Billing Code: 4120-03

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; System of Records

AGENCY: Centers for Medicare & Medicaid Services (CMS), Department of Health and Human Services (HHS).

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, as amended, the Department of Health and Human Services (HHS) is modifying an existing system of records maintained by the Centers for Medicare & Medicaid Services (CMS), titled "Home Health Agency (HHA) Outcome and Assessment Information Set (OASIS)," System No. 09-70-0522. This system of records covers information about patients receiving home health services from a Medicare and/or Medicaid approved HHA. Home health agencies required to comply with Medicare Conditions of Participation (CoP) are now mandated to collect OASIS on patients with any payer source, instead of just patients with Medicare/Medicaid pay sources. The amended System of Records Notice (SORN) includes other modifications which are explained in the Supplementary Information section, below.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is effective [INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*], subject to a 30-day period in which to comment on the new and revised routine uses, described below. Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: The public should submit written comments on this notice, by mail or email, to Barbara Demopulos, CMS Privacy Act Officer,7500 Security Blvd., N1-14-56, Baltimore, MD 21244-1850, or barbara.demopulos@cms.hhs.gov. Comments will be available for public viewing at the same location. To review comments in person, please contact Barbara Demopulos.

FOR FURTHER INFORMATION CONTACT: General questions about the modified system of records may be submitted to the following: Jermama Keys, National Program Coordinator, Home Health Quality Reporting Program, Centers for Medicare & Medicaid Services by mail or email at 7500 Security Blvd., Baltimore MD, 21255, Mail Stop S3-02-01, Baltimore, MD 21244-1850. Office: 410-786-7778, or email jermama.keys@cms.hhs.gov.

SUPPLEMENTARY INFORMATION:

I. Reason for modifying System of Records 09-70-0522

The primary reason for this modification is to provide notice that the system of records will now include all "all-payer" Outcome and Assessment Information Set (OASIS) records; specifically, it will include OASIS records for all patients receiving home health services from a Medicare and/or Medicaid approved HHA regardless of payer, instead of being limited to OASIS records of home health services paid only by Medicare or Medicaid. ("All-payer" refers to the payment system that applies to home health services; in an "all payer" payment system, all payers--including state and federal health programs, private insurers, employers, and individuals--pay the same rate for the services.) Exemptions from OASIS data collection and submission requirements remain the same, i.e., OASIS is not required for home health care patients receiving pre-partum or post-partum services, patients under 18 years of age, and patients receiving only personal care, housekeeping services, or chore services.

II. Modifications made to the System of Records Notice (SORN)

The modified SORN published in this notice differs from the existing SORN in these respects.

- The System Manager(s) section has been updated to change the applicable office name in which the System Manager is located from the Center for Medicaid and State Operations (CMSO) to the Center for Clinical Standards and Quality (CCSQ) and to add contact information, i.e., a telephone number.
- The Authority section has been updated to include U.S. Code citations for the sections of the Social Security Act cited, to add section 1895 of the Social Security Act (42 U.S.C. 1395fff) which established the framework for payment for home health services provided under Medicare, and to remove section 951 of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (Pub. L. 108-173) which is no longer applicable.
- The Categories of Individuals section has been broadened to include patients with non-Medicare/non-Medicaid payers, except patients who are exempt from OASIS data collection and submission.
- The Categories of Records section has been expanded to include records of all payers and to remove a reference to "patients with the payment sources of Medicare traditional fee for service, Medicaid traditional fee for service, Medicare Health Maintenance Organization (HMO)/managed care or Medicaid HMO/managed care."
- The Sources section has been revised to state that the individual record subject and clinical data are the sources of the information in OASIS records, instead of stating that OASIS is the source.
- In the Routine Uses section, the following routine uses have been revised and added:
    - Routine use 5, which authorizes disclosures to national accrediting organizations, has been revised to refer to "The Joint Commission on Accreditation of Healthcare Organizations" as simply "The Joint Commission."
    - Routine use 6, which authorizes disclosures to the Department of Justice in litigation, has been expanded to include "a court or other adjudicative body" as disclosure recipients and to broaden "litigation" to include "other adjudicative proceeding." In addition, a phrase

requiring that the disclosures be compatible with the purpose for which the information was originally collected has been removed as redundant (it is redundant because a routine use is, by definition, a disclosure that is compatible with the original collection purpose).

  - Routine use 13 is new; it authorizes disclosures to a congressional office in the course of responding to its written inquiry about a written constituent request.

- At the end of the Routine Uses section, the note "*Additional circumstances affecting all routine use disclosures*" has been revised to change "beneficiary" to "patient" in the parenthetical statement "(instances where the patient population is so small that individuals could, because of the small size, use this information to deduce the identity of the patient)," to further reiterate the payer source expansion.

- The Storage section now states that "All records are stored electronically" instead of that records are stored on paper and magnetic disk.

- The Retention and Disposal section has been updated to cite and describe the applicable National Archives and Records Administration (NARA) approved schedule.

- The Safeguards section has been revised to describe additional safeguards used to protect the records from unauthorized access (the existing SORN described only training and ensuring that disclosure recipients have adequate security in place) and to cite additional security-related statutes and regulations that apply to the records.

- The Record Access Procedures, Contesting Record Procedures, and Notification Procedures sections have been revised to add that a request must include the individual's email address or other contact information, place of birth, and signature; to no longer require that the individual's sex and health insurance claim number be included; and to explain that the individual may verify his or her identity either by having his or her signature notarized or by providing a statement under penalty of perjury.

- The SORN has been reformatted to conform to the "Full" SORN template prescribed in OMB Circular A-108, issued December 23, 2016.

Barbara Demopulos,
Privacy Act Officer,
Division of Security, Privacy Policy and Oversight,
Information Security and Privacy Group,
Office of Information Technology,
Centers for Medicare & Medicaid Services.

SYSTEM NAME AND NUMBER:

Home Health Agency (HHA) Outcome and Assessment Information Set (OASIS), 09-70-0522.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

The address of system location is: Centers for Medicare & Medicaid Services (CMS) Data Center (North Bldg. First Floor and South Bldg.), 7500 Security Blvd., Baltimore, MD 21244-1850.

SYSTEM MANAGER(S):

The System Manager is the Director, Division of Continuing Care Providers, Survey and Certification Group, Center for Clinical Standards and Quality (CCSQ), CMS, 7500 Security Blvd. - S2-12-25, Baltimore, MD 21244-1850, Phone Number 410-786-3000.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Maintenance of the records is authorized by 42 U.S.C. secs. 1302(a); 1320c-3; 1395x(m), (o), and (z); 1395z; 1395aa; 1395bb; 1395cc; 1395hh; 1395bbb; 1395fff; and 1396a (secs. 1102(a), 1154, 1861(m), 1861(o), 1861(z), 1863, 1864, 1865, 1866, 1871, 1891, 1895, and 1902 of the Social Security Act). These statutes authorize the Administrator of CMS to require HHAs participating in the Medicare and Medicaid programs to complete a standard, valid, patient assessment data set, i.e., OASIS, as part of their comprehensive assessments and updates when evaluating adult, non-maternity patients as required by the Conditions of Participation (CoP) regulations at 42 CFR 484.55.

PURPOSE(S) OF THE SYSTEM:

The primary purposes for which the records are used are to: (1) study and help ensure the quality of care provided by home health agencies (HHA); (2) aid in administration of the survey and certification of Medicare/Medicaid HHAs; (3) enable regulators to provide HHAs with data for their internal quality improvement activities; (4) support agencies of the state government to determine, evaluate and assess overall effectiveness and quality of HHA services provided in the state; (5) provide for the validation, and refinements of the Medicare Prospective Payment System; (6) aid in the administration of federal and state HHA programs within the state; and (7) monitor the continuity of care for patients who reside temporarily outside of the state.

Information maintained in this system is also disclosed to: (1) support regulatory, reimbursement, and policy functions performed within the Agency or by a contractor, consultant, or grantee; (2) assist another federal and/or state agency, agency of a state government, an agency established by state law, or its fiscal agent, for evaluating and monitoring the quality of home health care and contribute to the accuracy of health insurance operations; (3) support research, evaluation, or epidemiological projects related to the prevention of disease or disability, or the restoration or maintenance of health, and for payment related projects; (4) support the functions of Quality Improvement Organizations (QIO); (5) support the functions of national

accrediting organizations; (6) support litigation involving the Agency; and (7) combat fraud, waste, and abuse in certain health care programs.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The records are about patients receiving home health services at a Medicare and/or Medicaid approved HHA, regardless of payer, except those receiving pre-partum and post-partum services, patients under 18 years of age, and patients receiving only personal care, housekeeping services, or chore services.

CATEGORIES OF RECORDS IN THE SYSTEM:

The records are Outcome and Assessment Information Set (OASIS) records, consisting of individual-level demographic and identifying data and clinical status data. Demographic and identifying data include, for example, the patient's name; date of birth; state of residence and zip code; sex, ethnicity, and race; and Social Security number (SSN), Medicare Beneficiary Identifier (MBI), or Medicaid number, as applicable. Clinical status data include, e.g., the reason for the assessment; dates of the patient's admission, discharge, or transfer to a facility, and the type of facility; the patient's medications, treatments, procedures, health conditions, and diagnoses; and assessments of the patient's hearing, speech, vision, cognitive patterns, mood, behavior, mobility, and nutritional status.

RECORD SOURCE CATEGORIES:

Data in the Outcome and Assessment Information Set is obtained directly from the individual record subject and from home health care clinicians and other providers who are sources of clinical data.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to other disclosures which are authorized directly by the Privacy Act at 5 U.S.C. 552a(b), information about a subject individual may be disclosed from this system of records, without the subject individual's consent, as provided in these routine uses which are published pursuant to 5 U.S.C. 552a(b)(3):

1. To support agency contractors, consultants, or grantees who have been engaged by the agency to assist in the performance of an activity related to this system of records and who need to have access to the records to perform the activity.

2. To assist another federal or state agency, an agency of a state government, or an agency established by state law, or its fiscal agent to:

a. Contribute to the accuracy of CMS's proper payment of Medicare benefits;
b. Enable such agency to administer a federal health benefits program, or as necessary to enable such agency to fulfill a requirement of a federal statute or regulation that implements a health benefits program funded as a whole or in part with federal funds; and/or
c. Evaluate and monitor the quality of home health care and contribute to the accuracy of health insurance operations.

3. To assist an individual or organization for research, evaluation or epidemiological projects related to the prevention of disease or disability, or the restoration or maintenance of health, and for payment related projects.

4. To support Quality Improvement Organizations (QIO) in order to assist the QIO to perform Title XI and Title XVIII functions relating to assessing and improving HHA quality of care.

5. To support national accrediting organizations with approval for deeming authority for Medicare requirements for home health services (i.e., The Joint Commission, the Accreditation

Commission for Health Care, Inc., and the Community Health Accreditation Program). Information will be released to these organizations upon specific request, and only for those facilities that they accredit, that participate in the Medicare program, and that meet the following requirements:

a. Provide identifying information for HHAs that have an accreditation status with the requesting deemed organization;
b. Submit a finder file identifying beneficiaries/patients receiving HHA services;
c. Complete a signed data exchange agreement or a CMS data use agreement; and
d. Safeguard the confidentiality of the data and prevent unauthorized access.

6. To support the Department of Justice (DOJ) or a court or other adjudicatory body when any of the following is a party to litigation or other adjudicative proceedings or has an interest in such proceedings and the agency determines that the records are both relevant and necessary to the proceedings:

a. The agency or any component thereof; or
b. Any employee of the agency in his or her official capacity; or
c. Any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee; or
d. The United States Government.

7. To assist a CMS contractor (including, but not necessarily limited to, fiscal intermediaries and carriers) that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, or abuse in such program.

8. To assist another federal agency or an instrumentality of any governmental jurisdiction within or under the control of the United States (including any State or local governmental agency), that

administers, or that has the authority to investigate potential fraud, waste, or abuse in, a health benefits program funded in whole or in part by federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, or abuse in such programs.

9. To disclose beneficiary-identifiable information to public health authorities, and those entities acting under a delegation of authority from a public health authority, when requesting such information to carry out statutorily-authorized public health activities pertaining to emergency preparedness and response. Disclosures under this routine use will be limited to "public health authorities," "public health activities," and "minimum necessary data" as defined in the HIPAA Privacy Rule (45 CFR 154.502, 164.512(b), 164.502(b) and 164.514(d)(3)(iii)(A)).

10. To disclose to health plans (which are defined for this purpose as plans or programs that provide health benefits, whether directly, through insurance, or otherwise, and which include—(1) a policy of health insurance; (2) a contract of a service benefit organization; and (3) a membership agreement with a health maintenance organization or other prepaid health plan) when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, or abuse in such programs. Disclosures may include provider and beneficiary-identifiable data.

11. Records may be disclosed to appropriate agencies, entities, and persons when (1) HHS suspects or has confirmed that there has been a breach of the system of records; (2) HHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, HHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and

persons is reasonably necessary to assist in connection with HHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

12. Records may be disclosed to another federal agency or federal entity when HHS determines that records from this system of records are reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach; or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

13. To disclose information to a Member of Congress or a Congressional staff member in response to a written inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained. The Congressional office does not have any greater authority to obtain records than the individual would have if requesting the records directly.

Additional circumstances affecting all routine use disclosures:

To the extent that this system of records contains Protected Health Information (PHI) as defined by HHS regulation "Standards for Privacy of Individually Identifiable Health Information" (45 CFR parts 160 and 164, subparts A and E), disclosures of such PHI that are otherwise authorized by the above routine uses may be made only if and as permitted or required by the "Standards for Privacy of Individually Identifiable Health Information." (See 45 CFR 164.512(a)(1).)

In addition, our policy will be to prohibit release even of data not directly identifiable, except pursuant to one of the routine uses or if required by law, if we determine there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals could, because of the small size, use this information to deduce the identity of the patient).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

All records are stored electronically.

POLICIES AND PRACTICE FOR RETRIEVAL OF RECORDS:

Personal identifiers used for retrieval include the subject individual's Medicare Beneficiary Identifier (MBI), Social Security number (SSN), or state assigned Medicaid number if applicable.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records are retained and disposed of in accordance with the following records disposition schedule approved by the National Archives and Records Administration (NARA):

- DAA-0440-2015-0008, Bucket 6, Provider and Health Plan Records, Destroy no sooner than seven years after cutoff but longer retention is authorized.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Safeguards conform to HHS Information Security and Privacy Program, https://www.hhs.gov/ocio/securityprivacy/index.html. The information is safeguarded in accordance with applicable laws, rules, and policies, including the HHS Policy for Information Security and Privacy Protection (IS2P); the CMS Information Systems Security and Privacy Policy (IS2P2); the E-Government Act of 2002, which includes FISMA, 44 U.S.C. 3541 through 3549, as amended by the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. 3551 through 3558; all pertinent National Institutes of Standards and Technology (NIST) Special Publications (SP), the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, subtitle D, §13400-13424, the HIPAA Omnibus Rule (2013), 45

CFR §164.502 and 164.524, the 21st Century Cures Act (2016) §4003,4004 and 4006, the Office of the National Coordinator (ONC) Final Rule on Interoperability and Information Blocking (2020), 45 CFR 171 and the corresponding implementing regulations OMB Circular A-130, Managing Information As a Strategic Resource. Records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include protecting the facilities where records are stored or accessed with security guards, badges and cameras, securing hard-copy records in locked file cabinets, file rooms or offices during off-duty hours, limiting access to electronic databases to authorized users based on roles and two-factor authentication (user ID and password), using a secured operating system protected by encryption, firewalls, and intrusion detection systems, requiring encryption for records stored on removable media, and training personnel in Privacy Act and information security requirements. Records that are eligible for destruction are disposed of using destruction methods prescribed by NIST SP 800-88, as revised.

RECORD ACCESS PROCEDURES:

An individual seeking access to records about him or her must submit a written access request to the System Manager identified in the "System Manager(s)" section. An access request must contain the individual's full name, current address, email address or other contact information, and, for identity verification purposes, signature and date and place of birth. In addition, to verify the requester's identity, the signature must be notarized, or the request must include the individual's written certification that the individual is the person the individual claims to be and understands that the knowing and willful request for or acquisition of a record pertaining to an individual under false pretenses is a criminal offense subject to a fine of up to $5,000. An individual may also request an accounting of disclosures that have been made of the records about the individual, if any.

CONTESTING RECORD PROCEDURES:

An individual seeking to amend a record about him or her must submit a written amendment request to the System Manager identified in the "System Manager(s)" section. The request must contain the same information required for an access request, and must reasonably identify the record, specify the information contested, state the corrective action sought, provide the reasons for the amendment, and include any supporting justification or documentation. The individual must verify his or her identity in the same manner required for an access request. The right to contest records is limited to information that is factually inaccurate, incomplete, irrelevant, or untimely (obsolete).

NOTIFICATION PROCEDURES:

An individual who wishes to know if this system of records contains records about him or her must submit a written notification request to the System Manager identified in the "System Manager(s)" section. The request must contain the same information required for an access request, and the individual must verify his or her identity in the same manner required for an access request.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

72 FR 63906 (Nov. 13, 2007); updated 78 FR 23938 (Apr. 23, 2013); 78 FR 32257 (May 29, 2013); 83 F 6591 (Feb. 14, 2018).

[FR Doc. 2025-13004 Filed: 7/10/2025 8:45 am; Publication Date: 7/11/2025]