US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/17/2017

OPDIV:

IHS

Name:

Information Security Ticketing

PIA Unique Identifier:

P-3775076-347465

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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?

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.

The purpose of the Information Security Ticketing system is to enable IHS users to report Information Technology IT security and privacy incidents to the IHS Cybersecurity Incident Response Team (CSIRT) and the IHS Privacy Team. The tickets contain key information regarding the incident such as date/time of incident, incident summary, detailed incident description, and incident mitigation.

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

The Information Security Ticketing system will collect and store users' contact information including user names, first and last names, work location (facility name), phone numbers, and email addresses. The system will also contain information related to specific incidents such as device information (e.g., Internet Protocol IP address), attempted breaches, isolated malicious code, and date/time of incident, and may contain names and titles of individuals associated with specific incidents. Though not requested or required, reporters of incidents often inadvertently include patient name, date of birth, chart number and medical notes. Legal documents are specific to Office of Inspector General Requests for information. Specifically OI-2 forms from OIG inspectors.

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

The Information Security Ticketing system will collect and store users' contact information including user names, first and last names, work location (facility name), phone numbers, and email addresses. The system will also contain information related to specific incidents such as device information (e.g., ip address), attempted breaches, isolated malicious code, and date/time of incident, and may contain names and titles of individuals associated with specific incidents. The system will also limit potential damage of incidents, raise awareness about threat vectors, protect the agency against cyber vulnerabilities, and restore systems where attacks are successfully launched. The collection and analysis of IT security and privacy incidents will allow the agency to develop protective measures to prevent/protect from cyber attacks, and also to develop response/restoration strategies. Legal documents are specific to Office of Inspector General Requests for information. Specifically OI-2 forms from OIG inspectors.

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

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Legal Documents

Device Identifiers

Employment Status

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The collection of Personally Identifiable Information PII allows the IHS CSIRT to verify reported incident data and engage in follow-on discussions to respond to and mitigate the impact of IT security and privacy incidents.

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

Research will be a secondary use for which the PII will be used in the ticketing system. Although Protected Health Information (PHI) , Social Security Numbers (SSN), and Dates of Birth (DOB) are not requested, users may inadvertently submit this type of information. In these cases, the information will not be used or shared but merely stored.

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

Health Insurance Portability Accountability Act 45 CFR 164.530 and The Privacy Act of 1974. Office of Management and Budget (OMB) M-06-19 requires the collection of certain information associated with incident reporting.

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 used to cover the system or identify if a SORN is being developed.

IHS Medical, Health and Billing Records (#09-17-0001).

Identify the sources of PII in the system.

Email

Online

Government Sources

Within OpDiv

Other Federal Entities

Identify the OMB information collection approval number and expiration date

5 U.S.C. § 301 and 44 U.S.C. § 3101 authorizes the collection of this information.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

HHS Headquarters

Other Federal Agencies

Department of Homeland Security United States Computer Emergency Readiness Team - DHS US-CERT

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 and DHS US-CERT serves as the central reporting point for all federal information security incidents, required by The Federal Information Security Management Act (FISMA), and designated in OMB M-06-19.

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?

Mandatory

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.

There is no option to object to the information collection as FISMA and OMB M-06-19 require incident reporting.

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.

The agency conducts post-incident reviews and an annual risk assessment of the security controls (as part of the Authorization to Operate process) of the ticketing 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.

Users:

Users will be able to access and view their ticket submissions.

Administrators:

For data integrity.

Developers:

For data integrity and testing purposes.

Contractors:

Direct contractors will need access to the system to review, analyze, and mitigate incidents.

Others:

IHS authorized federal employees will need access to the system to validate and authorize mitigation actions.

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).

IHS Division of Information Security (DIS) Information System Security Officer (ISSO) 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 information collected in the system shall be governed by the mandatory instructions found in General Records Schedule (GRS) 3.2, Item 020: Computer Security Incident Handling, Reporting and Follow-Up Records. Incident files shall be cut off at the end of the calendar year. Files shall be deleted from the system 3 years from the date all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.

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.