US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/27/2025

OPDIV:

IHS

Name:

Web Services

PIA Unique Identifier:

P-1528933-000447

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?

Yes

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)?

Yes

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

Describe the purpose of the system.

IHS Web Services hosts and maintains Internet, Intranet and SharePoint web sites for IHS. These are for public dissemination of health information, IHS activities and for a variety of applications including and limited to workflow management for various custom applications, inventory management, training, financial management, career opportunities and management. All servers are located at the Bureau of Indian Affairs (BIA) Datacenter in Albuquerque, NM. IHS Web Services internet sites have IHS employees and contractors, Tribal members and general public as the user base. Intranet and SharePoint sites are accessible only for users within the IHS network.

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

PII collected: Name (First and Last), Social Security Number (SSN), Date of Birth (DOB), Email Address, Phone number, Certificates, Education Records, Financial Account information, Legal documents, and User credentials.

For access control the public citizens used username and passwords. IHS employees and Direct

Contractors use HHS user credentials to access servers and username/password to access Admin section.

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

IHS Web Services hosts and maintains Internet, Intranet and SharePoint web sites for IHS. These are for public dissemination of health information, IHS activities and for a variety of applications including and limited to workflow management for various custom applications, inventory management, training, financial management, career opportunities and management.

PII information collected are Name (First and Last), Social Security Number (SSN), Date of Birth (DOB), Email Address, Phone number, Certificates, Education Records, Financial Account information, Legal documents, and User credentials are collected for contact information, proof of identity (document an applicants identity), financial management, training, career opportunities, inventory management, accessing applications, and to control access.

Using PII serves several purposes: it documents an applicant's identity, describes their application status, aids in the approval process by administrators, helps diagnose submission issues, and verifies incident data while supporting follow-up discussions to address and mitigate security and privacy incidents.

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
E-Mail Address
Phone Numbers
Financial Accounts Info
Certificates
Legal Documents
Education Records
Login Credentials

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

Public Citizens

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Using PII serves several purposes: it documents an applicant's identity, describes their application status, aids in the approval process by administrators, helps diagnose submission issues, and verifies incident data while supporting follow-up discussions to address and mitigate security and privacy incidents.

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

Secondary uses for PII are User Acceptance Testing and troubleshooting/diagnosing issues with application.

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.

09-17-0004 Indian Health Service Sanitation Facilities Construction Individual Applicant Records

09-17-0002 Indian Health Service Scholarship and Loan Repayment Programs

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Email

Online

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Other

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

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.

There are no formal agreements in place. IHS as an Operating Division of the Department of Health and Human Services (DHHS) is required to share certain information with Headquarters.

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.

Users can opt out by not using Web Services.

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.

Web Services conducts User Acceptance Testing during pre-deployment and conducts post-deployment reviews and an annual risk assessment of the security controls (as part of the Authorization to Operate process) of the Web Services system to ensure data integrity, availability, accuracy, and relevancy.

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).

Records Management, Privacy (HIPAA) 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.

The retention and destruction of Personally Identifiable Information (PII) in our system is governed by NARA-approved records retention schedules and follows established federal guidelines for records management.
PII maintained in the system falls under the following General Records Schedules (GRS):

• GRS 3.1, item 020 (DAA-GRS-2013-0005-0004): This applies to administrative records related to routine operations, including PII in correspondence and tracking systems. These records are scheduled for destruction 3 years after they are superseded or become obsolete, but longer retention is authorized if required for business use.
• GRS 3.2, item 030 (DAA-GRS-2013-0006-0003): This applies to PII contained in records created during the user identification and authorization process for access to systems. Under this schedule, records are retained until business use ceases.

These retention schedules are followed to ensure compliance with federal requirements for protecting and managing PII throughout its lifecycle. Destruction of PII is carried out in accordance with approved methods, including secure shredding or digital sanitization, once the retention period

has expired or business use no longer justifies retention.
For additional details and the full list of applicable records retention schedules, please refer to the Indian Health Service Records Disposition Schedule:
https://www.ihs.gov/DRPC/recordsmanagement/dispositionschedule/

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

Administrative Control: All contractors and employees are required to complete Security Awareness training every year.
Contractors accessing servers need to complete Role Based Training (RBT) require enhanced privilege cards (ALT card) .

Technical control: PII information/fields are encrypted in database tables and uses Microsoft BitLocker full disk encryption. Websites are https only. Active Directory user access control(s) are in place to limit access.

Physical control: All servers are located at the BIA Datacenter in Albuquerque, NM. protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199. We follow agency guidelines and mandates regarding data security.

Identify the publicly-available URL:

www.ihs.gov

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?

No

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 uner the age of thirteen?

No

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

Yes

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

Yes