PTA / PIA: HRSA - NPDB - QTR3 - 2025 - HRSA1446081

Created Date: 7/29/2025 12:25 PM Last Updated: 11/28/2025 3:24 PM

General Information

PTA / PIA Name:	HRSA - NPDB - QTR3 - 2025 - HRSA1446081	**PTA / PIA ID:**	3567989
Component Name:	HRSA - National Practitioner Data Bank	**ATO Boundary Name:**	National Practitioner Data Bank
Overall Status:	Complete	**# of Days - Open:**	149
Submitter:		**Submit Date:**	7/30/2025
Next Assessment Date:	11/27/2028	**Expiration Date:**	11/27/2028
Office:		**OpDiv:**	HRSA
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	5/10/2024
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Olufunmilayo Fayese
PTA 01A:	POC Title and Organization	ISSO
PTA 01B:	POC Email Address	OFayese@hrsa.gov
PTA 01C:	POC Phone Number	301-443-2905
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	No major changes impacting the PIA or system security have occurred since the last PIA.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The National Practitioner Data Bank (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.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	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. The information must identify the specific practitioner and is not voluntary. NPDB Reports and Subject Profiles are stored for 75 years. Query Transactions, Compliance & Research Data, Dispute Resolution Case Files, and Entity Registration Forms are stored for 50 years.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Username Password Email Address CAC Card

PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	Federal law requires that health care entities, hospital, professional societies and state licensing boards report adverse information on physicians, dentists and other health care practitioners to the NPDB. Information includes: Name, Work Address, Home Address, Social Security Number or Individual Tax Identification Number, Date of Birth, Year or Graduation, Professional License Number(s), Field of Licensure, Physician Specialty, Name of the state or territory in which the license is held, Drug Enforcement Administration (DEA) registration numbers, National Provider Identifier (NPI), Names of each hospital with which the practitioner is affiliated ,Name and address of the entity making the payment, Name, title, and telephone number of the official responsible for submitting the report on behalf of the entity and details of the adverse action information contained in the NPDB report such as length of judgment and date of judgment.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	www.npdb.hrsa.gov iqrs.npdb.hrsa.gov
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes

PTA 09:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	The purpose of the NPDB website at www.npdb.hrsa.gov is to provide the capabilities to support the reporting and querying activities on adverse actions on medical practitioners, providers, and suppliers. The website supports the registration of entities and identity proofing of users, querying, reporting including disputed reports, and compliance monitoring activities on the reporting entities. Who has access to the website: Individual practitioners, suppliers, and providers: Query on themselves and dispute reports the individual is a subject of. Registered Entities Users: Report and query on adverse actions based on the laws that define the NPDB. HRSA Staff: Supports report compliance and the disputed report processes. NPDB Contractor Staff: Supports the customer service operations and system activities on a daily basis. General Public: Access public information associated with the purpose of the NPDB and how to use the web site. How users access the website: Individual practitioners, suppliers, and providers: Access the public and restricted website applications over the Internet after identity verification and using MFA. Registered Entities: Access the public and restricted website applications over the Internet after identity verification and using MFA. HRSA Staff: Access Compliance and Disputes web applications using MFA via government issued Personal Identity Verification (PIV) card. NPDB Contractor Staff: Access the website using Zscaler Private Access remote access solution with MFA.
PTA 10:	Does the website have a posted privacy notice?	Yes
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	Yes
PTA 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	Yes
PTA 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Web bug/beacons- Does Not Collect PII

PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	Yes
PTA 21A:	What are the AI tools and how are they used?	Amazon Q – Generative AI-powered Assistant is used to summarize customer service center calls. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Social Security Number Taxpayer ID Number (TIN) Financial Account Information (e.g., account numbers, credit card numbers) Biographical Information Name Date of Birth Certificates (e.g., training certificates) Education Records Employment Status/History Legal Documents Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Email Address (Business) Mailing Address (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Medical Notes, 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)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999

PIA 25:	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 go to http://www.npdb.hrsa.gov/resources/aboutGuidebooks.jsp?page=BDefiningEligibleEntities.jsp
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	PII is used for test, development, and research purposes. Limited PII is used for system development and testing to verify system functionality. Extremely limited PII is used to generate summarized de-identified management reports to HRSA, HHS, and the general public.
PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	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.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	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.
PIA 28:	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
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes

PIA 29A:	Please specify which PII data elements are used to retrieve records.	-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) -Unique Physician Identification Number (UPIN) -National Provider Identifier (NPI)
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	SORN: 09-15-0054 - National Practitioner Data Bank (NPDB) https://www.federalregister.gov/documents/2023/03/24/2023-06096/privacy-act-of-1974-system-of-records
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Hard Copy Mail/Fax Online Government Sources State/Local/Tribal Other Federal Entities Non-Government Sources Members of the Public Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	New OMB Control Number 0906-0081 Expiration Date 01/31/2027
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies Private Sector State or Local Agency/Agencies

PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	Other Federal Agencies: pay.gov - Name, credit card, and bank account information is shared to process credit card and Electronic Funds Transfer (EFT) transactions. 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. 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.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	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.
PIA 32D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	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.
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Mandatory
PIA 33A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	--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
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	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.

PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	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.
PIA 36:	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. If no process exists, explain why not.	The NPDB provides a robust dispute resolution processes via the Report Response Service, Subject Notification Documents which are sent to individual practitioners, and the ability for reporting entities to make corrections. In addition, an individual can call the National Practitioner Data Bank customer service center if they have concerns about use of their PII.
PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	Data Accuracy: Data is reviewed for compliance with reporting requirements. A complex matching algorithm process ensure queries and reports match properly. Reporting entities can correct any inaccuracies identified at any time. Data Availability: Changes to the database are maintained for 7 days with automatic replay to any point in time within the 7 day span. Weekly instance snapshots are copied and automatically replicated to 3 data centers in AWS US East and US West for potential restoration of data in case of any disruptions. Object based storage is replicated across both AWS US East and US West regions to further ensure data availability. Data Integrity: Information is maintained exactly as submitted, and can only be altered in accordance with NPDB guidelines. A file integrity monitoring solution is used to monitor all virtual instances associated with NPDB. All system activity is audited and analyzed with automated alerting mechanisms when anomalies associated with integrity occur. Data Relevancy: This is maintained by following the specific retention and destruction schedules.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors Others
PIA 38A:	Select the type of contractor.	Third-Party Contractor (Contractors other than HHS Direct Contractors)
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 38C:	Identify the additional person(s) who will have access to the PII in the system not mentioned in the list above.	None

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	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. Federal Staff: A select number of HRSA staff may access PII for compliance and disputes efforts.
PIA 40:	Describe the administrative 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.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Principle of least privilege - Administrator, tester, operator, and developer access is granted based on their specific roles. All environments and databases have role-based access to PII.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All users are required to complete the annual security awareness training and sign Rules of Behavior.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	All team members receive annual security training that discusses their responsibility when handling and protecting PII. Periodic technical, job- training is conducted on an as needed basis or as required by system changes. This specialized training may take the form of vendor seminars, security-related product demonstrations and conferences, professional technical association and user group meetings.

PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The Records Management Plan specifies the minimum retention period for temporary and permanent disposition items. The minimum retention period for temporary records are: NPDB Reports and Subject Profiles — 75 years Query Transactions, Compliance & Research Data, Dispute Resolution Case Files, and Entity Registration Forms — 50 years The only permanent records are the Public Use files, which will be transferred to NARA every 5 years when the newest records in the transfer are 15 years old.

PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Security controls are provided by joint efforts of the NPDB contractor and Amazon Web Services (AWS) cloud provider. Administrative Safeguards: Government and contractor personnel who support the NPDB must obtain favorable adjudication for a Level 5 Position of Public Trust, must complete annual security training with Rules of Behavior acknowledgment, are assigned role-based access to the system on a limited need-to-know basis, and have all physical and logical access to the system removed upon termination of employment. Users responsible for reporting and/or querying to the NPDB must determine their eligibility to access the NPDB by completing a registration process, must acknowledge the Rules of Behavior, and must complete the registration process every two years. The registration process is based on the National Institute of Standards and Technology (NIST) SP 800-63-3 Digital Identity Guidelines. Every 3 years the system must be authorized to operate based on acceptable risks, and security controls and risks are assessed every year. Technical Safeguards: Include firewalls, network intrusion detection, malware detection and prevention, secure remote access driven by policy-based rules, and file integrity monitoring, Distributed Denial of Service prevention, data loss prevention, encryption at rest, E-mail security, identity proofing and multifactor authentication enforcement. 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 control families and Plastic Card Industry Data Security Standard (PCI DSS) control families selected and implemented are verified by third party auditors. Physical Safeguards. AWS provides physical safeguards at all data centers and include access monitoring and logging, professional security staff utilizing surveillance and detection systems, multi-factor authentication access mechanisms, and 24/7 alarm monitoring by AWS Security Operations Centers.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	9/30/2025
Privacy Analyst Review Comments:	For PIA 32B, please spell out the EFT acronym to say Electronic Funds Transfer (EFT).	**# of Days - PA Review:**	62

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	10/15/2025
SOP Review Comments:		**# of Days - SOP Review:**	15

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	11/24/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 11/24/2025 AI Review completed, this PIA is ready for SAOP review and approval. 7/30/2025 Please see comments and update accordingly: PTA-4: Please spell out acronym "NPDB" the first time its being use. PTA-21A: Please include the AI Statement in your response it should read "Amazon Q – Generative AI-powered Assistant is used to summarize customer service center calls. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks." PIA-32B: Please spell out acronym "EFT" the first time its being used.	**# of Days - APA Review:**	40

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	11/28/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	4

SAOP Signature

Date	User	Type	Name	Original Value	New Value
11/28/2025 12:08 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 04	Data Feed Service, pta_pia_HSRSA_Release	10/15/2025	PTA-4 - update completed, the acronym NPDB has already been spelt out, please see the details under PTA-4, thank you	
PTA 04	VILLAFUERTE, NESTOR	10/15/2025	PTA-4 - update completed, the acronym NPDB has already been spelt out, please see the details under PTA-4, thank you	
PTA 04	VILLAFUERTE, NESTOR	10/15/2025	PTA-4 - update completed, the acronym NPDB has already been spelt out, please see the details under PTA-4, thank you	
PTA 04	BLAND, CRYSTAL	10/15/2025	PTA-4 - update completed, the acronym NPDB has already been spelt out, please see the details under PTA-4, thank you	
PTA 04	BLAND, CRYSTAL	10/15/2025	PTA-4 - update completed, the acronym NPDB has already been spelt out, please see the details under PTA-4, thank you	11-24-2025 Email_RE_ AI PIA Review_HRSA1446081.pdf