraph (f)(1) to read as follows:

§ 170.524 Principles of proper conduct for ONC-ATLs.

* * * * *

(f)* * *

(1) Retain all records related to the testing of Complete EHRs and/or Health IT Modules to the ONC Certification Criteria for Health IT beginning with the codification of those certification criteria in the Code of Federal Regulations through a minimum of three years from the effective date of the removal of those certification criteria from the Code of Federal Regulations; and

* * * * *

17. Amend § 170.550 by revising paragraphs (g), (h)(1) and (h)(3)(iii), (v), and (viii), and (m) introductory text to read as follows:

§ 170.550 Health IT Module certification.

* * * * *

(g) *Health IT Module dependent criteria.* When certifying a Health IT Module to the ONC Certification Criteria for Health IT, an ONC-ACB must certify the Health IT Module in accordance with the certification criteria at:

* * * * *

(h) * * *

(1) *General rule.* When certifying a Health IT Module to the ONC Certification Criteria for Health IT, an ONC-ACB can only issue a certification to a Health IT Module if the privacy and security certification criteria in paragraphs (h)(3)(i) through (ix) of this section have also been met (and are included within the scope of the certification).

(3)* * *

(iii) Section 170.315(b)(1) through (3) and (6) through (9) are also certified to the certification criteria specified in § 170.315(d)(1) through (3), (d)(5) through (8), (d)(12) and (13), and, by January 1, 2026, (d)(14);

(v) Section 170.315(e)(1) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), (5), (7), (9), (12), (13), and, by January 1, 2026, (d)(14);

(viii) Section 170.315(g)(7) through (10) is also certified to the certification criteria specified in § 170.315(d)(1), (9), (12), (13), and, by January 1, 2026, (d)(14); and (d)(2)(i)(A) and (B), (d)(2)(ii) through (v), or (d)(10);

* * * * *

(m) *Time-limited certification and certification status for certain ONC Certification Criteria for Health IT.* An ONC-ACB may only issue a certification to a Health IT Module and permit continued certified status for:

* * * * *

PART 171—INFORMATION BLOCKING

18. The authority citation for part 171 continues to read as follows:

Authority: 42 U.S.C. 300jj–52; 5 U.S.C. 552.

19. Amend § 171.102 by

a. Adding, in alphabetical order, the definition of "Business associate";

b. Revising the definition of "Health IT developer of certified health IT"; and

c. Adding, in alphabetical order, the definitions of "Offer health information technology or offer health IT", and "Provide".

The additions and revision read as follows:

§ 171.102 Definitions

* * * * *

Business associate is defined as it is in 45 CFR 160.103.

* * * * *

Health IT developer of certified health IT means an individual or entity, other than a health care provider that self-develops health IT not offered to others, that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj-11(c)(5) (ONC Health IT Certification Program).

* * * * *

Offer health information technology or *offer health IT* means to hold out for sale, resale, license, or relicense; or to sell, resell, license, relicense, or otherwise provide or supply health information technology (as that term is defined in 42 U.S.C. 300jj(5)) that includes one or more Health IT Modules certified under the ONC Health IT Certification Program, for use by other individual(s) or entity(ies) under any arrangement other than the following:

(1) Donation and subsidized supply arrangements are not considered offerings when an individual or entity donates, gives, or otherwise makes available funding to subsidize or fully cover the costs of a health care provider's acquisition, augmentation, or upkeep of health IT, provided such individual or entity offers and makes such subsidy without condition(s) limiting the interoperability or use of the technology to access, exchange or use electronic health information for any lawful purpose.

(2) Implementation and use activities conducted by an individual or entity as follows:

(i) Issuing user accounts and/or login credentials for the individual's or organization's employees to use the individual's or organization's health IT to access, exchange, or use *electronic health information* (as defined in this section) in the course of their employment.

(ii) Implementing, operating, or otherwise making available production instances of application programming interface (API) technology (whether certified or not) that supports access, exchange, and use of *electronic health information* (as defined in this section) that the individual

or entity has in its possession, custody, control, or ability to query or transmit from or across a *health information network* or *health information exchange* (as defined in this section).

(iii) Implementing, operating, and making available production instances of online portals for patients, clinicians, or other health care providers, or public health entities to access, exchange, and use *electronic health information* (as defined in this section) that the individual or entity has in its possession, custody, control, or ability to query or transmit from or across a *health information network* or *health information exchange* (as defined in this section).

(iv) Issuing login credentials or user accounts for the individual's or entity's production, development, or testing environments to public health authorities or such authorities' employees as a means of accomplishing or facilitating access, exchange, and use of *electronic health information* (as defined in this section) for public health purposes including but not limited to syndromic surveillance.

(v) Issuing login credentials or user accounts for independent healthcare professionals who furnish services in a healthcare facility to use the facility's electronic health record or other health IT system(s) in furnishing, documenting, and accurately billing for that care.

(3) Consulting and legal services arrangements as follows:

(i) Legal services furnished by outside counsel—when furnishing legal services to a client in any matter or matters pertaining to the client's seeking, assessing, selecting, or resolving disputes over contracts or other arrangements by which the client obtains use of certified health IT. Outside counsel also does not offer health IT if or when facilitating limited access or use of the client's health IT or EHI within it to independent expert witnesses engaged by counsel, opposing parties' counsel and experts, and special masters and court personnel, as necessary or appropriate to legal discovery.

(ii) Health IT consultant assistance selection, implementation and use consultant —provided by an individual or firm when furnishing expert advice and consulting services to a health IT customer or user that help the customer or user, or on the customer's behalf, do any or all of the

following with respect to any health IT product that the consultant does not sell or resell, license or relicense, or otherwise supply to the customer under any arrangement on a commercial basis or otherwise:

(A) define the customer or user business needs; evaluate or select health IT product(s);

(B) negotiate for the purchase, lease, license, or other arrangement under which the health IT product(s) will be used; or

(C) oversee configuration, implementation, or operation of health IT product(s).

(iii) Comprehensive and predominantly non-health IT clinician practice or other health care provider administrative or operations management services—provided by an individual or entity when furnishing a clinician practice or other health care provider administrative or operational management consultant services where the management consultant acts as the agent of the provider or otherwise stands in the shoes of the provider in dealings with the health IT developer or commercial vendor, and/or in managing the day-to-day operations and administrative duties for the health IT, as part of a comprehensive array of predominantly non-health IT administrative and operational functions that would otherwise fall on the clinician practice or other health care provider's partners, owner(s), or staff.

* * * * *

Provide is defined as it is in § 170.102.

* * * * *

20. Revise § 171.103 to read as follows:

§ 171.103 Information blocking.

(a) Information blocking means a practice that except as required by law or covered by an exception set forth in subpart B or subpart C of this part, is likely to interfere with access, exchange, or use of electronic health information; and

(b) If conducted by:

(1) A health IT developer of certified health IT, health information network or health information exchange, such developer, network or exchange knows, or should know, that such practice is likely to interfere with access, exchange, or use of electronic health information; or

(2) A health care provider, such provider knows that such practice is unreasonable and is likely to interfere with access, exchange, or use of electronic health information.

20. Amend § 171.204 by revising paragraphs (a)(1) and (3) and adding paragraphs (a)(4) and (5) to read as follows:

§ 171.204 Infeasibility exception - When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information due to the infeasibility of the request not be considered information blocking?

* * * * *

(a) *** (1) *Uncontrollable events.* The actor cannot fulfill the request for access, exchange, or use of electronic health information because of a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.

* * * * *

(3) *Third party seeking modification use*. The request is to enable use of EHI in order to modify EHI (including but not limited to creation and deletion functionality) provided the request is not from a health care provider requesting such use from an actor that is its business associate.

(4) *Manner exception exhausted*. The actor is unable to fulfill a request for access, exchange, or use of electronic health information because paragraphs (i), (ii), and (iii) are all true.

(i) The actor could not reach agreement with a requestor in accordance with § 171.301(a) or was technically unable to fulfill a request for electronic health information in the manner requested;

(ii) The actor offered all alternative manners in accordance with § 171.301(b) for the electronic health information requested but could not reach agreement with the requestor; and

(iii) The actor does not provide the same access, exchange, or use of the requested electronic health information to a substantial number of individuals or entities that are similarly situated to the requester.

(5) *Infeasible under the circumstances.* (i) The actor demonstrates, prior to responding to the request pursuant to paragraph (b) of this section, through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of the following factors that led to its determination that complying with the request would be infeasible under the circumstances:

(A) The type of electronic health information and the purposes for which it may be needed;

(B) The cost to the actor of complying with the request in the manner requested;

(C) The financial and technical resources available to the actor;

(D) Whether the actor's practice is non-discriminatory and the actor provides the same access, exchange, or use of electronic health information to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

(E) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged; and

(F) Why the actor was unable to provide access, exchange, or use of electronic health information consistent with the exception in § 171.301.

(ii) In determining whether the circumstances were infeasible under paragraph (a)(3)(i) of this section, it shall not be considered whether the manner requested would have:

(A) Facilitated competition with the actor.

(B) Prevented the actor from charging a fee or resulted in a reduced fee.

* * * * *

21. Revise § 171.301 to read as follows:

§ 171.301 Manner exception - When will an actor's practice of limiting the manner in which it fulfills a request to access, exchange, or use electronic health information not be considered information blocking?

An actor's practice of limiting the manner in which it fulfills a request to access, exchange, or use electronic health information will not be considered information blocking when the practice follows the conditions of this section.

(a) *Manner requested*. (1) An actor must fulfill a request for electronic health information in any manner requested, unless the actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request in the manner requested.

(2) If an actor fulfills a request for electronic health information in any manner requested:

(i) Any fees charged by the actor in relation to fulfilling the request are not required to satisfy the exception in § 171.302; and

(ii) Any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the exception in § 171.303.

(b) *Alternative manner*. If an actor does not fulfill a request for electronic health information in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request in the manner requested, the actor must fulfill the request in an alternative manner, as follows:

(1) The actor must fulfill the request without unnecessary delay in the following order of priority, starting with paragraph (b)(1)(i) of this section and only proceeding to the next consecutive paragraph if the actor is technically unable to fulfill the request in the manner identified in a paragraph.

(i) Using technology certified to standard(s) adopted in part 170 that is specified by the requestor.

(ii) Using content and transport standards specified by the requestor and published by:

(A) The Federal Government; or

(B) A standards developing organization accredited by the American National Standards Institute.

(iii) Using an alternative machine-readable format, including the means to interpret the electronic health information, agreed upon with the requestor.

(2) Any fees charged by the actor in relation to fulfilling the request are required to satisfy the exception in § 171.302.

(3) Any license of interoperability elements granted by the actor in relation to fulfilling the request is required to satisfy the exception in § 171.303.

(c) *TEFCA manner*. If an actor who is a QHIN, Participant, or Subparticipant offers to fulfill a request for EHI access, exchange, or use for any purpose permitted under the Common Agreement and Framework Agreement(s) from any other QHIN, Participant, or Subparticipant using Connectivity Services, QHIN Services, or the specified technical services in the applicable Framework Agreement available to both parties, then:

(i) The actor is not required to offer the EHI in any alternative manner;

(ii) Any fees charged by the actor in relation to fulfilling the request are not required to satisfy the exception in § 171.302; and

(iii) Any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the exception in § 171.303.

(d) *Definitions*. The terms used in paragraph (c) of this section shall have the following meanings.

(1)(i) *Qualified Health Information Network* (*QHIN)* means a Health Information Network that is a U.S. Entity that has been Designated by the Recognized Coordinating Entity (RCE) and is a party to the Common Agreement countersigned by the RCE.

(ii) *Participant* means a U.S. Entity regardless of whether the entity is a Covered Entity or a Business Associate, that has entered into a Participant-QHIN Agreement whereby the QHIN

agrees to transmit and receive information via QHIN-to-QHIN exchange on behalf of the party to the Participant-QHIN Agreement for the Exchange Purposes.

(iii) *Subparticipant* mans a U.S. Entity regardless of whether the entity is a Covered Entity or Business Associate, that has entered into either:

(A) a Participant-Subparticipant Agreement to use the services of a Participant to send and/or receive information; or

(B) a Downstream Subparticipant Agreement pursuant to which the services of a Subparticipant are used of the Common Agreement to send and/or receive information.

(iv) *Connectivity Services* means the technical services provided by a QHIN.

(v) *Framework Agreement(s)* means any one or combination of the Common Agreement, a Participant-QHIN Agreement, a Participant-Subparticipant Agreement, or a Downstream Subparticipant Agreement, as applicable.

(2) QHIN Services means any technical services provided within a QHIN.

Xavier Becerra,
Secretary,
Department of Health and Human Services.

BILLING CODE 4150-45-P

[FR Doc. 2023-07229 Filed: 4/11/2023 8:45 am; Publication Date: 4/18/2023]