

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/01/2020

OPDIV:

IHS

Name:

IHS Secure Video and Web Conferencing

PIA Unique Identifier:

P-4166785-603444

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)?

No

Describe the purpose of the system.

IHS Secure Video and Web Conferencing is an Encrypted voice and video communications for use by the Agency, allowing connections through the Trusted Internet Connection to outside users for the provision of telehealth.

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

The system collects call log files and call statistics, duration, packet loss, network addresses, communication speed etc. There is an option to record calls, if enabled, and that is stored on an encrypted server inside the Indian Health Service network. A request to retrieve the recorded call has to be initiated to the system administrators. The system is encrypted from end to end and nothing more than call statistics is stored, unless the call is recorded. Those recordings are stored on an encrypted server that only the system administrators have access to. The recording feature is not to be used during patient visits. If it were used, it would record the pictures of the provider and the patient along with the audio heard during the meeting.

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

The system is a phone and video system with secure web based communication capabilities. It allows for device voice and video communications from multiple types of devices. IHS staff can initiate communications within IHS and with external patients and providers. The public (outside of IHS) would receive a link from the IHS staff member to join a call.

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

Phone Numbers

Device Identifiers

IHS username and password

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

Employees

Public Citizens

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?

The purpose is to connect employees, doctors, or patients to one another via voice and video.

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

Testing, Training, and Collaboration

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

Indian Health Care Improvement Act, Snyder Act

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

Email

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

Not Applicable

Is the PII shared with other organizations?

No

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.

To not use the service.

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.

Periodic review daily to ensure the system and service is accurate and functioning properly.

Identify who will have access to the PII in the system and the reason why they require access.

Administrators:

To administrate the system and ensure availability.

Developers:

To administrate the system and ensure availability.

Contractors:

Direct, to administrate the system and ensure availability.

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).

Department specific privacy awareness 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.

Retention and destruction will be in line with GRS 4.2: Information Access and Protection Records Item 130: Personally Identifiable Information Extracts. Emails from the system will be destroyed every 30 days in conjunction with GRS 5.2: Transitory and Intermediary Records, Item 010 – Transitory records.

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 will be utilized to secure the system's PII. At a high level, the data and recordings are stored on a recording server that is encrypted with BitLocker. The data in transmission is encrypted, as well as at rest. Only the system administrators (2 in the agency) can retrieve these recordings and provide access for playback. Both of those administrators have Public Trust background investigations, have privileged administrative accounts, and requests for those videos are made to them in writing.

Identify the publicly-available URL:

<https://join.meet.ihs.gov/>

This URL is used by IHS staff to initiate a call. A unique URL is generated for each call.

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?

No

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?

Yes

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

No