

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/27/2025

OPDIV:

IHS

Name:

Health Facilities Data System

PIA Unique Identifier:

P-6939442-993603

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?

No

Does the system include a Website or online application available to and for the use of the general public?

Yes

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.**

The Healthcare Facilities Data System (HFDS) is a centralized tool used by the Indian Health Service (IHS) to:

Track and account for Government and Tribal real property assets.

Distribute funds to Maintenance & Improvement (M&I) and Biomedical Equipment (E) program managers.

Manage the backlog of facility deficiencies through FEDS (Facilities Engineering Deficiency System).

Monitor energy usage across facilities.

Report to Congress and external agencies.

Justify funding levels and support requests for budget increases.

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

The HFDS collects and maintains data including the following:

1. Real property data including attributes relating to an Installation/Site and its associated building(s), land and structure(s). Data includes attributes such as Installation name and address, building

number, size and age.

2. Lease information for government owned leases and GSA leases.

3. Manage each facility's backlog of deficiencies (BEMAR). This includes any item that needs to be repaired or replaced (e.g. life safety hazards, handicap accessibility, mechanical, electrical, etc.)

4. Track energy usage including what each area is doing to conserve energy.

5. Calculate and track funds to be distributed from the annual congressional appropriation for maintenance and improvement activities (M&IE) in federally owned buildings where tribally owned space is used to provide healthcare services.

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

FDS is a public-facing web application requiring login access. Users are authenticated via Structured Query Language (SQL) Server, with most linked to D1 network credentials and others using standalone SQL logins. Access is restricted by geographic region and role-based permissions, controlling data visibility and editing rights. The system uses a ColdFusion front-end with a SQL Server backend, hosted in the Bureau of Indian Affairs (BIA) data center and managed by IHS Office of Information Technology (OIT).

The HFDS collects and maintains data including the following:

1. Real property data including attributes relating to an Installation/Site and it's associated building (s), land and structure(s). Data includes attributes such as Installation name and address, building number, size and age.

2. Lease information for government owned leases and GSA leases.

3. Manage each facility's backlog of deficiencies (BEMAR). This includes any item that needs to be repaired or replaced (e.g. life safety hazards, handicap accessibility, mechanical, electrical, etc.)

4. Track energy usage including what each area is doing to conserve energy.

5. Calculate and track funds to be distributed from the annual congressional appropriation for maintenance and improvement activities (M&IE) in federally owned buildings where tribally owned space is used to provide healthcare services

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

Yes

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

Name

E-Mail Address

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

Employees

Vendor/Suppliers/Contractors

Tribal Members

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The purpose of the PII being to establish user name and password to login to the application.

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

Testing the application and training the users.

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

25 USC §1632 and 25 USC 450

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.

GSA-GOVT-10

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Identify the OMB information collection approval number and expiration date

None/Local/Tribal

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.

Individuals can choose not to use the application. IHS does not offer an alternative.

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.

System administrators periodically reviews user account , privileges and roles for accuracy and currency.

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.

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

Users are receiving system specific training based on user roles.

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.

When a user account is removed from the system, all associated PII is permanently deleted from the database server. All records will be dispositioned under DAA-0513-2015-0007 Records retention Schedule, destroy after 5yrs.

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.

Identify the publicly-available URL:

<https://facilops.ihs.gov/hfds/>

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null