US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/16/2025

OPDIV:

IHS

Name:

Lab Analyzers IHS wide

PIA Unique Identifier:

P-4554816-590702

The subject of this PIA is which of the following?

General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

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)?

No

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

Describe the purpose of the system.

Laboratory analyzers are used to perform various tests on patient samples to assist healthcare providers with diagnosis and treatment.

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

Laboratory analyzers transmit the following information: patient name, date of birth, medical record number, laboratory test results, and the date the test was performed. The analyzers receive data from the Indian Health Service Resource Patient Management System (RPMS) through the laboratory middleware, and the middleware then transmits the information to the analyzer. These three systems—RPMS, laboratory middleware, and the analyzer—work together in an integrated workflow.

Personally identifiable information (PII) is stored temporarily on the analyzer. Each analyzer can store a predetermined number of data lines, as specified by the manufacturer. A single line contains

PII and associated test information (test name, result, and date/time performed) for one patient sample. Once the storage limit is reached, new entries overwrite the oldest ones. For example, if an analyzer can store 500 lines and all lines are full, the 501st sample will replace the 1st (oldest) sample. The system does not collect or store any user credentials.

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

Prior to testing, laboratory staff receive the sample in the Indian Health Service (IHS) Resource Patient Management System (RPMS), which links the sample and the ordered tests to the appropriate analyzer through the laboratory middleware. When a sample is placed on the analyzer, it performs the required test(s). Once testing is complete, the patient results are transmitted back to RPMS via the laboratory middleware.

The analyzer receives Personally Identifiable Information (PII) and test information (test name, result, and date/time performed) through its connection to the laboratory middleware. The middleware then provides the same information to RPMS.

The analyzer, laboratory middleware, and RPMS operate using uni-directional or bi-directional connections that utilize standard HL7 messaging. These systems exchange PII and test information electronically via TCP/IP connections. TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of communication protocols that enables devices on a network to communicate with one another.

HL7 (Health Level Seven) is a standardized messaging language used in healthcare to exchange electronic patient data among different systems—such as analyzers, laboratory middleware, and RPMS—serving as a universal format for sharing medical information across applications.

RPMS PIA: P-4381853-884031, Resource Patient Management System
Laboratory Middleware PIA: P-4796196-841511, Laboratory Interface Middleware
Laboratory Middleware TPWA: T-9450702-377278, Laboratory Middleware."

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

Yes

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

Date of Birth
Name
Medical Records Number
Medical Notes
Device Identifiers
Each analyzer is assigned a device identifier and is provided at the time of installation.
Lab Results

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

Employees
Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of the PII used in laboratory analyzers is to enable automated testing of patient specimens (such as blood, urine, or other biological samples) and to generate accurate, timely diagnostic results. Laboratory analyzers use this information to automate testing processes and deliver reliable results that support clinical decision-making."

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

N/A

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.

Privacy Act of 1974; Report of Amended or Altered System; Medical, Health and Billing Records System. https://www.govinfo.gov/content/pkg/FR-2010-01-12/pdf/2010-285.pdf.

IHS SORN for Medical, Health and Billing Records System. 09-17-0001

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.

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within the OPDIV

State/Local/Tribal

Other Federal Entities

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

N/A

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.

N/A

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.

According to the Indian Health Manual, Part 2, Chapter 7, it is IHS policy to provide adequate notice of its uses and disclosures of PHI, as well as the individual's rights and the agency's legal duties regarding PHI. A copy of the Notice of Privacy Practices is provided to new patients, patients whose charts are reactivated, and patients who have reached legal age. The Patient Registration Office supplies the current Notice to the patient, and staff obtain the patient's acknowledgment of receipt by having them sign the Acknowledgment of Receipt of the IHS Notice of Privacy Practices. The signed acknowledgment is then filed in 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.

ndian 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.

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

HS policy requires 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.

All complaints are addressed to the Service Unit Chief Executive Officer, or a 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.

Complaints are documented, maintained, and filed, and include a brief explanation of resolution, if any.

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.

ndian 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.

The System Administrator grants the most restrictive access privileges needed to perform job related roles and responsibilities.

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.

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

In person orientation and competency on the system; as well as annual Privacy training.

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."

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

Administrative Controls: IHS.gov Privacy Policy Statement: Applies to all IHS webpages and outlines how PII and PHI are collected, used, and protected. IHS does not collect PII or PHI unless voluntarily provided by the individual. Any personal information willingly submitted is protected by established security practices. Non-personal information related to website visits may be automatically collected and temporarily stored. IHS does not disclose, give, sell, or transfer personal information unless required by Federal law or law enforcement. Health Information Privacy Requirements Users are directed to the HHS Office for Civil Rights and the IHS HIPAA Office for information regarding HIPAA Privacy and Security Rule protections. Privacy Act Requirements Individuals are informed of their rights under the Privacy Act of 1974.Information and assistance regarding Privacy Act compliance may be obtained from an IHS Privacy Official.

Technical Controls: Technical safeguards protect PII stored or processed by the system: Active Directory User Access Control Provides authentication, authorization, and role-based access to ensure only approved users may access PII.
Microsoft BitLocker Full Disk Encryption Encrypts system drives to prevent unauthorized access to PII in the event of device loss, theft, or compromise.

Physical Control: The physical environment hosting the system employs the following safeguards: Albuquerque Data Center (ADC) Physical Access Controls-Access to the data center is restricted to authorized personnel only. Physical security controls protect the servers and infrastructure housing the ticketing system’s PII from unauthorized entry