de: 4160-15

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Health Resources and Services Administration

Privacy Act of 1974; System of Records

AGENCY: Health Resources and Services Administration (HRSA), Department of Health and Human Services (HHS).

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, as amended, HHS is modifying a system of records maintained by HRSA's Bureau of Health Workforce, System Number 09-15-0054, National Practitioner Data Bank (NPDB).

DATES: This notice is effective upon publication, subject to a 30-day period in which HRSA will accept comments 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 address written comments on the system of records to npdbpolicy@hrsa.gov or by mail, addressed to: Director, Division of Practitioner Data Bank, Bureau of Health Workforce, HRSA, HHS, 5600 Fishers Lane, Mailstop 11SWH03, Rockville, MD 20857.

FOR FURTHER INFORMATION CONTACT: General questions about the revised system of records may be submitted by telephone to 301-443-2300 or by email or mail to David Loewenstein, Director, Division of Practitioner Data Bank, at the addresses listed above.

SUPPLEMENTARY INFORMATION:

I. Background on the National Practitioner Data Bank Information Technology System (NPDB IT System)

The NPDB IT system is a web-based repository of reports containing information on practitioner medical malpractice payments and certain adverse actions related to health care practitioners, providers, and suppliers. Established in 1986, this is a workforce tool that prevents record subjects from moving state to state without disclosure or discovery of previous damaging performance. Federal regulations at 45 CFR Part 60 authorize eligible entities to report to and/or query the NPDB. Individuals and organizations who are subjects of these reports have access to information about them and, unless excepted, information about who accessed reports about them. The reports are confidential and not available to the public. (Information that would reveal whether the NPDB contains a report about a particular individual is generally exempt from disclosure to third parties based on Freedom of Information Act exemptions at 5 U.S.C. 552(b)(3), (6) and/or (7)(C).) The NPDB assists in promoting quality health care and deterring fraud and abuse within health care delivery systems.

The records in the NPDB repository that are about individuals and are retrieved by personal identifier constitute a Privacy Act system of records. Records that are about health practitioners, providers, and suppliers that are entities, not individuals, are outside the scope of the system of records.

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

The NPDB SORN has been modified to reflect a major change in equipment configuration and hosting (i.e., from using a data center to using a cloud environment to improve the availability of the information in the system) and to limit the SORN descriptions more clearly to records about individuals. Formatting changes have also been made to conform to the template prescribed in the current Office of Management and Budget (OMB) Circular A-108. The modifications include:

- Updating the System Location section to reflect that the agency component responsible for the system of records is now the Bureau of Health Workforce instead of the Division

of Practitioner Data Banks, as previously indicated, and that the Bureau's name has changed from "Bureau of Health Professions" to "Bureau of Health Workforce;" to omit the Division's address (because records are not located there); and to describe the current system hosting location as being within a secure cloud service environment (it was previously described as a secure contractor run data center at an undisclosed location).

- Updating the System Manager(s) section to change the official serving as System Manager from the "Director" to the "Deputy Director" of the Division of Business Operations.
- Revising the Authority section to include U.S. Code citations after the name of each Act cited (i.e., 42 U.S.C. 11101-11152, 1320a-7e, and 1396r-2) and to cite to an additional Act's name and the relevant section, namely Section 6403 of the Patient Protection and Affordable Care Act, which amended 42 U.S.C. 1320a-7e and 1396r-2.
- Adding a new paragraph at the start of the Categories of Individuals section stating that the records are about individual health care practitioners, providers, suppliers, and certifying officials and administrators of eligible entities about whom information is maintained in the NPDB IT system; and clarifying that the existing paragraph is describing the "NPDB IT system," (which includes records about both individuals and entities, broader than the system of records).
- Expanding and updating the Categories of Records section to add three record categories (subject profile records, dispute resolution case files, and entity registration records) to the existing two categories (reports, and query histories, now referred to as "query data"); to add one category of information to the description of reports (i.e., "(1) identifying information, such as name, work address, etc."); to omit a list of data elements from the description of reports; and to revise the description of query data to state that it meets Privacy Act accounting of disclosures requirements and to explain why the data available for self-query does not include query activity initiated by law enforcement agencies.

- Updating Record Source Categories by adding a new item (10), individual practitioners, providers, and suppliers when providing data as part of the NPDB Self-Query process.
- In the Routine Uses section, revising six routine uses and removing one unnecessary routine use, as described below:
    - Routine use 1, which authorizes disclosures to hospitals requesting information, has been revised to add "but not limited to" after "such as," and to add "providers and suppliers" to the description of subject individuals who the disclosed information could be about.
    - Routine use 3, which authorizes disclosures to a health care entity with respect to a professional review activity, has been revised to cite 45 CFR 60.3 as the source of the term "professional review activity."
    - Routine use 4, which authorizes certain disclosures to a state licensing or certification authority that requests information in two described situations, has been revised to add the word "all" to limit one of the situations to when the authority requests information in the course of conducting a review of "all" health care practitioners or health care entities.
    - Routine use 8, which authorized disclosures to a health care provider, supplier, or practitioner who requests information about themself, or itself, has been removed as unnecessary, because disclosures to the subject individual do not need to be authorized by publication of a routine use.
    - Routine use 8 (formerly numbered as routine use 9), which authorizes disclosures to a health care entity that queries the system for information itself, has been revised to limit the disclosed information to that which is "otherwise releasable to the entity (e.g., would not reveal a law enforcement investigation)."
    - Routine use 11 (formerly numbered as routine use 12), which authorizes disclosures to the Department of Justice in the event of litigation, has been revised

to include “a court or other tribunal” as an additional disclosure recipient, to change “litigation” to “pending or potential litigation,” and to remove redundant wording about compatibility with the original collection purpose, which repeated part of the definition of a routine use.

    - In routine use 12 (formerly numbered as routine use 13), which authorizes disclosures to the contractor engaged to operate and maintain the NPDB, two examples of operation and maintenance functions have been revised, changing “upgrading hardware and software” to “upgrading infrastructure and software” and changing “performing system backups” to “ensuring that timely system backups are completed.”

- Updating the Storage section, which previously stated that records are maintained “on database servers with disk storage, optical jukebox storage, backup tapes, and printed reports,” to now state that records are maintained “in electronic form, using cloud storage.”
- Updating the Retrieval section as follows:
    - To avoid implying that date of birth, educational information, and “other identifying information” are themselves “personal identifiers” (because they do not fit the description in 5 U.S.C. 552a(a)(5)), and instead explain that “date of birth, educational information, work address, etc.” may be used for retrieval “in combination with” any of the personal identifiers listed;
    - To add Taxpayer Identification Number, Federal Employer Identification Number, Drug Enforcement Agency Number, Unique Physician Identification Number, and National Provider Identifier to the list of personal identifiers; and
    - To revise a note at the end of the section to state that a matching algorithm uses the “personal identifiers” to “match queries to the subjects of NPDB reports”

(instead of stating that the algorithm uses the "data elements" to "match reports to the subject").

- Revising the Retention section, which previously stated that the records are unscheduled and require long term retention, to now identify the applicable National Archives and Records Administration-approved disposition schedule and disposition periods.
- Revising the Safeguards section to add an introductory paragraph and to change the safeguards descriptions as follows:
    - The administrative safeguards description now refers to "organizational" and "non-organizational" users instead of "internal" and "external" users; no longer includes signed disclosure agreements (but continues to include signed Rules of Behavior); refers to "system authorization" instead of "certification and accreditation;" and now includes continuous monitoring and risk assessments.
    - The technical safeguards description states that encryption uses "256-bit SSL" instead of "128-bit SSL" and "meets FIPS 140.2 validation requirements" and adds this statement: "All NIST 800-53 rev 4 control families and Plastic Card Industry Data Security Standard control families selected and implemented are verified by third party auditors."
    - The physical safeguards description now excludes cipher locks, locked hardware cages, and man trap with biometric hand scanner; includes badge reader-controlled access, logging and monitoring of access, and multi-factor authentication mechanisms with door alarming devices that detect if the mechanisms were bypassed upon entering or exiting; and replaces "closed circuit TV" with "professional security staff using surveillance, detection systems, and other electronic means."
- Revising the Record Access Procedures section as follows:

- Updating the opening paragraphs and reorganizing them under the subheadings "Information Available by Self-Query" and "Requests by Electronic Transmission."
- Providing alternative identity verification methods for "Requests by Electronic Transmission" (i.e., online identity proofing, mailing a notarized form, or uploading a notarized form) and mentioning that a fee is charged.
- Revising the "Requests by Mail" instructions to require mailing address to be included, to require the individual's notarized signature for identity verification purposes, and to mention that a fee is charged.
- Revising the "Requests by Telephone" instructions to include steps for obtaining the individual's notarized signature for identity verification purposes.
- Updating the description of the penalty for submitting a request under false pretenses, which previously was up to $11,000 for each violation and is now up to $25,076 per violation as of 2022 and is subject to increase each year based on inflation; and updating the citation to the applicable regulation, which was formerly 42 CFR 1003.103(c) and is now 42 CFR 1003.810.

Because some of these changes are significant, a report on the modified system of records was sent to OMB and Congress in accordance with 5 U.S.C. 552a(r), by the HHS Senior Agency Official for Privacy, or the designee, in accordance with OMB Circular A-108, section 7.e.

Diana Espinosa,

Principal Deputy Administrator.

SYSTEM NAME AND NUMBER:

National Practitioner Data Bank, 09-15-0054.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

A contractor operates and maintains the system through a technical service contract managed by the Bureau of Health Workforce, Health Resources and Services Administration. The technical infrastructure of the system resides in a secure cloud service provider environment. Mail processing and customer service functions associated with the system are conducted at the contractor's secure facility.

SYSTEM MANAGER(S):

Deputy Director, Division of Business Operations, Bureau of Health Workforce, Health Resources and Services Administration, U.S. Department of Health and Human Services, 5600 Fishers Lane, Rockville, MD 20857, npdbpolicy@hrsa.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title IV of the Health Care Quality Improvement Act of 1986, as amended (42 U.S.C. 11101-11152); Section 1128E of the Social Security Act, as amended (42 U.S.C. 1320a-7e); Section 1921 of the Social Security Act, as amended (42 U.S.C. 1396r-2); and Section 6403 of the Patient Protection and Affordable Care Act (amending 42 U.S.C. 1320a-7e and 1396r-2).

PURPOSES(S) OF THE SYSTEM:

The purposes for which records about individuals in the National Practitioner Data Bank information technology system (NPDB IT system) are used are to: (1) receive reports containing information on medical malpractice payments and certain adverse actions, as enumerated in the Categories of Records section below, related to individual health care practitioners, suppliers, and providers; (2) store such reports so that future queriers may have access to pertinent information in the course of making important decisions related to the delivery of health care

services; and (3) disseminate such data to individuals and entities that qualify to receive the reports under the governing statutes as authorized by the Health Care Quality Improvement Act of 1986, Section 1921 of the Social Security Act, and Section 1128E of the Social Security Act to protect the public from unfit practitioners and to prevent fraud and abuse. The NPDB IT system also allows individual practitioners, providers, and suppliers to self-query to access reports about them.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The records in this system of records are about individual health care practitioners, providers, and suppliers, and certifying officials and administrators of eligible entities about whom information is maintained in the NPDB IT system.

Health care practitioners are defined by 45 CFR 60.3 and include, for example, physicians, dentists, nurses, allied health care professionals, and social workers. Health care suppliers are defined by 45 CFR 60.3, and health care providers are defined by 45 CFR 60.3.

CATEGORIES OF RECORDS IN THE SYSTEM:

The records in the NPDB IT system that are about individuals and retrieved by personal identifier are reports, subject profile records, dispute resolution case files, entity registration records, and query data.

Reports include, but are not limited to:

(1) identifying information, such as name, work address, etc.;

(2) medical malpractice payment reports for all health care practitioners (e.g., physicians, dentists, nurses, optometrists, pharmacists, podiatrists, etc.);

(3) adverse licensure and certification action reports taken by states against health care practitioners, health care entities, providers or suppliers;

(4) adverse licensure and certification action reports taken by federal agencies against health care practitioners, providers, or suppliers;

(5) adverse clinical privileging actions reports for physicians, dentists, or other health care practitioners who may have medical staff privileges;

(6) adverse professional society membership action reports for physicians, dentists, or other health care practitioners;

(7) negative actions or findings taken against health care practitioners, health care entities, providers, or suppliers by peer review organizations and private accreditation entities;

(8) federal or state criminal convictions related to the delivery of a health care item or service reports for health care practitioners, providers, or suppliers;

(9) civil judgments related to the delivery of a health care item or service for health care practitioners, providers, or suppliers;

(10) reports of exclusions of health care practitioners, providers, or suppliers from participation in state or federal health care programs; and

(11) other adjudicated actions taken against health care practitioners, providers, or suppliers by federal agencies, state agencies, or health plans.

Query histories (also called disclosure histories) indicate the dates that a health care practitioner's, provider's, supplier's, or entity's report(s) were accessed/queried in the system; by whom; and meet accounting of disclosures requirements in the Privacy Act at 5 U.S.C. 552a(c). An individual practitioner's, provider's, or supplier's report(s) and disclosure history are available to them, if they elect to submit a self-query. However, consistent with the exemptions

established for this system of records pursuant to 5 U.S.C. 552a (k)(2), which exempts all investigative materials (i.e., all law enforcement queries) from certain Privacy Act requirements, including the accounting of disclosures and access requirements at 5 U.S.C. 552a(c) and (d) (1)-(4), the disclosure history will not include disclosures from query activity initiated by law enforcement agencies.

Subject Profile records contain data on subjects of reports, such as address, date of birth, and licensure data extracted from one or more NPDB reports. Subject profiles are used as part of the NPDB matching process to compare and score data on NPDB queries to the data on NPDB subject profile records.

Subjects of NPDB reports may initiate a dispute if they feel the NPDB report is inaccurate or not reportable. NPDB staff adjudicate each dispute based on information collected by the reporter and subject of each report according to the law and regulations. For each dispute that gets elevated to the Health Resources and Services Administration (HRSA), a case file is created containing all the documentation, correspondence, analysis, and a letter that renders a decision to keep the disputed report as-is, to send the disputed report to the reporter for correction, or to void the report altogether so it is not disclosable in response to any query. Dispute cases are occasionally needed for evidence in civil trials. Additionally, content in past cases can be used by NPDB staff as a benchmark or template to help expedite adjudication of future cases.

The NPDB maintains information about individuals in entity registration records to serve two purposes: (1) to ensure that each organization identifies a representative to serve as its certifying official, the individual selected and empowered by an entity to certify the legitimacy of registration for participation in the NPDB; and (2) to establish an entity administrator at each organization who will be in charge of user management and organizational administration for NPDB matters at the organization. For both the certifying official and entity administrator,

entity registration documents are required to verify each representative's identity, prove the entity exists, and verify each representative's affiliation with that entity.

Query data is stored to support the NPDB system, support and track user base activities, and ensure accurate matching processes. All querying activities are tracked, monitored, and stored within the NPDB system in accordance with all federal requirements. Query data includes both data submitted by registered NPDB organizations when trying to retrieve matched NPDB report records and by individual practitioners, providers, and suppliers when using the NPDB Self-Query service that provides individual practitioners, providers, and suppliers with any matched NPDB reports on themselves. Query data includes the same identifying information found in the NPDB report record and subject profile records which supports the NPDB matching and report retrieval processes.

RECORD SOURCE CATEGORIES:

The records contained in the system are submitted by the following entities: (1) insurance companies and others who have made payment as a result of a malpractice action or claim; (2) state health care licensing and certification authorities; (3) federal licensing and certification agencies (e.g., the Drug Enforcement Administration); (4) peer review organizations and private accreditation entities; (5) hospitals and other health care entities (includes professional societies); (6) federal and state prosecutors and attorneys; (7) health plans; (8) federal government agencies; (9) state law and fraud enforcement agencies; and (10) individual practitioners, providers, and suppliers when providing data as part of the NPDB Self-Query process.

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

Information about a subject individual is or may be disclosed from this system of records to parties outside the agency, without the individual's consent, for the following routine uses:

(1) To hospitals requesting information such as, but not limited to, adverse licensure actions, medical malpractice payments or exclusions from Medicare and Medicaid programs taken against all licensed health care practitioners such as physicians, dentists, nurses, podiatrists, chiropractors, psychologists, and providers and suppliers. The information is accessible to both public and private sector hospitals that can request information concerning a physician, dentist, or other health care practitioner who is on its medical staff (courtesy or otherwise) or who has clinical privileges at the hospital, for the purpose of: (a) screening the professional qualifications of individuals who apply for staff positions or clinical privileges at the hospital; and (b) meeting the requirements of the Health Care Quality Improvement Act of 1986, which prescribes that a hospital must query the NPDB once every 2 years regarding all individuals on its medical staff or who hold clinical privileges.

(2) To other health care entities, as defined in 45 CFR 60.3, to which a physician, dentist, or other health care practitioner has applied for clinical privileges or appointment to the medical staff or who has entered or may be entering an employment or affiliation relationship. The purpose of these disclosures is to assess the individual practitioner's qualifications for staff appointment or clinical privileges.

(3) To a health care entity with respect to "professional review activity" (45 CFR 60.3). The purpose of these disclosures is to aid health care entities in the conduct of professional review activities, such as those involving determinations of whether a physician, dentist, or other health care practitioner may be granted membership in a professional society, the conditions of such membership, or changes to such membership; and ongoing professional review activities of the professional performance or conduct of a physician, dentist, or other health care practitioner.

(4) To a state health care practitioner and/or entity licensing or certification authority that requests information in the course of conducting a review of all health care practitioners

or health care entities or when making licensure determinations about health care practitioners and entities. The purpose of these disclosures is to aid the board or certification authority in meeting its responsibility to protect the health of the population in its jurisdiction, and to assess the qualifications of individuals seeking licenses or certifications.

(5) To federal and state health care programs (and their contractors) that request information to aid them in ensuring the integrity of their programs and the professional competence of affiliated health care practitioners and uncovering information needed to make appropriate decisions in the delivery of health care.

(6) To state Medicaid Fraud Control Units that request information to assist with investigating fraud, waste, and abuse and in the prosecution of health care practitioners and providers relating to Medicaid programs.

(7) To utilization and quality control Peer Review Organizations and those entities which are under contract with the Centers for Medicare & Medicaid Services, when they request information to protect and improve the quality of care for Medicare beneficiaries in the course of performing quality of care reviews and other related activities.

(8) To a health care entity that has been reported on, when the entity queries the system to receive information concerning itself and the information is otherwise releasable to the entity (e.g., would not reveal a law enforcement investigation).

(9) To an attorney, or an individual representing themselves, who has filed a medical malpractice action or claim in a state or federal court or other adjudicative body against a hospital, and who requests information regarding a specific physician, dentist, or other health care practitioner who is also named in the action or claim, provided that: (a) this information will be disclosed only upon the submission of evidence that the hospital failed to request information from the NPDB as required by law and (b) the information will be used solely with respect to litigation resulting from the action or claim against the

hospital. The purpose of these disclosures is to permit an attorney (or a person representing themselves in a medical malpractice action) to have information from the NPDB on a health care practitioner, under the conditions set out in this routine use.

(10) To any federal entity, employing or otherwise engaging under arrangement (e.g., such as a contract) the services of a physician, dentist, or other health care practitioner, or having the authority to sanction such individuals covered by a federal program, which: (a) enters into a memorandum of understanding with the U.S. Department of Health and Human Services (HHS) regarding its participation in the NPDB; (b) engages in a professional review activity in determining an adverse action against a practitioner; and (c) maintains a Privacy Act system of records regarding the health care practitioners it employs, or whose services it engages under arrangement. The purpose of such disclosures is to enable hospitals and other facilities and health care providers under the jurisdiction of federal agencies such as the Public Health Service, HHS; the Department of Defense; the Department of Veterans Affairs; the U.S. Coast Guard; and the Bureau of Prisons, Department of Justice, to participate in the NPDB. The Health Care Quality Improvement Act of 1986 includes provisions regarding the participation of such agencies and of the Drug Enforcement Agency.

(11) To the Department of Justice or to a court or other tribunal in the event of pending or potential litigation, for the purpose of enabling HHS to present an effective defense, where the defendant is: (a) HHS, any component of HHS, or any HHS employee in their official capacity; (b) the United States where HHS determines that the claim, if successful, is likely to affect directly the operation of HHS or any of its components; or (c) any HHS employee in their individual capacity where the Department of Justice has agreed to represent such employee, for example in defending a claim against the Public Health Service based upon an individual's mental or physical condition alleged to have

arisen because of activities of the Public Health Service in connection with such individual.

(12) To the contractor engaged by the agency to operate and maintain the system. Operation and maintenance functions include, but are not limited to, providing continuous user availability, developing system enhancements, upgrading infrastructure and software, providing information security assurance, and ensuring that timely system backups are completed.

(13) To a health plan requesting data concerning a health care provider, supplier, or practitioner for the purposes of preventing fraud and abuse activities and/or improving the quality of patient care, and in the context of hiring or retaining providers, suppliers and practitioners that are the subjects of reports.

(14) To federal agencies requesting data concerning a health care provider, supplier, or physician, dentist, or other practitioner for the purposes of anti-fraud and abuse activities and investigations, audits, evaluations, inspections, and prosecutions relating to the delivery of and payment for health care in the United States and/or improving the quality of patient care, and in the context of hiring or retaining the providers, suppliers, and individuals that are the subject of reports to the system. This would include law enforcement investigations and other law enforcement activities.

(15) To appropriate agencies, entities, and persons when (a) HHS suspects or has confirmed that there has been a breach of the system of records; (b) 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 (c) 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.

(16) To another federal agency or federal entity, when HHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in electronic form, using cloud storage.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by any of the following personal identifiers, singly or in combination, and/or in combination with other identifying information, such as date of birth, educational information, work address, etc.:

- Name
- Social Security Number
- Taxpayer Identification Number
- Federal Employer Identification Number
- Drug Enforcement Agency Number
- License Number
- Unique Physician Identification Number
- National Provider Identifier

A matching algorithm uses these identifiers to match queries to the subjects of NPDB reports.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records are maintained and disposed of in accordance with National Archives and Records Administration-approved disposition schedule DAA-0512-2017-0002, available at: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-health-

and-human-services/rg-0512/daa-0512-2017-0002_sf115.pdf, which provides the following disposition periods:

- *Item 1.1 NPDB reports; item 2.1 query transactions; and item 1.3 NPDB subject profile records*: Cutoff at the end of each calendar year and destroy 75 years after cutoff (unless needed longer for legal or business purposes).
- *Item 4.1 NPDB dispute resolution case files*: Cutoff at the close of the case and destroy 50 years after cutoff.
- *Item 5.1 Entity registration records*: Cutoff 50 years after the last (most recent) registration renewal and destroy 50 years after cutoff (unless longer retention is authorized).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Safeguards conform to the HHS and HRSA Information Security and Privacy Program, https://www.hhs.gov/ocio/securityprivacy/index.html. Information is safeguarded in accordance with applicable laws, rules, and policies, including the HHS Information Security and Privacy documents, all pertinent National Institutes of Standards and Technology (NIST) publications, and OMB Circular A-130, Managing Information as a Strategic Resource.

Administrative Safeguards. Authorized users include organizational users, such as government and contractor personnel, who support the NPDB. Organizational users (HRSA users and their contractors) are required to obtain favorable adjudication to hold a public trust position. Government and contractor personnel who support the NPDB must attend annual security training and sign the Rules of Behavior annually. Authorized users are given role-based access to the system on a limited need-to-know basis. All physical and logical access to the system is removed upon termination of employment. Non-organizational users, who are responsible for meeting NPDB reporting and/or querying requirements to the NPDB, are responsible for determining their eligibility to access the NPDB through a self-certification process that requires completing an Entity Registration process. All non-organizational users must re-register every 2

years to access the NPDB. The registration process consists of an electronic authentication process where each user needs to prove their identity and organizational affiliation based on requirements in the NIST SP 800-63 *Digital Identity Guidelines.*

Other administrative safeguards include system authorization that is required every 3 years which authorizes operation of the system based on acceptable risks. Through a continuous monitoring process, security assessments of the security controls implemented are conducted annually to verify compliance with all required controls. In addition, a Risk Assessment is conducted, at least annually, based on NIST SP 800-30 *Risk Management Guide for Information Technology Systems* guidance. Any weaknesses identified during the assessment are documented in the Plan of Actions and Milestones and monitored to effectively reduce risks and vulnerabilities to an acceptable level in accordance with HHS and HRSA policies.

Technical Safeguards. Technical safeguards include firewalls, network intrusion detection, host-based intrusion detection and file integrity monitoring, user identification, data loss prevention, and passwords restrictions. All web-based traffic is encrypted using 256-bit SSL and all network traffic is encrypted internally. All encryption used in the system meets FIPS 140-2 validation requirements. All NIST 800-53 rev 4 control families and Plastic Card Industry Data Security Standard control families selected and implemented are verified by third party auditors.

Physical Safeguards. At the NPDB Operations site, safeguards are in place 24 hours a day, 7 days a week and include picture identification badges, badge reader-controlled access, security guard monitoring, and fire and environmental safety controls. The cloud service provider provides physical safeguards to all its data centers. Physical access to the cloud service provider environment is logged, monitored, and retained. Physical access is controlled at building ingress points by professional security staff using surveillance, detection systems, and other electronic means. Authorized staff use multi-factor authentication mechanisms to access data centers. Door alarming devices are also configured to detect instances where an individual exits or enters

a data layer without providing multi-factor authentication. Alarms are immediately dispatched to the cloud service provider's 24/7 operations center for immediate logging, analysis, and response.

RECORD ACCESS PROCEDURES:

Although this system of records is exempt from the Privacy Act access requirement, the exemption is limited to law enforcement query records and is discretionary. Notwithstanding the access exemption, an individual record subject (individual health care practitioner, provider, or supplier) may seek access to any records about that individual in the NPDB. Access requests will be governed by NPDB-specific access provisions in 45 CFR 60.18 and 60.19.

Information Available by Self-Query. Individuals may generally access records about them over the web by registering to use the NPDB web application(s) and submitting an on-line form (also known as a self-query) or viewing a specific report on-line after being notified via U.S. mail that a report has been submitted to the NPDB and paying a fee. Report subjects will receive, with their self-query response, an accounting of disclosures that have been made of report records about them, if any, excluding any disclosures that were made in response to law enforcement queries (consistent with 5 U.S.C. 552a(c)(3) and the access exemption established for this system of records).

Requests by Electronic Transmission. Alternatively, individuals may submit a written request for records about them, electronically, to the NPDB website. The request must include the same identifying information listed in "Requests by Mail," below and requires paying a fee. For identity verification purposes, the request can be notarized, then mailed to the NPDB address specified in "Requests by Mail" below or uploaded to the NPDB website for processing. Qualified practitioners can also use Experian Precise ID for online identity proofing as an alternative to the paper-based notarization process. Output is delivered via U.S. mail or returned online.

Requests by Mail. As an alternative to making a request by self-query or by electronic transmission, individuals may submit a "Request for Information Disclosure" to the NPDB, P.O. Box 10832, Chantilly, VA 20153-0832 for any report about them. The request must contain the following identifying information: name, address, date of birth, Social Security Number (optional), professional schools and years of graduation, and the professional license(s). For license requests, the following must be included: the license number, the field of licensure, the name of the state or territory in which the license is held and, if applicable, Drug Enforcement Administration registration number(s). The practitioner must submit the completed form, signed and notarized, and pay a fee, before the self-query request will be fulfilled.

Requests in Person. Due to security considerations, the NPDB cannot accept requests in person.

Requests by Telephone. As an alternative to self-query, electronic transmission, or mail, individuals may make an access request by telephone, by providing all of the applicable identifying information listed pertaining to them in "Requests by Mail" above to the NPDB Customer Service Center operator. The NPDB Customer Service Center operator will complete the form and mail it to the practitioner for verification. Once verified, the practitioner must submit the completed form, signed and notarized, and pay a fee, before the self-query request will be fulfilled.

Penalties for Violation. Submitting a request under false pretenses is a criminal offense and subject to a civil monetary penalty (currently up to $25,076 as of 2022, and subject to increase each year based on inflation) for each violation. See 42 CFR 1003.810.

CONTESTING RECORD PROCEDURES:

Because of the system of records' exemptions (described in the below "Exemptions" section), the procedures for disputing an NPDB report will not apply to law enforcement query history information that is exempt from access. All amendment requests will be governed by NPDB-specific amendment provisions in 45 CFR 60.21.

The NPDB mails (based on the address provided in the report) or emails (based on the email address provided by the subject) a notification of any report filed in it to the subject individual. A subject individual may contest the accuracy of information in the NPDB and file a dispute. To dispute the accuracy of the information, the individual must contact the NPDB and the reporting entity to: (1) request that the reporting entity file a correction to the report and (2) request the information be entered into a "disputed" status and submit a statement regarding the basis for the inaccuracy of the information in the report. If the reporting entity declines to change the disputed report or takes no action, the subject may request that the Secretary of HHS review the disputed report. To seek a review, the subject must: (1) provide written documentation containing clear and brief factual information regarding the information of the report, (2) submit supporting documentation or justification substantiating that the reporting entity's information is inaccurate, and (3) submit proof that the subject individual has attempted to resolve the disagreement with the reporting entity but was unsuccessful. HHS can only determine whether the report was legally required to be filed and whether the report accurately depicts the action taken and the reporter's basis for action. Additional detail on the process of dispute resolution can be found in the NPDB regulations, at 45 CFR 60.21.

NOTIFICATION PROCEDURES:

An individual report subject is notified via U.S. mail or email when a report concerning that individual is submitted to the NPDB via Subject Notification Document; however, the mail or email address may not be current. A subject individual may make a notification request, inquiring whether the system of records contains a record about them, in the same manner specified in the "Record Access Procedures" section, above, for making an access request. This procedure is unchanged by the exemption published for the system of records. The procedure is governed by NPDB-specific provisions in 45 CFR 60.18 and 60.19.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Secretary has exempted law enforcement query records in this system of records from certain provisions of the Privacy Act. In accordance with 5 U.S.C. 552a(k)(2) and 45 CFR 5b.11(b)(2)(ii)(L), with respect to law enforcement query records, this system of records is exempt from subsections (c)(3), (d)(1)-(4), (e)(4)(G) and (H), and (f) of 5 U.S.C. 552a. See 76 FR 72325 (Nov. 23, 2011).

HISTORY:

78 FR 47322 (Aug. 5, 2013), 83 FR 6591 (Feb. 14, 2018).

[FR Doc. 2023-06096 Filed: 3/23/2023 8:45 am; Publication Date: 3/24/2023]