US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/16/2016

OPDIV:

HRSA

Name:

BHW National Practitioner Data Bank

PIA Unique Identifier:

P-3956759-017793

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The National Practitioner Data Bank (NPDB) successfully migrated to a virtual Infrastructure as a Service (IaaS) platform and received a FedRAMP Authority To Operate (ATO).

Describe the purpose of the system.

The NPDB is a confidential information clearinghouse created by Congress to improve health care quality, protect the public, and reduce health care fraud and abuse in the U.S.

The NPDB is primarily an alert or flagging system intended to facilitate a comprehensive review of the professional credentials of health care practitioners, providers, and suppliers; the information from the NPDB is used in conjunction with, not in replacement of, information from other sources.

Describe the type of information the system will collect, maintain (store), or share.

Federal law requires that health care entities, hospital, professional societies and state licensing boards report adverse information (health care related convictions and judgments, licensure actions, medical malpractice payments, exclusions from government programs and other adjudicated

actions) on physicians, dentists and other health care practitioners to the NPDB. The information must identify the specific practitioner and is not voluntary.

Why We Collect Your Personal Information:
Information is vital to the existence of the NPDB. Without collecting the information contained in the NPDB our mission could not be fulfilled. This information facilitates the tenants of our mission, including protecting the public and providing quality health care.

We only collect the information received by law that is necessary to fulfill our mission. No other information is collected.

Data used in matching a specific practitioner include:

-Name
-Social Security Number (SSN) / Individual Taxpayer Identification Number (ITIN)
-Federal Employer Identification Number (FEIN)
-Drug Enforcement Agency Number (DEA)
-Fully Qualified State License Number (FQSL)
-Graduation Date
-Data of Birth (DOB)
-Gender
-Unique Physician Identification Number (UPIN)
-National Provider Identifier (NPI)

Address and telephone information is also collected to support mailing of documents and e-mail addresses are collected to facilitate self-service and user communications. Medical notes may optionally be provided as part of the reports collected from the system users.

Legal documents may be provided as part of the dispute resolution process initiated by subjects of reports.

Employment and license termination decision are collected for certain reports associated with termination of privileges but are not used as part of subject matching.

Financial accounts associated with credit cards and Electronic Funds Transfer (EFT) are required to support payment processing for queries.

Credentialing information is not tracked by the system.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The NPDB collects and discloses information to authorized entities on medical malpractice payments, adverse clinical privileges and licensure and other adverse actions taken against physicians, dentists, and other health care practitioners by State licensing authorities, hospitals and professional societies. The NPDB also collects and discloses data to authorized entities on health care related civil judgments and criminal convictions, adverse licensure and certification actions, exclusions from health care programs, and other adjudicated actions taken against health care providers, suppliers and practitioners.

We collect the information used for matching as specified in question 12.

The information must identify the specific practitioner and is not voluntary.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Notes

Financial Accounts Info

Certificates

Legal Documents

Education Records

Employment Status

Taxpayer ID

Federal Employer Identification Number (FEIN)

Drug Enforcement Agency Number (DEA)

Fully Qualified State License Number (FQSL)

Unique Physician Identification Number (UPIN)

National Provider Identifier (NPI)

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Public Citizens

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The NPDB program shares information with the Registered Entities, such as Hospitals and Managed Care Organization in accordance with Federal law. Federal law also mandates the disclosure of the information to specific user groups, such as state and federal Licensing & Certification Authorities. The NPDB uses PII to uniquely/personally identify and match a report to a specific physician, dentist, or other practitioner. To see a complete list of eligible entities and their ability to report and query, please see http://www.npdb.hrsa.gov/resources/aboutGuidebooks.jsp?page=BDefiningEligibleEntities.jsp

Describe the secondary uses for which the PII will be used.

PII is used for test, development, and research purposes. A limited amount of PII is used in test and development as it is required to form accurate test and development cases and verify system functionality. Research requires an extremely limited amount of PII to generate summarized de-identified management reports to HRSA, HHS, and the general public.

Describe the function of the SSN.

Federal law requires that adverse information on physicians, dentists and other health care practitioners be reported to the NPDB. The information must identify the specific practitioner and is

not voluntary. Federal law also mandates the disclosure of the information to specific user groups. The SSN is one of the data elements the NPDB uses to uniquely/personally identify and match a report to a specific physician, dentist, or other practitioner.

Cite the legal authority to use the SSN.

The NPDB regulation 45 CFR 60.7, 60.8, and 60.9 authorizes the collection of SSN in accordance with section 7 of the Privacy Act of 1974. Section 1128E of HIPAA mandates the collection of Individual Taxpayer Identification Numbers (ITIN) as defined in section 7701(a)(41) of the Internal Revenue Code of 1986.

Identify legal authorities governing information use and disclosure specific to the system and program.

--Section 6403 of the Affordable Care Act
--Title IV of Public Law 99-660, the Health Care Quality Improvement Act
--Section 1921 of the Social Security Act, the Medicare and Medicaid Patient and Program Protection Act
--Section 1128E of the Social Security Act, the Health Insurance Portability and Accountability Act

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-15-0054, HHS/HRSA/BHPR

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Online

Government Sources

State/Local/Tribal

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

NPDB: 0915-0126

Expiration Date: May 31, 2016

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Other Federal Agencies

pay.gov - Name, credit card, and bank account information is shared to process credit card and EFT transactions.

State or Local Agencies

State Licensing Boards, for licensing, certifying, or otherwise authorizing physicians, dentists, and other health care practitioners to provide health care services. Law Enforcement officials, to determine the fitness of individuals to provide health care services, and to protect health and safety of individuals receiving health care.

Private Sector

Registered Entities, such as Hospitals and Managed Care Organizations, who are required by law to query as part of their background check when hiring physicians or adding them to insurance networks.

Describe any agreements in place that authorizes the information sharing or disclosure.

Information Sharing Agreement with Financial Management Service (pay.gov).
Agreements with State or Local Agencies or Private Sector are not required, as information is only disclosed to registered entities.

Describe the procedures for accounting for disclosures.

An authorized user can access the NPDB Self Query Service to see if any reports have been submitted about them. In addition, an individual receives a Notification of a Report from NPDB when reports have been submitted about them. This notification alerts the individual that the report will be disclosed to registered entities in accordance with federal law.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The NPDB provides a nationwide database that makes adverse information on physicians, dentists, and other health care practitioners available to health care entities, hospitals, professional societies, and State licensing boards. Also provides information on health care related convictions and judgments, licensure actions, exclusions from government programs and other adjudicated actions. These entities are required to report information to this database, and the individual that is the subject of the report has the ability to receive a copy of the file. Data is shared only with the Registered Entities, and new entities are investigated before receiving access.

Practitioners are notified by mail when they are the subjects of a new report.

We communicate via NPDB Correspondence, quarterly Newsletters, Informational Web Site Postings, and User Review Panel meetings.

The NPDB querying process is an important part of conducting background checks on health care providers before granting clinical privileges.

Practitioners are aware they will likely be queried during this process.

Is the submission of PII by individuals voluntary or mandatory?

Mandatory

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Entities are required to report information to the NPDB, and the individual that is the subject of the report has the ability to receive a copy of the file. There is no option to opt-out. Entities are also required by law to provide PII for querying purposes. There is also not an opt-out alternative for querying the NPDB. An opt-out option would be counter-intuitive to the NPDB mission and purpose of protecting patient safety.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

The NPDB is required to disclose information to authorized organizations in accordance with Federal law. This is not voluntary.

Practitioners are notified if they are the subject of a new report.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

An individual can call the National Practitioner Data Bank customer service center if they have concerns about use of their PII.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Accuracy: Data is reviewed for compliance with reporting requirements. A sophisticated matching algorithm and duality control process ensure queries and reports match properly. Reporting entities can correct inaccuracies any time if inaccuracies are identified. Roles-based permission help ensure data integrity.

Availability: The NPDB Contingency Plan ensures the system will remain accessible in the event of an emergency. Required down time is scheduled during off-peak hours with advance notification.

Confidentiality: Disclosure to the general public is prohibited.

Information may only be disclosed as specified in NPDB regulations.

Integrity: Information is maintained exactly as submitted, and can only be altered in accordance with NPDB guidelines.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Self-Query users enter their PII to access their own reports in the NPDB. Registered entities access PII for reporting and querying.

Administrators:

Administrators use PII in database tables for enhancing and troubleshooting the system.

Developers:

Developers use PII in database tables for enhancing and troubleshooting the system.

Contractors:

Contractors, including administrators, testers, operations staff, and developers, use PII in database tables only for enhancing and troubleshooting the system.

Others:

A select number of HRSA staff may access PII for compliance and disputes efforts.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Self-Query users may only access their own PII. Registered entity users may only query or report based on their NPDB registration permission established by their entity type. Administrators, developers, testers and operations staff; have role-based permissions restricting access to environments on an as required basis only. HRSA compliance and disputes users may access PII according to role-based permissions to support the compliance and dispute business processes only.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Administrator, tester, operator, and developer access is granted based on their specific role. All environments and databases have role-based access for PII.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All users are required to complete annual security awareness training, sign Rules of Behavior, etc. In addition, all users receive weekly security tips.

Describe training system users receive (above and beyond general security and privacy awareness training).

Users with significant security responsibilities are required to complete HRSA's Significant User Training every other year. Significant users include the ISSO, Project Manager, Developers, Database Administrators, and System Engineers.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

NPDB records policy is pending National Archives and Records Administration (NARA) approval. This policy states NPDB reports are permanent records. Both paper and electronic are maintained indefinitely. Data is kept on-line indefinitely and will be stored in the data centers. There are policies in place regarding paper handling or electronic media. Contractors delete instances and snapshots in the server environment to delete PII when no longer needed. AWS controls for destruction of media will be used to destroy media. Cloud service provider personnel do not have direct access to the data, only the underlying infrastructure the data resides on.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

NPDB received an ATO November 7, 2014. NPDB relies on network security controls provided by joint efforts of the contractor and AWS. NPDB implements firewalls (AWS Security Groups) and host base intrusion detection (AlertLogic) to secure the NPDB perimeter. Boundary entry points are controlled by AWS Security Groups, AWS Virtual Private Cloud isolation, and protected by AlertLogic Threat Detection to prevent unauthorized access. All traffic to the NPDB web servers is encrypted using 2048 bit SSL in the production environment. The NPDB system uses pay.gov to process credit card transactions. It is an Internet system where the NPDB originates Secure Hyper Text Transfer Protocol (HTTPS) requests for billing and receives HTTPS responses.

All PII is secured through the use of multiple secured AWS data centers referred to as availability zones AWS controls the underlying hardware in the virtual environment. The contractor (SRA) controls the virtual environment configuration residing in the virtual internment. All transmission of PII is secured via 2048 bit encrypted FIPS 140-2 compliant mechanisms.

The NPDB system supports external (end-user) and internal user groups that are controlled by permissions, rights, and level of access. External users must enter a valid User Id, Password, and Databank Identifier in order to access the system.

Employees of the covered entities are advised of the legal consequences of misuse of NPDB information. NPDB personnel (internal users) are briefed on the sensitivity of NPDB information and the requirements for its protection. Prior to gaining access, employees are required to sign the NPDB Non-Disclosure Statement, acknowledging understanding of their responsibilities and consequential penalties for non-compliance. External users (customers) are required to sign

registration forms before they are granted access to the system. Upon accessing the web site, users are also informed, via sign-on warnings, that unauthorized use can subject the user to fine and imprisonment under Federal Statute. The contractor shall comply with existing federal and departmental laws, regulations, and requirements.
Physical access controls are in place at AWS data centers that meet NIST 800-53 guidelines. Technical and physical controls are managed by AWS or SRA, as defined in the System Security Plan.