Indian Health Service

Managing Your Privacy Office

HEATHER MCCLANE/BRYAN BURRELL

PRIVACY OFFICER/ LEAD CONSULTANT, HIM

15 AUG 2024

Privacy at IHS

Carl Mitchell – Senior Agency Official for Privacy (SAOP)

Heather McClane – Senior Official for Privacy (SOP)

IHS Area Privacy Coordinators – (in the GAL)

Facility Privacy Liaisons

What does the Privacy Role entail?

Privacy Review for Acquisitions – Privacy Act Applicability Memo

Privacy Incident Response – Conducting Investigations

Subpoena Review and Analysis

HIPAA Walk Through

Requests for Restriction

Requests for Correction/Amendment

Request for Communication by Alternate Means

Sensitive Patient Tracking

Proactive Sensitivities

Privacy Training Assistance

Privacy Act Applicability Memo

In accordance with HHS-OCIO-OIS-2021-03-001, HHS Policy for Information Technology Procurements - Security And Privacy Language. Privacy reviews are required for the following acquisition types:

Procurements requiring information security and/or physical access;

Procurements involving personally identifiable information (PII) or records of individuals;

Procurements involving government-owned/contractor-operated (GOCO), contractor-owned/ contractor-operated (COCO);

Procurements involving cloud services;

Other procurement types

- Hardware,
- Non-commercial and open source software,
- Information technology application design, development or support.

PA Memo continued

In accordance with the afore mentioned policy, privacy reviews procurements ***before*** acquisition to identify:

Applicable System of Records (HHS-OCIO-OIS-2021-03-001)

Applicable FAR Clauses (HHS-OCIO-OIS-2021-03-001)

Applicable HHSAR Clauses (HHS-OCIO-OIS-2021-03-001)

Federal Compatible Terms of Service (M-13-10)

Privacy Impact Assessment (PTA, PIA, TPWA) (M-03-22 & M-10-23)

Business Associate Agreement requirements (HIPAA)

Identify Required Privacy Training (HHS-OCIO-OIS-2021-03-001)

IHS SORN's

IHS has no exempt systems.

09-17-0001 Medical, Health, and Billing Records Systems
SORN history: 75 FR 1625 (1/12/10), *83 FR 6591 (2/14/18)

09-17-0002 Indian Health Service Scholarship and Loan Repayment Programs
SORN history: 74 FR 50222 (9/30/09), *83 FR 6591 (2/14/18)

09-17-0003 Indian Health Service Medical Staff Credentials and Privileges Records
SORN history: 88 FR 33151 (5/23/23)

09-17-0004 Indian Health Service Sanitation Facilities Construction Individual Applicant Records
SORN history: 74 FR 43143 (8/26/09), *83 FR 6591 (2/14/18)

09-17-0005 Personal Health Records (PHR) Administrative Records - IHS
SORN history: 77 FR 65564 (10/29/12), *83 FR 6591 (2/14/18)

09-17-0006 Community Health Aide Program (CHAP) Records
SORN history: 88 FR 74495 (10/31/23)

*83 FR 6591 (2/14/18) added two security-related routine uses required by OMB in January 2017

Government Wide SORN's

A government-wide system of records is a system of records where one agency has regulatory authority over records in the custody of multiple agencies, and the agency with regulatory authority publishes a SORN that applies to all of the records regardless of their custodial location. The application of a government-wide SORN ensures that privacy practices with respect to the records are carried out uniformly across the Federal Government in accordance with the rules of the responsible agency. For a government-wide system of records, all agencies – not just the agency with government-wide responsibilities – are responsible for complying with the terms of the SORN and the applicable requirements in the Privacy Act, including the access and amendment provisions that apply to records under an agency's control.

This list of SORNs is provided for informational purposes only and may not include every government-wide SORN. Visitors to this website should not rely upon any information provided on this website for the purpose of making decisions related to agency practices and policies.

To search across all Government SORNs access the FPC SORN Dashboard. The FPC SORN dashboard regularly pulls newly published SORNs from the Federal Register, and includes documents from 1994 to the present day.

FAR and HHSAR Clauses

The 3 Privacy Act-specific clauses are:

FAR:

48 CFR 52.224-1 Privacy Act Notification

48 CFR 52.224-2 Privacy Act

HHSAR:

48 CFR 352.224-70 Privacy Act - This HHSAR clause requires tailored language to be included in the SOW, specifying 1) the applicable system(s) of records or proposed system(s) of records, 2) the design, development and/or operation work the Contractor is to perform, and 3) the records disposition instructions to be followed by the Contractor upon completion of contract performance.

Terms of Service

The two most common terms found in typical terms of service agreements that the federal government cannot agree to are indemnification and jurisdiction for governing law.

An indemnification clause states that an agency would agree to pay legal costs if involved in a future legal dispute. This violates the restrictions of Anti-Deficiency Act and Adequacy of Appropriations Act, because agencies cannot agree to obligate federal funds for a fiscal year that have not been appropriated by Congress.

A clause referencing governing law or jurisdiction typically identifies a specific governing state or court system in which disputes will be settled. However, the federal government is controlled by federal, not state, law, and legal disputes involving the federal government must be heard in federal, not state, courts.

* COR's generally enter into negotiations with OGC on Terms if the vendor is willing to negotiate

Federal Compatible Terms of Service

Indemnification, Liability, Statute of Limitations: Any provisions in the TOS related to indemnification and filing deadlines are hereby waived, and shall not apply except to the extent expressly authorized by law. Liability for any breach of the TOS as modified by this Amendment, or any claim arising from the TOS as modified by this Amendment, shall be determined under the Federal Tort Claims Act, or other governing federal authority. Federal Statute of Limitations provisions shall apply to any breach or claim.

Governing law: Any arbitration, mediation or similar dispute resolution provision in the TOS is hereby deleted. The TOS and this Amendment shall be governed by and interpreted and enforced in accordance with the laws of the United States of America without reference to conflict of laws. To the extent permitted by federal law, the laws of the State of [Company to insert name of state if one is mentioned in its TOS] (excluding [Company's state] choice of law rules) will apply in the absence of applicable federal law.

E-Government Act

Privacy Impact Assessments ("PIAs") are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form.

A PIA is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a system.

The Act requires an agency to make PIAs publicly available, except when an agency in its discretion determines publication of the PIA would raise security concerns, reveal classified (i.e., national security) information, or sensitive (e.g., potentially damaging to a nation interest, law enforcement effort or competitive business interest contained in the assessment) information.

Section 208

(a) PURPOSE.—The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

(b) PRIVACY IMPACT ASSESSMENTS.—

(1) RESPONSIBILITIES OF AGENCIES.—

(A) IN GENERAL.—An agency shall take actions described under subparagraph (B) ***before***—

(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

(ii) initiating a new collection of information that—

(I) will be collected, maintained, or disseminated using information technology; and

(II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements

Section 208 continued

(B) AGENCY ACTIVITIES.—To the extent required under subparagraph (A), each agency shall—

(i) conduct a privacy impact assessment;

(ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and

(iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

What kind of PIA do I need?

Privacy Threshold Analysis (PTA)

Privacy Impact Assessment (PIA)

Third Party Website Application (TPWA)

Privacy Threshold Analysis (PTA)

PTAs analyze how information is handled in information technology (IT) systems and electronic information collections.

A PTA is a Privacy Impact Assessment on a system that does not contain PII or only contains HHS employee information.

If the analysis determines that the IT system does not collect, disseminate, maintain or dispose of PII the PTA is signed and submitted to HHS for approval.

If the analysis determines that the IT system or electronic information collection collects, disseminates, maintains, or disposes of PII, a PIA is required.

Privacy Impact Assessment (PIA)

PIAs are used to assess the privacy risks of IT systems and electronic information collections that collect, disseminate, maintain, and/or dispose of PII about members of the public.

PIAs are also used to ensure that the handling of the information conforms to applicable legal, regulatory, and policy requirements regarding privacy, and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

PIAs further provide transparency into how HHS collects, disseminates, maintains, or disposes of the public's PII.

Given that IHS handles a large amount of PII, it is critical that responsible organizations follow the requirements set forth in this policy to protect PII and retain the public's trust.

Third Party Website Application (TPWA)

A TPWA PIA is required “for any Federal agency use of third-party Websites or applications” to engage with the public for the purpose of implementing the principles of the Open Government Directive

Web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a “.com” Website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency’s official Website.

How to find or obtain PTA, PIA or TPWA

First check one of three folders on the I Drive:

Current PIA

Current PTA

Current TPWA

If you don't find an approved PIA, PTA or TPWA there check one of the next two folders:

Initiated NOT Approved PIA

Initiated NOT Approved TPWA

Initiated NOT Approved

If you find the PIA or TPWA you need in one of the Initiated NOT Approved folders:

Fill out the form

Send completed form to Heather.McClane@ihs.gov

* If you do not find the form you need in any of the folders, contact Heather McClane to initiate PIA for you. When you contact Heather be sure to include your Privacy Assessment Memo and Statement of Work (which includes the federal compatible terms of service if the form you need is for third party website or application)

Privacy Incident Response

In this role, you advise staff where to file privacy incidents:
https://pirt.ihs.gov/privacy/

Investigate reported incidents

Provide closure information to your Area Privacy Coordinator

Subpoena Review and Analysis

Review all subpoenas

Is the United States a Party?

If not, send to your Area Privacy Coordinator who will send to OGC to determine if this should be sent as a FOIA to the FOIA office. The Area Privacy Coordinator will send to FOIA office.

If the US is a Party, answer these questions and send the subpoena and the responses to these questions to your Area Privacy Coordinator.

Do you have the records being requested?

How long will it take you to gather them?

Are there staff being asked to testify?

Are they available the day requested?

Your Area Privacy Coordinator will send to the OGC and will provide further guidance.

HIPAA Walk Through

A walk-through compares your privacy requirements with actual employee practices. Some common items to look for:

Is the NPP posted? Is it available at the front desk if requested?

Can patients and visitors see computer monitors? Are unattended computers screens locked or left open? Are PIV cards left unattended? Are desks clear of patient information when unattended?

Are doors that are meant to be kept closed and locked actually closed and locked?

Check printers and faxes, are there documents left on them?

Put on gloves, check the trash, is there PHI/PII in it? Are there shred boxes under desks? Is there a locked shredding bin?

Requests for Restriction

The request for restriction must be in writing using IHS 912-1 form.

NOTE: The patient is not required to provide a reason for the request.

The IHS is not required to agree to the request, however, is required to examine feasibility for each request without just outright denying it.

Before agreeing to the restriction, the IHS must contact the OGC.

A restriction agreed to by the IHS shall not prevent the use or disclosure for which authorization is not required as outlined in the IHS Notice of Privacy Practices.

* Restrictions are entered in SPT, in the EAR option.

Requests for Correction/Amendment

The patient must complete the IHS-917 form, "Request for Correction/Amendment of Protected Health Information."

Document the date you received the IHS-917 form and provide an acknowledgment of receipt of the IHS-917 form within 10 working days. (See 2-7.9B for a model letter on acknowledgment of receipt.)

If a decision on the request for correction or amendment can be made within 10 working days of the IHS' receipt of the request, the IHS will notify the patient of the receipt of the patient's correction or amendment request and its decision within that 10 day period.

In consultation with the appropriate staff member review the request for correction or amendment and inform the patient in writing within 60 days after receipt of the request, of approval or denial of the request for correction or amendment. The IHS-917 form will be filed at the site of the contested entry in the individual's medical record and maintained for the life of the record.

Request for Communication by Alternate Means

All requests for confidential communications to be sent by alternate means or to an alternate location shall be in writing on the IHS-963 form "Request for Confidential Communication by Alternate Means or Alternate Location" and must describe the alternate means or the alternate location.

The CEO or (his or her) designee will approve or disapprove all requests. The CEO or (his or her) designee will approve the request if it is reasonable.

The request must be filed in the patients record.

Sensitive Patient Tracking

SPT should be run every month on all staff (including Area/HQ staff, contractors and volunteers) who have access to EHR/RPMS.

Larger facilities can run SPT on a schedule per department (be sure not to publish your schedule or set your schedule, e.g. Dental every January and June).

Some departments require a higher level of scrutiny and should be on the rotation every month e.g. those with larger numbers of reported incidents.

Proactive Sensitivities

Has there been a high profile accident in your community?

Is there a celebrity coming to your community?

Are there any patients who have been in the news?

Go into SPT and manually mark those patients as sensitive. This gives a warning to the end user that we are watching who accesses the record.
e.g. This record is marked as sensitive, to continue click ok.

Privacy Training Assistance

All I/T/U employees, volunteers and contractors can take the IHS privacy training at www.ihs.gov/privacytraining.

Sometimes staff need one-on-one assistance to pass the tests in each module. In this case, you would provide the one-on-one assistance.

Individuals who fail a test five times are advised that they have failed five times, they can ask for one-on-one assistance or simply take the test again.

*Often these individuals think this means they have been locked out or need to be rest. They just need to click the module again and the test is open to take

Questions?


INDIAN HEALTH SERVICE
PHS · 1955 ·