US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/20/2025

OPDIV:

IHS

Name:

IHS National Patient Information Reporting System (NPIRS)

PIA Unique Identifier:

P-3904086-331244

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.

Agency

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.

National Patient Information Reporting System (NPIRS) has been moved from the Division of Information Technology (DIT) to the Division of Data Management and Analytics (DDMA). We have expanded the service capabilities across the NPIRS ecosystem.

Describe the purpose of the system.

The National Patient Information Reporting System (NPIRS) is the reporting environment for the Indian Health Services (IHS) and consists of a National Data Warehouse (NDW) and a myriad of functional data marts. The NPIRS environment was developed in 1986 and the purpose of NPIRS is to provide an Enterprise Business Intelligence/Analytic environment that enables reporting, data discovery, data mining, predictive analysis and trending of key performance indicators in support of patient care and patient care management by providing strategic actionable information to managers at all levels of the Indian Health Services to allow them to better manage individual patients, local facilities, regional and national programs. NPIRS additionally provides IHS the ability to produce

reliable and timely reports in support of statutory, regulatory, and administrative obligations, including user population counts, workload reporting, accreditation, and performance measures.

The NPIRS environment employs industry best practices around methodologies, processes and architectures that support the transformation of raw data into meaningful and useful information in the Indian Health Services (IHS) Business Intelligence (BI) environment. NPIRS supports delivery of executive dashboards, ad-hoc reports and predictive analytic solutions as well as maintenance and oversight of the National Data Warehouse and various functional reporting data marts

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

The NPIRS system collects information from the Indian Health Services electronic health record system that is covered by a separate PIA. Additional information is collected from tribal and urban operated non-RPMS COTS electronic health record systems. Health and medical records containing examination, diagnostic and treatment data, proof of IHS eligibility, social data (such as name, address, date of birth, Social Security Number (SSN), tribe), laboratory test results, and dental, social service, domestic violence, sexual abuse and/or assault, mental health, and nursing information.
Follow-up registers of individuals with a specific health condition or a particular health status such as cancer, diabetes, communicable diseases, suspected and confirmed abuse and neglect, immunizations, suicidal behavior, or disabilities.
Logs of individuals provided health care by staff of specific hospital or clinic departments such as surgery, emergency, obstetric delivery, medical imaging, and laboratory.
Surgery and/or disease indices for individual facilities that list each relevant individual by the surgery or disease.

Third-party reimbursement and billing records containing name, address, date of birth, dates of service, third party insurer claim numbers, SSN, health plan name, insurance number, employment status, mother maiden name, medical record number, medical notes, military status, veteran status insurance eligibility, and Prescriber National Provider Identifier and other relevant claim information necessary to process and validate third-party reimbursement claims.
Contract Health Service (CHS) records containing name, address, date of birth, dates of care, Medicare or Medicaid claim numbers, SSN, health plan name, insurance number, employment status, and other relevant claim information necessary to determine CHS eligibility and to process CHS claims.
There is a requirement to submit personal information and includes Behavioral Health data to include pharmacy and prescription information and data that supports of public health nursing initiatives.
The NPIRS environment employs industry best practices around methodologies, processes and architectures that support the transformation of raw data into meaningful and useful information in the Indian Health Services (IHS) Business Intelligence (BI) environment. NPIRS supports delivery of executive dashboards, ad-hoc reports and predictive analytic solutions as well as maintenance and oversight of the National Data Warehouse and various functional reporting data marts.

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

The National Patient Information Reporting System (NPIRS) is the reporting environment for the Indian Health Services (IHS) and consists of a National Data Warehouse (NDW) and a myriad of functional data marts. The NPIRS environment was developed in 1986 and the purpose of NPIRS has always been to produce accurate and timely reports that are required by statute and regulation and provide a broad range of clinical and administrative information to managers at all levels of the Indian Health Services to allow them to better manage individual patients, local facilities, regional and national programs.

The National Patient Information Reporting System (NPIRS) consist of a database of healthcare information gathered from all the associated direct Indian Health Service (IHS), Tribal, and Urban

healthcare sites and regional administrative offices of the Indian health system. These include over 500 healthcare sites and 12 regional offices in 39 states. The data in the NDW comes from government and commercial healthcare information systems that are largely transaction-based, utilized at the local level to support the provision of patient care, as well as from other specified sources (e.g. IHS Fiscal Intermediary, Social Security Administration). The data includes demographic data; third-party eligibility information; patient-based clinical data (e.g., health factors); and encounter-based clinical data (e.g., purpose of visit, procedures, medications, laboratory test results, radiological results). Historical records of change are also maintained to support historical reporting as required.

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
Mother's Maiden Name
Mailing Address
Medical Records Number
Medical Notes
Military Status
Employment Status
Veterans Status Insurance Eligibility
Medicare or Medicaid Claim Numbers
Health Plan/Insurance Name
Inpatient/Outpatient Prescription Name, Dispensed Amount, Prescription Date, Dosage Amount, Prescriber National Provider Identifier
National Drug

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

Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients
No

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The primary purpose for using Personally Identifiable Information (PII) in the NPIRS environment is to support healthcare operations and public health functions while ensuring compliance with legal and policy requirements.

Specifically, PII is used to:
Provide health services to individuals by IHS and its contractors.
Support law enforcement and public health reporting (e.g., crimes, communicable diseases, child abuse).
Enable data processing and maintenance by authorized contractors and volunteers.
Share statistical and demographic information with internal and approved external entities in compliance with HIPAA and privacy safeguards."

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

PII is utilized for internal training, testing or research purposes.

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

P.L. 94-437, as Amended, 925 U.S.C. 1662, Section 602, 1880,1913; and E.O. 9397."

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.

09-17-0001 - Medical, Health, and Billing Records Systems.

Identify the sources of PII in the system.

Government Sources

Within OpDiv

State/Local/Tribal

Other Federal Entities

Identify the OMB information collection approval number and expiration date

OMB approval not required

Is the PII shared with other organizations?

Yes

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

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

Any sharing of information from the National Data Warehouse environment, is only release with the appropriate Data Sharing Agreements Memorandum of Understanding/Agreements (MOU/MOA), ISA and approval by both legal and the privacy office. Business Associate Agreements (BAA) are leveraged to support data sharing with tribes and urban programs.

Describe the procedures for accounting for disclosures.

The IHS, with respect to each system of records under its direct control (i.e., Privacy Act System of Record 09-17- 0001, Medical, Health, and Billing Records) must keep a record of the date, nature, and purpose of each disclosure of a record to any person or Agency under subsection (b) of the Privacy Act (5 U.S.C. § 552a) and the name and address of the person or Agency to whom the disclosure is made. This record must be kept for 5 years or the life of the record; whichever is longer, after the disclosure for which the accounting has been made. An individual (beneficiary) is entitled, upon request, to get access to this disclosure record of his or her own personal records with the exception for disclosures made under subsection (b) (7) of the Privacy Act (as a result of civil or criminal law enforcement activity). The IHS must inform any person or other Agency about any correction or notation of dispute made by the IHS in accordance with subsection (d)(4) of the Privacy Act (Access of Records) of any record that has been disclosed to the person or Agency if an accounting of the disclosure was made. This is a mandatory reporting requirement and may be recorded utilizing the IHS-505, "Disclosure Accounting Record" form.

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

Indian Health Manual - Part 2, Chapter 7 - It is IHS policy to provide adequate notice of its uses and disclosures of PHI and of the individual's rights and IHS' legal duties with respect to PHI. A copy of the Notice is provided to new patients, patients whose charts are reactivated, and patients who reach legal age. The Patient Registration Office provides a copy of the current Notice to the patient. The staff member has the patient acknowledge receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. The signed "Acknowledgement of Receipt of IHS Notice of Privacy Practices" is filed into the patient's medical record.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

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.

Individuals can choose not to present to an Indian Health Service facility for their healthcare.

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

It is IHS policy to provide adequate notice of its uses and disclosures of Public Health Information/Personally Identifying Information (PHI/PII) and of the individual's rights and IHS' legal duties with respect to PHI/PII. The IHS prominently and clearly displays the Notice (2-7.18) in every facility (http://www.hipaa.ihs.gov/). A copy of the Notice is also provided to new patients, patients whose charts are reactivated, and patients who reach legal age. The Patient Registration Office or other appropriate department provides a copy of the current Notice to the patient. The patient acknowledges receipt of the Notice by signing the Acknowledgment of Receipt of IHS Notice of Privacy Practices. An IHS staff member signs and dates the Acknowledgment form and files the signed "Acknowledgment of Receipt of IHS Notice of Privacy Practices" into the patient's medical record. No less than every three years, IHS provides notification of the availability of the Notice and how to obtain the Notice. If the Notice is revised by a material change, the revised Notice must be posted in clear and prominent locations in every facility and on its web site, on or after the effective date of the revision. The revised Notice will be posted on the IHS website within the 60 days of a material revision. The revised Notice is also given to all patients who come into a facility after the effective date of the revision and is available upon request on or after the effective date of the revision. Additionally, IHS provides the revised notice to all eligible patients registered in the patient registration system within 60 days of the revision of the Notice. Any individual, whether or not a patient, has the right to request and receive a copy of the Notice at any time, except an inmate. Inmates have no rights to the Notice (45 CFR § 164.520 (a)(3)).

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.

All complaints are addressed to the Service Unit Chief Executive Officer or (his or her) designee for investigation. Complaints are documented, maintained, and filed, and include a brief explanation of resolution, if any. Note: Complaints may also be filed directly with the Secretary, DHHS.

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

Automated data verification and validation processes are automatically executed monthly to ensure the health and confidence of the data persisted in the NPIRS data stores. These automated administrative and housekeeping processes apply various business rules to ensure data is accurate, secure and available for reporting. Privacy and Security conduct initial and recurring reviews of PII information contained in resulting results for various user communities.

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

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

The Information Technology Access Control (ITAC) supervisors are responsible for submitting appropriate access requests for IHS system users on their team and for reviewing their team members' access. The System Administrator then grants the most restrictive access privileges needed to perform job related roles and responsibilities.

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.

The system utilizes least privilege and role-based access controls. Access is granted to a limited number of authorized administrators, developers, direct contractors, and federal employees. Standard users do not have access to 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.

Any user that access a reporting solution developed by NPIRS, has to go through both Security and Privacy guidelines. That includes, but is not limited to the user submitting an ITAC for access and approval by the ISO that the user has required security training for access approval. - Role-based training, IHS Rules of Behavior agreements, and Information System Security and Privacy Awareness training courses are required to be completed annually by all IHS users.

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

All users must complete the training as defined by the agencies security and privacy divisions before they are permitted access to any NPIRS reporting solution.

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.

NPIRS is not the authoritative source system of information. NPIRS collects information from electronic health record systems and serves as the custodian of information to support enterprise reporting. The data used by NPIRS is transitory and will be destroyed in accordance with source system disposition schedule, which to date, includes retaining data for 75 years. In compliance with IHS Records Retention Schedule, Medical Records, DAA-0513-2014-0003

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

Administrative controls: The system utilizes least privilege and role-based access controls.
Technical controls: Active Directory user access control, and Microsoft BitLocker full disk encryption.
Physical controls: physical access controls in the Albuquerque Data Center (ADC) will be utilized to secure the ticketing system's PII.