US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/30/2025

OPDIV:

IHS

Name:

PACS IHS

PIA Unique Identifier:

P-2711307-368253

The subject of this PIA is which of the following?

Electronic Information Collection

Identify the Enterprise Performance Lifecycle Phase of the system.

Requirements Analysis

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.

A Picture Archiving and Communication System (PACS) is a digital imaging system used in healthcare (IHS) to capture, store, distribute, and display medical images.

Virtual machines are used to reduce the overall system footprint by storing medical diagnostic images and interfacing patient identification with the Electronic Health Records (EHR) for permanent storage.

A comprehensive installation, service and support agreement for PACS equipment with licenses, servicing of applications and hardware for all IHS Staff.

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

The personally identifiable information (PII) data collected is the patient name, date of birth, medical record number, test results, and device identifier. IHS Staff will access the PACS system via username/password, PIV, and/or Active Directory

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

A Picture Archiving and Communication System (PACS) is a digital imaging system used in healthcare (IHS) to capture, store, distribute, and display medical images.

Virtual machines are used to reduce the overall system footprint by storing medical diagnostic images and interfacing patient identification with the Electronic Health Records (EHR) for permanent storage.

The personally identifiable information (PII) data collected is the patient name, date of birth, medical record number, test results, and device identifier. IHS Staff will access the PACS system via username/password, PIV, and/or Active Directory.

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
Device Identifiers
Test results
User credentials

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?

To identify the patients and link the images to their medical record.

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.

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Other

Government Sources

Within OPDIV

State/Local/Tribal

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

NA. This system is exempt from an OMB Information Collection Number through Public Law 114-255 / 21st Century Cures Act, Section 2035: Exemption for the IHS from the Paperwork Reduction Act requirements.

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.

Contract for Radiologist analyzing images and outside physicians consulting diagnosis and treatment.

Describe the procedures for accounting for disclosures.

The requester and its agents will establish HIPAA and Privacy Act specific safeguards to ensure the confidentiality and security of individually identifiable records or record information.

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

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.

The only method to opt out is for the patient not to receive healthcare from the IHS.

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.

The process for reporting suspected unauthorized access or disclosure of PII is through the IHS privacy incident reporting process, which is available online. In addition each IHS health facility has a process for patient complaints.

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

Periodic reviews are performed to ensure compliance with privacy regulations, including Privacy Act, HIPPA and Government Act of 2002, at various time-frames based on area.

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.

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

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. In this case, only personnel with RPMS lab access keys will have access to PII.

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.

Access to PII is assigned to personnel based upon current job responsibilities. Indian Health Manual,

Part 8, Chapter 21 - Access Control 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 (least privileges and role base access).

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).

Operational training for use and system viability

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.

The PACS system stores the PII data according to the records retention schedule.
The PII associated with the patient information in this system becomes part of the patient's Electronic Health Record. 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: All personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.

Technical Controls: Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Physical Controls: The information technology (IT) hardware used to host protected information is located in a secured IHS facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.