

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/11/2025

OPDIV:

IHS

Name:

Network Printers

PIA Unique Identifier:

P-2126517-200774

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)?

Yes

Indicate the following reason(s) for updating this PIA.**Describe the purpose of the system.**

A network printer is a device that listens for requests from different computers or laptops. Documents are sent from the computer to the printer for hard copy printing. Printers can also be used to make copies, scan documents to other computer users and to fax documents to other departments or outside businesses. Printers to contain an internal hard drive that temporarily stores information and collects data about the printer such as number of printed pages, error logs and configuration information.

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

Printers do not collect data but they do produce documents that can contain PHI/PII from users that send requests to be printed, scanned, or copied. Printers can fax documents containing PHI/PII to departments or outside businesses. Scanners can send documents containing PHI/PII to folders within the secure network.

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

A network printer can collect, maintain or temporarily store information related to print jobs, scanning, copying, emailing and faxing of documents. This includes information such as the content of the printed documents, printing preferences, and user data for tracking usage. Information is stored temporarily for efficient printing and printers do not permanently maintain sensitive data. All staff use printers for replication of patient data, appointments, patient records, insurance information, tribal identification, HIPAA forms, patient consents and employment information.

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

Photographic Identifiers

Driver's License Number

Biometric Identifiers

Mother's Maiden Name

Vehicle Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Certificates

Legal Documents

Education Records

Device Identifiers

Military Status

Employment Status

Foreign Activities

Passport Number

Taxpayer ID

Tribal enrollment number.

System does not ask for this however end users will be printing this information.

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

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

Printing patient information is necessary for record keeping, documentation and communication within the facility or for outside sources. These are medical records, prescriptions, or treatment plans that are essential for healthcare providers to provide accurate and coordinated care for patients. Printed records are also used as a back up when the electronic system fails.

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

Testing and training.

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

Snyder Act (25 U.S.C. 13); Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.); and the Transfer Act of 1954 (42 U.S.C. 2001-2004).

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Identify the OMB information collection approval number and expiration date

None. No OMB approval required.

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Other Federal Entities

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.

Not Applicable.

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.

Patients can seek care at another health care facility.

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.

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.

Quarterly, semiannual and annual reviews.

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

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.

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 and separate privacy training.

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

System users receive training on specific policies, procedures and tools to ensure the safeguarding of sensitive information, secure data handling practices and the importance of maintaining confidentiality. Additionally, users are educated on the legal and compliance aspects of PHI/PII. Regular updates and refresher courses ensure users stay informed about evolving security measures and best practices.

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.

No PII stored on system.

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

Active Directory user access control, Microsoft BitLocker full disk encryption, and physical access controls in the Albuquerque Data Center (ADC) will be utilized to secure the ticketing system's PII. Note: web address is a hyperlink.

