US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/21/2025

OPDIV:

IHS

Name:

PATH EHR

PIA Unique Identifier:

P-6870847-023303

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Development

Is this a FISMA-Reportable system?

No

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?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

The PATH EHR system is a commercial off the shelf electronic health record system that is being used to replace the existing EHR system in use in IHS which is being retired after approximately 40 years of service in order to enhance security, provide better performance, and expand the usability of collected health data to both providers and patients.

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

1) Health and medical records containing medical records number, examination, diagnostic and treatment data, proof of IHS eligibility, demographic data (such as name, address, phone number, email address, date of birth, Social Security Number (SSN), tribe, mother's maiden name, military veteran status), clinical assessments, dental treatment records, behavioral health data, implanted medical device identifiers, and prescribed medication information.

2) 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.

3) Logs of individuals who have been provided health care by staff of specific hospital or clinic departments such as surgery, emergency, obstetric delivery, medical imaging, and laboratory.
4) Surgery and/or disease indices for individual facilities that list each relevant individual by the surgery or disease.
5) Emergency Department log book, clinical imaging, monitoring strips and tapes such as fetal monitoring strips and EEG and EKG tapes.
6) Third-party reimbursement, billing and financial records containing name, address, date of birth, dates of service, third party insurer claim numbers, SSN, health plan name, insurance number, employment status, and other relevant claim information necessary to process and validate third-party reimbursement claims.
7. Purchase Referred Care (PRC) 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 PRC eligibility and to process PRC claims.
8. Organization and Provider Information, such as Provider License #, Taxpayer ID, and Drug Enforcement Agency (DEA) Provider ID.
9. Legal documents - Scanned images of IHS 810 Authorization for Use or Disclosure of Protected Health Information, Driver's License, Tribal Identification Card.

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

PATH EHR is a centralized integrated solution for management of both clinical and administrative information in healthcare facilities operated by the IHS. Flexible hardware configurations, over 50 software applications, and network communication components combine to create a comprehensive clinical, financial, and administrative solution; a solution that can stand alone or function in concert with other components as needed. Professionals in American Indian, Alaska Native, and private sector health facilities use PATH E HR every day to efficiently manage programs, maximize revenue generation, and most important, to provide high-quality care for patients.
1) Health and medical records containing medical records number, examination, diagnostic and treatment data, proof of IHS eligibility, demographic data (such as name, address, phone number, email address, date of birth, Social Security Number (SSN), tribe, mother's maiden name, military veteran status), clinical assessments, dental treatment records, behavioral health data, implanted medical device identifiers, and prescribed medication information.
2) 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.
3) Logs of individuals who have been provided health care by staff of specific hospital or clinic departments such as surgery, emergency, obstetric delivery, medical imaging, and laboratory.
4) Surgery and/or disease indices for individual facilities that list each relevant individual by the surgery or disease.
5) Emergency Department log book, cClinical imaging, monitoring strips and tapes such as fetal monitoring strips and EEG and EKG tapes.
6) 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, and other relevant claim information necessary to process and validate third-party reimbursement claims.
7. Purchase Referred Care (PRC) 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 PRC eligibility and to process PRC claims.
8. Organization and Provider Information, such as Provider License #, Taxpayer ID, and Drug Enforcement Agency (DEA) Provider ID.

9. Legal documents - Scanned images of IHS 810 Authorization for Use or Disclosure of Protected Health Information, Driver's License, Tribal Identification Card.

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
Driver's License Number
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Legal Documents
Device Identifiers
Military Status
Employment Status
Taxpayer ID

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients
n/a

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

1. To serve as the official documentation of an individual’s healthcare.
2. To provide a description of an individual’s diagnosis, treatment and outcome, and to plan for immediate and future care of the individual.
3. To serve as a means of communication among members of the health care team who contribute to the individual’s care. This includes Federal and non-Federal (public or private) health care providers that provide health care services to IHS individuals, to whom information is disclosed in accordance with applicable law for purposes of planning for or providing such services, or reporting results of medical examination and treatment.
4. To support access to individual health information by authorized users through health information exchange.
5. To improve the health of populations and communities by providing insights at the population level for immunizations, disease screening and prevention, and disease surveillance.
6. To process and collect third-party claims and facilitate fiscal intermediary functions and to process debt collection activities.

7. To support the ability of clinicians and facilities to participate in government quality and incentive payment programs through quality and performance measures generated from PATH EHR
8. To support the ability of the IHS to understand and report on the success of its mission through quality and performance measures and related metrics derived from PATH EHR data.
9. To train authorized users of PATH EHR on system features, functions, and enhancements, to improve user performance.

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

1. To contribute to continuing education of IHS staff to improve the delivery of health care services.
2. Research activities carried out in collaboration with academic or government institutions, as authorized and monitored by regional and national Institutional Review Boards (IRB).
3. PII may be shared with school health care programs that serve AI/AN for the purpose of student health maintenance.
4. PII may be shared with correctional institutions as necessary to support appropriate care for AI/AN individuals.
5. PII may be shared to provide relevant health care information to funeral directors or representatives of funeral homes to allow necessary arrangements prior to and in anticipation of an individual's impending death.
6. The Centers for Disease Control and Prevention may use these records to monitor various communicable diseases.
7. By state agencies or other entities acting pursuant to a contract with CMS, for fraud and abuse control efforts, to the extent required by law or under an agreement between IHS and respective state Medicaid agency or other entities.
8.For the Bureau of Indian Affairs (BIA) or its contractors under an agreement between IHS and the BIA relating to disabled AI/AN children for the purposes of carrying out its functions under the Individuals with Disabilities Education Act (IDEAS), 20 U.S.C. 1400, et seq.
9. Records may be disclosed to organizations deemed qualified by the Secretary of DHHS and under a business associate agreement to carry out quality assessment/improvement, medical audits, utilization review or to provide accreditation or certification of health care facilities or programs.
18. Records may be disclosed under a business associate agreement to individuals or authorized organizations sponsored by IHS to conduct analytics and evaluation.

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

Departmental Regulations (5 U.S.C.301); Privacy Act of 1974 (5 U.S.C. 552a); Federal Records Act (44 U.S.C. 2901); Section 321 of the Public Health Service Act, as amended (42 U.S.C. 248); Section 327A of the Public Health Service Act, as amended (42 U.S.C. 254a); Snyder Act (25 U.S.C. 13); Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.); Transfer Act of 1954 (42 U.S.C. 2001–2004); HIPAA, HITECH (and subsequent regulations); and 21st Century Cures Act, 42 CFR Part 2.

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.

2/14/2018

Privacy Act System of Record 09-17- 0001, Medical, Health, and Billing Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Other

Identify the OMB information collection approval number and expiration date

Not Applicable

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Other Federal Entities

Other

Non-Governmental Sources

Public

Private Sector

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.

Depending on the external entity and applicable law, authority to share/disclose PII from PATH EHR may be covered by Business Associate Agreements (BAA), a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) with entities that are not Covered Entities or Business Associates under the Health Insurance Portability and Accountability Act (HIPAA), the Data Use and Reciprocal Support Agreement (DURSA) for Health Information Exchange (HIE) intermediaries and participants, Interconnection Security Agreements (ISA), Organized Healthcare Arrangements, or others. Individual facilities may have standard agreements in place such as: Organized Health Care Arrangement (OHCA), Qualified Service Organization Agreement (QSOA), Economy Act Agreements, ISA, Data Use Agreement (DUA), DURSA, BAA, or any other agreements at the local level. In specific cases, disclosure will occur in response to patient or proxy Release of Information requests, court orders, or subpoenas.

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.

All transmissions of patient information from the PATH EHR occur either electronically or via hard copy, either to entities that have completed binding agreements and rigorous technical testing, or to clinician users who are employed by those entities, appropriately credentialed and authenticated to access this information. The PATH EHR system logs all connections, queries, and responses to those queries, and retains these logs in accordance with applicable 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.

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.

All non-IHS entities (Tribal Health Programs and urban Indian healthcare organizations) that connect to the IHS PATH EHR are obligated under HIPAA to provide notices of privacy practices to their patients. They are further obligated under the Multi-Purpose Agreement that governs their connections to the PATH EHR to confirm their commitment to and compliance with applicable laws and regulations concerning such notices.

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.

Per the policy provided in the Indian Health Manual Part 2 Chapter 7 Section 22, "Under the HIPAA Privacy Rule, patients have the right to request restriction(s) of the use and/or disclosure of their PHI to carry out treatment; payment and health care operations; inpatient hospital directory; and disclosures to relatives, family members, personal representatives, close friends, health care givers, and any other person involved in the patient's care or payment who is identified by the patient. The IHS is not required to agree to the request. However, a patient still may object to the disclosure of information for the inpatient hospital directory and to relatives, friends, and others involved in patient care under 45 CFR 164.510(b). See Section 2-7.19, "Procedure for the Uses and Disclosures of Protected Health Information for Involvement in the Patient's Care and for Notification Purposes."

The initial collection of PII occurs at the various healthcare facilities at the point of registration and is required to determine eligibility for services. All patients at all facilities are provided with a Notice of Privacy Practices. They are also offered Form IHS-810, "Authorization for Use or Disclosure of Protected Health Information". By completing and signing this document, patients may consent to or

decline sharing of their protected health information with external entities outside the I/T/U ecosystem through the 4DH and eHealth Exchange.

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 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 Acknowledgement form and files the signed "Acknowledgement 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.

Part 2 Chapter 7 Section 8 "Procedure for Requests for Correction/Amendment of PHI" of the Indian Health Manual provides the policy and procedures for patients to report inaccurate data and request correction.

Individual Service Units are responsible for addressing concerns, and the patient may escalate to higher authority, e.g., the IHS Privacy Act Officer. Patients may file complaints directly to the Secretary, HHS through the OCR HIPAA website (under the authority of the HIPAA Privacy Rule)

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.

Per Part 3, Chapter 3, Section 9J - Health Record Alterations and Modification. Electronic progress notes, operative reports, and discharge summaries are occasionally entered by practitioners in the Text Integration Utility (TIU) and the Electronic Health Record (EHR) software for the wrong patients, or the information within the document(s) may be erroneous. A local procedure, following the EHR for Health Information Management (HIM) Guide found at here, must be established for correcting erroneous patient information entered electronically. It is the responsibility of the HIM to ensure there is a process in place to correct erroneous health record information. Refer to Indian Health Manual Exhibit 3-3-A Comparison of Update, Administrative Correction, Addenda, and Amendment Requests.

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.

Per the Indian Health Manual Part 8 Chapter 19 Least Privilege - It is the policy of the IHS that each IT user will be authorized the most restrictive set of privileges or access needed for performing authorized tasks. All elevated system privilege accounts must be controlled and limited to Office of Information Technology (OIT) support personnel, Area Information Systems Coordinators (ISC), or their designated alternates.
Scope. This policy applies to all IHS information system users, owners, custodians, and business associates, as well as access to any IHS information system. Authorized personnel who have a legitimate need to use those resources shall be granted access to specific IT resources in the performance of job duties or responsibilities. Any access privilege granted will be limited only to the information resources required to do the job.

Indian Health Manual, Part 8, Chapter 21 - Access Control
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.

Per Part 8, Chapter 19 - Least Privilege - 19.3
PROCEDURES

Elevated System Privilege Accounts. All IT users with elevated system privilege accounts will be controlled and limited to those individuals with a true business need for access.
Specific Access Privileges. Users must be granted specific access privileges on each system, limited to those privileges required to perform their job functions and responsibilities. Supervisors must analyze the duties performed by their employees to verify that users only have the system privileges that are needed to perform their assigned duties.
Authorized Access. Users will only access resources to which they have been authorized, regardless of actual system permissions.
Unauthorized Access. Users will not circumvent the permissions granted to their accounts in order to gain access to unauthorized information resources.
Periodic Review. System Administrators, System Owners, and the ISSO will periodically review user privileges and modify, revoke, or deactivate access as appropriate.
Site Emergencies. In the event of a site emergency, it is possible that staff will need to be provided with elevated system privilege user access to perform trouble shooting activities. In this situation, the ISC is responsible for ensuring that all compromised passwords are changed and access is removed immediately following the resolution of the emergency.

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.

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.
Information Systems Security Awareness Training. All Users must complete the Information Systems Security Awareness (ISSA) training annually. New employees must complete ISSA training prior to or within 24 hours of gaining access to IHS information systems unless the user has read the IHS Quick Guide to Information Security or risk access deactivation.
Rules of Behavior. During a user's completion of ISSA training, the individual must review and accept the IHS Rules of Behavior (RoB) which is stored and tracked in the ISSA training system. Some users may also be responsible for completing role-based or system-based training and must acknowledge any specifically related RoB, such as, the RoB for privileged users.
Supervisors are required to validate user training compliance during the Annual Access Review, including ISSA training and any required role-based training.
In addition, all users of PATH EHR, which includes not only PII but also PHI, are required to take HIPAA Privacy, HIPAA Security, and Privacy Act Basics training annually. All staff that work with Substance Use Disorder patients or their records are required to take training concerning the provisions of 42 CFR Part 2 on an annual basis.

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

The Office of Information Technology provides application training for a variety of applications per the approval of the user's supervisor. All applications have a user manual for reference. Training classes reiterate the necessary security and privacy requirements for all applications. Subject courses can be found on IHS.gov.

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.

Records Retention Schedule Number DAA-0513-2014-0003, sequence 0003, titled "Health Records File. Electronic Health Record." cites the Retention Period as follows: "Destroy/delete 75 years after last episode of patient care or date of death."

Emergency Department Log book, Clinical imaging, monitoring strips and tapes such as fetal monitoring strips and EEG and EKG tapes disposition schedule is 3-13. 3-14, 3-18, and 3-20 are under revision.

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

IHS Administrative policies for storing, retrieving, accessing, retaining, and disposing of records in the system

Physical Controls: Records are kept in locked metal filing cabinets or in a secured room or in other monitored areas accessible to authorized users at all times when not actually in use during working hours and at all times during nonworking hours. Magnetic tapes, disks, other computer equipment (e. g., pc workstations) and other forms of personal data are stored in areas where fire and life safety codes are strictly enforced. Telecommunication equipment (e.g. computer terminal, servers, modems and disks) of the PATH EHR are maintained in locked rooms during nonworking hours. Network (Internet or Intranet) access of authorized individual(s) to various automated and/or

electronic programs or computers (e.g., desktop, laptop, handheld or other computer types) containing protected personal identifiers or
personal health information (PHI) is reviewed periodically and controlled for authorizations, accessibility levels, expirations or denials, including passwords, encryptions or other devices to gain access. Combinations and/or electronic pass cards on door locks are changed periodically and whenever an IHS employee resigns, retires or is reassigned.
Technical Controls: Users are limited to access, based on assigned roles in the system that are utilized for signing on the system, Single Sign On with PIV required to access the system.