National Institutes of Health

Office of the Senior Official for Privacy

Privacy

Frequently Asked Questions (FAQs)

Table of Contents

Privacy Act

1. Why have a Privacy Act?

- We have a constitutional right to privacy. Amendment IV of the U.S. Constitution says, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…";
- Information is affected by the collection, maintenance, use and dissemination by Federal agencies; and
- The use of the internet, computers, and other technology create the possibility for faster and greater distribution, which could lead to greater harm.

2. What does the Privacy Act do?

- Limits the collection of personal information;
- Prevents secret Government record systems;
- Prevents secret use of Government records;
- States individual's right to see and correct records;
- Requires safeguards to be implemented to protect the security and accuracy of the information; and
- Allows for civil remedies and criminal penalties to be assessed for violations under the Privacy Act.

3. Who does the Privacy Act cover and not cover?

- The Privacy Act covers:
  - U.S. citizens
  - Resident aliens
- The Privacy Act does not cover:
  - Non-resident aliens
  - The deceased
  - Organizations

4. When is NIH allowed to collect my information?

- NIH may not legally maintain records on individuals unless:
  - The information is relevant and necessary to accomplish an NIH or Department function required by statute or Executive Order;
  - The information in the record is acquired to the greatest extent practicable directly from the subject individual; and
  - The individual providing the record is informed when the record is collected under the authority NIH has for requesting the record.

5. When are supervisor notes considered agency records?

- Supervisor notes are agency records when they are:
  - Used as the basis for an employment action; and
  - Otherwise made a part of an employee's personnel file and treated as official agency documentation.
- Supervisor notes are NOT agency records when they are:
  - The personal property of the supervisor only;
  - Never circulated or shared with others;
  - Never passed to replacement supervisors or those acting in the absence of the supervisor;
  - Used as memory joggers only; and
  - Not used as official agency documentation.

6. What is a Privacy Act Records System?

- A group of records (more than one), not available in the public domain;
- A record that contains information about an individual that is personal in nature (i.e., name, age, sex, gender, ethnicity, home address, phone, SSN, medical credentials, medical, financial and/or educational background, etc.); and
- A record designed to be retrieved by the individual's name, or another personal identifier such as an ID number, protocol number, photo, fingerprint, etc.

7. What is a System of Records Notice (SORN)?

- A document posted in the Federal Register that notifies the public of what information is contained in a specific system and how that information is collected, used, maintained, and disseminated in relation to other systems; and
- A SORN also explains how individuals may gain access to information about themselves.

8. How do I submit a records request?

- An individual who wishes to request a specific record must submit a request **in writing** to the appropriate NIH Institute or Center (IC) that collected and maintains that record;
- The written request should be as specific as possible. Please describe what type of information was collected, who collected it, why it was collected, when it was collected, and, if known, who (individual or organization) collected it; and
- For more details regarding this process, please reference the "How Do I Submit a Privacy Act (PA) Request for Records?" segment of the Privacy Act section of this website.

9. How do I amend an incorrect record?

- An individual who notices that a record is incorrect must submit a request **in writing** to the appropriate NIH IC that collected and maintains that record;
- The written notice should include the current record and provide an accurate correction of the record; and

- For more details regarding this process, please reference the "How Do I Submit a Privacy Act (PA) Request for Records?" segment of the Privacy Act section of this website.

10. Can I appeal the denial to access or correct my information?

- Requesters who wish to appeal NIH's decision deny access to correct or amend his or her record must do so within 30 days of the receipt of a decision letter from NIH. Appeals should include the following information:
    - Reasons why the requested information should be corrected or amended under the Act; and
    - Why the denial may be in error.
- PA requesters wishing to submit an appeal should attach to their appeal, a copy of their original request and response letter, clearly mark the letter and the outside envelope "Privacy Act Appeal" and mail the documents to the following address:

  NIH Privacy Act Officer
  National Institutes of Health
  6011 Executive Boulevard
  Suite 601, MSC 7669
  Bethesda, Maryland 20892-7669

11. Are there circumstances in which certain information cannot be released?

- NIH will provide access to records within their possession unless one of the exceptions or exemptions applies:
    - The records contain information about a third party;
    - Information that is not about the subject of the file, and therefore not accessible under the Privacy Act;
    - Records were compiled in reasonable anticipation of a civil action or proceeding;
    - Records are maintained by the CIA; or
    - Records are maintained by an agency or component thereof, which performs as its principal function any activity pertaining to the enforcement of criminal laws.
- For more specific details regarding exemptions, please reference the "NIH Privacy Act Exceptions & Exemptions" segment of the Privacy Act section of this website.

12. Where can I find information regarding the Paperwork Reduction Act (PRA) / Office of Management and Budget (OMB) Clearance procedures?

- NIH PRA/OMB Website: http://www.hhs.gov/ocio/policy/collection/infocollectfaq.html
- The Paperwork Reduction Act (PRA) of 1995 requires agencies to obtain approval from OMB prior to soliciting and/or obtaining identical information from ten or more members of the public in multiple forms. PRA/OMB approval is required whether the Federal agency collects the information itself or uses an outside agent or contractor. OMB requires 90-120 days to approve new information collections and renew existing approvals.
- You can click on the Office of Extramural Research (OER) Intranet website at: http://odoerdb2.od.nih.gov/oer/policies/project_clearance/pcb.htm to obtain a list of NIH PRA/OMB Project Clearance Liaisons, and get more information about whether your IT system has been approved for PRA/OMB information collection.

13. Where can I find information about the HIPAA Privacy Rule?

- For additional information on a wide range of topics about the Privacy Rule, please visit the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) Privacy Rule Web Site at: www.hhs.gov/ocr/hipaa/. You can also call the OCR Privacy toll-free phone line at (866) 627-7748. Information about OCR's civil rights authorities and responsibilities can be found on the OCR home page at: www.hhs.gov/ocr.

14. Where can I find guidance regarding the HIPAA Privacy Rule and the Electronic Exchange of Health Information?

- The HHS OCR has published new HIPAA Privacy Rule guidance as part of the Department's Privacy and Security Toolkit to implement *The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* (Privacy and Security Framework). The Privacy and Security Framework and Toolkit is designed to establish privacy and security principles for health care stakeholders engaged in the electronic exchange of health information and includes tangible tools to facilitate implementation of these principles. The new HIPAA Privacy Rule guidance in the Toolkit discusses how the Privacy Rule supports and can facilitate electronic health information exchange in a networked environment. In addition, the guidance includes documents that address electronic access by an individual to his or her protected health information and how the Privacy Rule may apply to and supports the use of Personal Health Records. HIPAA guidance documents are available at: http://www.hhs.gov/ocr/hipaa/hit/. For more information on the Privacy and Security Framework and to view other documents in the Privacy and Security Toolkit, visit: http://www.hhs.gov/healthit/privacy/framework.html.

15. Can I subscribe to an electronic listserv in order to receive information sent directly to my email inbox?

- **Yes**. The HHS OCR operates an announce-only electronic list serv as a resource to distribute information about the HIPAA Privacy Rule. It is named OCR-Privacy-list. To subscribe to or unsubscribe from the list serv, please go to: http://list.nih.gov/cgi-bin/wa?SUBED1=ocr-privacy-list&A;=1.

16. Who can I contact if a person or organization covered by the Privacy Rule violates my health information privacy rights?

- NIH does not meet the definition of a "covered entity" and is therefore not covered by HIPAA because it does not bill third parties for the health care they receive at the Clinical Center. However, if you believe that a person or organization outside of NIH who is covered by the Privacy Rule (a "covered entity") violated your health information privacy rights or otherwise violated the Privacy Rule, you may file a complaint with OCR. For additional information about how to file a complaint, see the Fact Sheet "How to File a Health Information Privacy Complaint," available at: http://www.hhs.gov/ocr/privacyhowtofile.htm.

17. Where can I find information about the Family Educational Rights and Privacy Act (FERPA) regulation and other helpful information?

- FERPA is a Federal law that protects the privacy of students' "education records." (See 20 U.S.C. § 1232g; 34 CFR Part 99). The HIPAA Privacy Rule requires covered entities to protect individuals' health records and other identifiable health information and gives patients rights over their health information. The guidance is available at: http://www.hhs.gov/ocr/hipaa. Information about the Family Policy Compliance Office (FPCO) is available at: http://www.ed.gov/policy/gen/guid/fpco/index.html.

18. Where can I find U.S. Department of Health and Human Services (HHS) and U.S. Department of Education (ED) joint guidance on the application of FERPA and HIPPA to Student Health Records?

- The Departments of Education and Health and Human Services have jointly released guidance to explain the relationship between the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, and to address apparent confusion on the part of school administrators, health care professionals, and others as to how these two laws apply to student health records. The guidance also addresses certain disclosures that are allowed without consent or authorization under both laws, especially those disclosures related to health and safety emergency situations. The guidance was developed in response to the "Report to the President on Issues Raised by the Virginia Tech Tragedy" (June 13, 2007) as well as to address questions the respective Departments have heard generally from stakeholders regarding the intersection of the HIPAA Privacy Rule and FERPA. The Departments of Health and Human Services and Education are committed to a continuing dialogue with school officials and other professionals on these important matters affecting the safety and security of our nation's schools. While this guidance seeks to answer many questions that school officials and others have had about the intersection of these federal laws, ongoing discussions may cause more issues to emerge. Contact information for submitting additional questions or suggestions for purposes of informing future guidance is provided at the end of the guidance document available at: http://www.hhs.gov/vtreport.html.

Federal Information Security Management Act (FISMA)/ Privacy Impact Assessments (PIAs)

1. What is FISMA's purpose?

- Inform and raise awareness among Federal agency heads of the importance of information security programs;
- Facilitate the development of security programs through mandatory comprehensive reporting and evaluation; and
- Ensure that federal agencies take the necessary precautions to secure agency IT systems and protect personally identifiable information (PII) and mitigate the risk of a breach to PII.

2. What are the major components of the FISMA Section D report?

- Inventory of Systems that Contain Federal Information in Identifiable Form which require a Privacy Impact Assessment (PIA) or System of Records Notice (SORN);
- Links to PIAs and SORNs;
- Senior Agency Official for Privacy (SAOP) Responsibilities;
- Information Privacy Training and Awareness;
- PIA and Web Privacy Policies and Processes;
- Policy Compliance;
- Agency Use of Persistent Tracking Technology; and
- Privacy Points of Contact.

3. What is the FISMA report process/timeline?

- While FISMA compliance is an ongoing process, which requires quality reviews, the final annual report is due at the end of the Federal fiscal year (September 30);
- All FISMA report data is collected approximately two months in advance of the report deadline in order to compile the data and promote it, through the Department, to the IG; and
- Agencies must continually monitor IT systems and privacy procedures and responsibilities to ensure that OPDIVs are compliant with Federal IT and privacy laws.

-

4. What is a PIA?

- A means to assure compliance with applicable privacy laws and regulations;
- An evaluation tool used to determine the risks and effects of collecting, maintaining and disseminating personally identifiable information (PII) in an electronic Information Technology (IT) System used by multiple users (e.g., network, server, database) or through the use of a Third-Party Website or Application (TPWA);
- An analysis instrument to enable system developers and system owners/managers to identify and evaluate privacy risks; and
- A tool that evaluates:
    - Data in the IT System or TPWA;
    - Attributes of the Data;
    - Access to the Data;
    - Information Collection and Use Practices;
    - Privacy Notice Practices;
    - Information Sharing and Maintenance Practices;
    - If the IT System Contains Federal Records;
    - Whether the Use Creates or Modifies a Privacy Act System of Records;
    - Whether the Use Creates an Information Collection under the PRA;
    - Website Hosting and Uses of TPWAs to Collect or Maintain Data; and,
    - Maintenance of Administrative & Technical and Physical Controls
- Parts of a PIA include:
    - Date of Submission;
    - Agency/OPDIV/IC;
    - Title of System;
    - Existing, New or Modified?;
    - Unique Project Identifier;
    - System of Records Number;
    - OMB Info Collection Approval Number & Expiration Date;
    - Other Identifier;
    - System Overview;
    - Legislative Authority;
    - How will information be collected?;
    - How will IC use the information?;
    - Why is information collected?;
    - With whom will the information be shared?;
    - From whom will the information be collected?;
    - What will subjects be told about the collection?;
    - How will the message be conveyed?;
    - What are opportunities for consent?;
    - Will information be collected from children under 13 on the internet? If so, how will parental approval be obtained?;
    - How will information be secured?; and
    - How will information be retained and destroyed?

5. Why do we conduct PIAs?

- To help determine what type of information is collected by IT systems throughout NIH;
- To decide which precautions need to be implemented to protect such information;

- To provide privacy stakeholders an orderly process in which they can report IT system collected information to the SOP; and
- To have an orderly process for submitting IT system information related to privacy for FISMA reporting.

6. Which IT Systems or TPWAs Need a PIA?

- IT systems owned, operated, maintained, or controlled by the Federal government or a contracted company working on behalf of the agency;
- Web-based technologies that are not exclusively operated or controlled by a government entity, or that involve significant participation of a non-government entity;
- Those that have not been assessed previously;
- Those in development (as part of the certification and accreditation [C&A] process); and,
- Those assessed previously which have undergone a "major change".

7. What is a Major Change?

A "major change" is a modification to an IT System or TPWA that affects the following:

- Access control
- Type of data collected
- IT System or TPWA interconnection
- Information sharing
- Business processes

Examples of Major Changes

- Conversions: When converting paper-based records to electronic IT Systems or TPWAs.
- Anonymous to Non-Anonymous: When functions applied to an existing information collection change anonymous information into PII.
- Significant IT System or TPWA Management Changes: When new uses, including application of new technologies, significantly change how PII is managed in the IT System or TPWA.
- Significant Merging: When agencies adopt or alter business processes so that government databases holding PII are merged, centralized, matched with other databases, or otherwise significantly manipulated.
- New Public Access: When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic IT System or TPWA.

8. Who Should Prepare/Review/Approve PIAs?

- PIAs are completed by an IT System or TPWA Owner/Manager in consultation with the IC Privacy Coordinator, ISSO, Web Master, Paperwork Reduction Act (PRA) Liaison, Records Liaison and other key stakeholders, as applicable, via SPORT.
- They are distributed through the respective IC and NIH organizational channels for concurrence (i.e., Supervisory Chain/Executive Officers).
- The NIH Senior Official for Privacy (SOP) will review, approve, and date each PIA and promote it to the Department.
- On a quarterly basis, HHS will post a summary of the IT System or TPWA PIA on a public website at URL: http://www.hhs.gov/pia/nih/index.html
- The HHS OCIO will communicate to the NIH SOP the status of PIAs not approved for posting

9. When do I fill out the entire PIA vs. the PIA Summary?

- If the system for which the PIA is being completed collects PII, the entire PIA form must be completed. If it does NOT collect PII, you only need to complete the PIA Summary tab; and
- NOTE: If you are working to complete the PIA Summary, you must clearly explain why/how the system does not collect PII.

10. How do I determine if a system collects PII?

- PII is defined as any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual;
- If any of these, or any other categories of information that can be linked to an individual, are stored, maintained, passed through, or disseminated by the system, the system collects PII; and
- IC Privacy Coordinators should be able to validate whether or not a system collects PII based on the information provided to them by System Owners/Managers.

11. Must I complete a new PIA for an existing IT system each year?

- A new PIA is not required if information has been previously assessed under a similar evaluation, or if the system has not undergone any major changes as defined in OMB M03-22; and
- All existing PIAs must be reviewed for accuracy each year.

12. Are there any quick tips that would make PIA completion easier?

- Consult with other privacy stakeholders as appropriate (e.g. IC Privacy Coordinator, IC Chief Information Officer and ISSOs) when questions about PIAs, privacy, or other questions arise;
- Ensure that your answers are accurate and complete (specifically answer the questions, provide sufficient detail, spell out acronyms, check spelling etc.);
- Remember that PIAs are published to a public website;
- Avoid contradicting answers. For example, do not deny that the system collects Social Security Numbers (SSN) and then later claim that the system retrieves information using SSN;
- System Owners/Managers should work with IC Privacy Coordinators and ISSOs early in the SDLC to ensure that the PIA process is properly incorporated;
- Know the business objective of the system; and
- Know the difference between privacy and security

13. Does the FISMA Tool inform the OSOP when I update/promote a PIA?

- **No**. The FISMA Tool does not inform the OSOP when any changes are made to a PIA. System Owners/Managers and IC Privacy Coordinators should alert the OSOP when a PIA has been updated/promoted. This will improve the NIH's PIA process and increase its efficiency.

PIA Form

1. What is a Unique Project Identifier (UPI) Number and how can I find one?

- The UPI Number is used to report IT investments during the budget process and ensure the integration of strategic planning, budgeting, procurement, and the management of IT investments in support of the agency's mission and business needs. It reflects information such as the OPDIV and office where the investment project was initiated, the type of investment, and other information. The UPI is used by OMB to track the system through the PIA, C&A, and POA&M processes. The number is attached to Exhibit 53s and described in Exhibit 300s, which are submitted to OMB prior to major investment and budget requests. The number is long and appears as follows: 009-25-xx-xx-xx-xxxx-xx-xxx-xxx (Defined in OMB A-11, Sedction 53.8). If you are not sure if a UPI is associated with the system for which you are conducting a PIA, please contact the Project Officer. If he/she is not able to assist you, contact the OCIO IT Policy and Review Office (ITPRO), the OCIO Information Technology Acquisition Services Office (ITASO) or the OCIO Information Security and Awareness Office (ISAO);
- ***2008 UPI*** means the unique project identifier used to report the investment in the 2008 Budget. Indicating the UPI used for the 2008 Budget process allows crosswalk and historical analysis crossing fiscal years for tracking purposes;
- ***2009 UPI*** means the identifier depicting agency code, bureau code, mission area (where appropriate), part of the exhibit where investment will be reported, type of investment, agency four-digit identifier, and two-digit investment category code;
- NOTE: Not all systems require UPI numbers. If a UPI does not exist for a system, you must provide an explanation in the PIA form; and
- If you are unsure about the UPI, contact the Project Officer. If he/she is not able to assist you, contact the ODCIO IT Policy and Review Office (ITPRO), the ODCIO Information Technology Acquisition Services Office (ITASO), or the ODCIO Information Security and Awareness Office (ISAO).

2. What is a System of Records Notice (SORN) and where can I find one?

- A SORN describes the Privacy Act system of records, and the categories of PII collected, maintained, retrieved, and used within the system. It provides information to the public on various characteristics of the system (e.g. description, purpose, data collection, notification, retention and disposal, etc.) and how NIH intends to manage and protect the system. The SORN Number is that which is assigned to the Privacy Act SORN (also referred to as the Systems Notice)

  NOTE: If the system is subject to the Privacy Act, then a SORN must be cited as an answer in question 4; and

- All NIH SORNs are located at:
  http://oma.od.nih.gov/ms/privacy/pa-files/read02systems.htm

3. What is an OMB Information Collection Approval Number?

- The Paperwork Reduction Act (PRA) of 1995 requires agencies to obtain approval from OMB prior to soliciting and/or obtaining identical information from ten or more members of the public in

multiple forms. PRA/OMB approval is required whether the Federal agency collects the information itself or uses an outside agent or contractor. OMB requires 90-120 days to approve new information collections and renew existing approvals. The OMB Information Collection Approval Number should be identical to the one OMB assigned pursuant to having been filed under the Paperwork Reduction Act and is sometimes referred to as an OMB control number. It would only apply if the system maintains data as part of an approved OMB information collection from 10 or more members of the general public; and

- You can click on the Office of Extramural Research (OER) Intranet website at: http://odoerdb2.od.nih.gov/oer/policies/project_clearance/pcb.htm to obtain a list of NIH PRA/OMB Project Clearance Liaisons, and get more information about whether your IT system has been approved for PRA/OMB information collection.

4. Are there policies or guidelines in place with regard to the retention and destruction of PII?

- For Privacy Act systems of records, records retention and disposal procedures should be indicated within the SORN cited for the system. If the system is not subject to the Privacy Act and does not have a SORN in place, consult with the IC Records Liaison to ascertain the appropriate records retention and disposal schedule for the system. A list of IC Records Liaisons can be accessed from OMA's webpage at: http://oma.od.nih.gov/about/contact/browse.asp?fa_id=2

Web Privacy

1. Where can I find HHS Machine-Readable Privacy Policy?

- Please reference the link below:
  http://www.hhs.gov/web/508/index.html

2. Where can I find NIH Privacy Act Notification Criteria and Sample Statements?

- Please reference the link below:
  http://oma.od.nih.gov/ms/privacy/NSCriteria.doc

3. Who do I contact if a user inquires about the web site's privacy standards?

- Please contact your IC Privacy Coordinator if you have any questions regarding a web site's privacy standards, procedures, or requirements.
  http://oma.od.nih.gov/about/contact/browse.asp

4. Can I post a new web site or update an existing web site before it complies with NIH web privacy requirements?

- No. ICs must comply with NIH web privacy policies before posting a new web site or revising an existing one. See NIH Web Page Privacy Policy – NIH Manual Chapter 2805:
  http://www3.od.nih.gov/oma/manualchapters/management/2805

5. Does Section 508 compliance apply to emails?

- Section 508 or machine-readability compliance applies to website design and page information, documents available on the website (such as forms, newsletters and brochures), and on-line systems used both for internal and external purposes. Emails sent in text format can generally be read by everyone. If they include web links, the fully qualifying URL should be shown as well, including the 'http://www' part.

  However, Section 508 does apply to email messages, ***particularly*** those which are sent to larger groups, often referred to as 'broadcast mailings.' The current HHS standard with links to more information is available at the following website:
  http://www.hhs.gov/web/policies/webstandards/accessemail.html.

  The Department standard generally states, "HHS must make email accessible to persons with disabilities. All emails—internal or external—as well as their attachments, including graphics, audio, and video must be accessible." In terms of e-mails that are sent to smaller and known audiences, HHS states that these e-mails "**should** meet Section 508 standards as much as practicable. Alternative or accessible formats ["accommodations"] must be made available upon request."

Questions or concerns about Section 508 Compliance can be directed to the NIH Section 508 Help inbox at the email address: Section508Help@nih.gov.

Breach Response

1. What is a security or privacy breach?

- The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

2. What are some examples of paper and electronic breaches?

- Paper Breach:
  - Having hardcopy documents containing PII stolen from one's desk;
  - Losing a briefcase that contained hardcopy documents containing PII; and
  - Intentionally sharing hardcopy documents that contain PII without authorization.
- Electronic Breach:
  - Unauthorized users gain access to electronic documents containing PII via sharing of passwords, leaving work station unlocked/unattended, etc;
  - PII is posted, in any format, onto the world wide web without authorization; and
  - Having a laptop containing PII lost or stolen.

3. When do I report a breach?

- You should report both suspected and confirmed record breaches as soon as they are discovered in order to begin remediation and investigation of any compromised information.

4. To whom do I report a breach?

- All employees should immediately inform their supervisor immediately; and
- Supervisors should then notify the IC ISSO and IC Privacy Coordinator, as appropriate.
  - NIH IC ISSOs: http://ocio.nih.gov/security/security-isso.htm
  - NIH IC Privacy Coordinators: http://oma.od.nih.gov/about/contact/browse.asp

Training Resources

1. Is SPORT Tool training available? If so, how do I go about requesting it?

- Training is available periodically. Please contact the OSOP at privacy@mail.nih.gov, 301-451-3426; and
- HHS SPORT Tool Information is available at: https://ocio.nih.gov/nihonly/security/ProSight-FISMA-info.htm

2. Is it mandatory that I take NIH Privacy Awareness training?

- Yes. As mandated by FISMA and OMB Memorandum 07-19, all NIH employees and contractors are required to take privacy awareness training. It is imperative that NIH employees possess a general understanding of the importance of privacy protection. Privacy awareness training will also inform NIH staff of relevant privacy policy, guidelines, and procedures. Training must be completed annually.

NIH Third-Party Websites and Applications (TPWAs)

1. How do I identify a Third Party Website/Application

To first determine if a Website or web application is a Third Party Website/Application (TPWA), you may access the Health and Human Services (HHS) Center for New Media Website at http://newmedia.hhs.gov/standards/tos.html. Click on "New Media Tools" and then click on "Terms of Service [TOS] Agreements."

If the Website or application appears on the "Tools with Signed TOS Agreement" list it is a TPWA. Further, if it has a "yes" in the "TPWA PIA required" column, a Privacy Impact Assessment (PIA) is necessary. The list provides the TPWAs for which HHS has signed a federal-compatible terms of service "TOS" agreement, or for which the standard TOS has been cleared for use. This list is a living document that is regularly updated to reflect the use of new TPWA tools. If a tool is not listed on this list, you may contact the Department directly to inquire about the necessity of a PIA. As a general rule, if you are considering using a Web-based technology that is not exclusively operated or controlled by NIH or hosted on a .gov domain, it is a TPWA and will require a PIA.

The NIH Office of Communications and Public Liaison lists a number of TPWAs identified by Institute/Center (IC) at the following URL: http://www.nih.gov/Subscriptions.htm.

Note: The list maintained by the NIH Office of Communications and Public Liaison (link provided above) is only as current as the information provided to them by IC TPWA System Owners/Managers (e.g., staff responsible for opening an account or who handle responses, moderate comments or otherwise have knowledge of the design, development, operation or maintenance of a third-party Website or application).

To further determine if a Website/Application qualifies as a TPWA, apply this six question litmus test:

1) Is the Website or application part of an authorized law enforcement, national security, or intelligence activity? **Yes** - Other privacy laws will apply to the information collection. Therefore, you do not need to complete a TPWA PIA. **No** - Continue to Question 2.

2) Is the Website or application intended to be used for internal HHS/OPDIV activities only? **Yes** - You do not need to complete a TPWA PIA. **No** - Continue to Question 3.

3) Does HHS/OPDIV own or have contractual control of the operation or maintenance of the Website or application? **Yes** - You do not need to complete a TPWA PIA. However, you must ensure an IT System PIA was conducted previously on the Website or application (e.g., network, server, or database). **No** - Continue to Question 4.

4) Does another Federal department or agency own or have contractual control of the operation or maintenance of the Website or application? **Yes** - You do not need to complete a TPWA PIA. **No** - Continue to Question 5.

5) Is the Website or application intended to involve members of the public? **Yes** - You need to complete a TPWA PIA. Please collaborate with key stakeholders within your OPDIV, as needed. **No** - Continue to Question 6.

6) Was the Website or application designed for the purpose of implementing the Open Government Directive principles of transparency, participation, and/or collaboration?

Transparency

Providing the public with information about what HHS/OPDIV is doing by making it available online in an open medium or format that can be retrieved, downloaded, indexed, and searched by commonly used web search applications. An open format is one that is platform independent, machine readable, and made available to the public without restrictions that would impede the re-use of that information (e.g., OPDIV Internet Website, Open Government Webpage, Blogs and Social Media Websites that request feedback on and assessment of the quality of published information).

Participation

Contribution by the public of ideas and expertise so HHS/OPDIV can make policies with the benefit of information that is widely dispersed in society (e.g., links to Websites where the public can engage in existing participatory processes, mechanisms, innovative tools and practices that create new and easier methods for public engagement in and feedback on the Agency, Department or OPDIV's core mission activities).

Collaboration

The encouragement of partnerships and cooperation with other Federal and non-Federal governmental agencies, the public, and non-profit and private entities in fulfilling the Agency, Department or OPDIV's core mission activities, to include proposed changes to internal management and administrative policies (e.g., technology platforms that improve collaboration among people within and outside HHS/OPDIV, descriptions of and links to appropriate Websites where the public can learn about existing HHS/NIH collaboration efforts, prizes and competitions to obtain ideas from and increase collaboration with those in the private sector, non-profit, and academic communities).

Yes - You need to complete a TPWA PIA. Please collaborate with key stakeholders within your OPDIV, as needed. **No** - It is not a TPWA. **Stop here**.

2. Can NIH prepare one "umbrella" PIA to cover multiple websites or applications that are functionally comparable?

No. To ensure PIAs clearly articulate the practice of a Website or application, and the accountability of the program, HHS requires a PIA be conducted for each use of a Website or application technology. This decision is based on the Department's assessment that the same technologies have very different practices. For example, Websites such as Facebook and YouTube can be substantially similar across each Website or application. However, their practices may be sufficiently different, even within a specific domain (e.g., Facebook page vs. Facebook quiz). Additionally, HHS program practices vary, such as how comments on Facebook pages are handled (i.e., cut and pasted into an Excel spreadsheet, saved to a Word document in order to compose an e-mail, deleted if personally identifiable, brought to the attention of management if inflammatory or offensive, etc.).

3. Does HHS maintain a list of websites and applications defined as TPWAs?

No. Due to the fact that the area of Web 2.0 technology is changing rapidly and new technologies are appearing almost daily, the HHS Center for New Media and the HHS Cybersecurity Program do not maintain a comprehensive list of TPWAs. However, the HHS Center for New Media is the best source for technologies that are being used widely since they are often consulted prior to use, and have a list of TPWAs for which HHS has signed a federal TOS agreement.

4. Is there a library of TPWA PIA templates?

HHS does not have a library of templates at this time. However, NIH has posted templates for Facebook, Twitter, Flickr, SurveyMonkey, GovDelivery, and YouTube on the OMA Privacy SharePoint Website. Additional templates will be added in the future.

5. Why are we required to assess TPWAs when we have no contractual control over the operation of the Website or application, nor do we have control over how the third-party uses the information it stores?

Websites under HHS and federal contractual control have contracts between the Federal Government and the contractors (i.e., Challenge.gov) that stipulate certain required information security and privacy activities be conducted. The Federal Government has control over the content on the site and the management of the information collected through the Website. However, the data is not managed by the government once the contract is executed. In general, each government contract includes stipulations for the privacy and security of data utilized and/or collected for a government purpose. Therefore, the privacy policy of the relevant federal agency is posted on these sites.

The government does not control the operations of a third-party Website or application and how that third-party uses information. For example, by virtue of having an account, the government is not in the position to manage how Facebook discloses user data or shares metrics of followers of NIH accounts on Facebook. Therefore, OMB determined federal agencies are responsible for considering the privacy implications of engaging with the public on TPWAs.

6. Do I Need To Conduct A TPWA PIA for the following?

Blogs?

If you create a blog (e.g., Feedback at NIH) through a third-party blogging platform such as Blogger, WordPress, Tumblr etc., you must complete a TPWA PIA. However, be cognizant of the fact that, by using a blogging platform administered by a third-party (even if the blog is embedded on a NIH.gov Website), any information provided by a member of the public on the blog can cause the information—which may contain PII—to be accessible to NIH. However, if the blog is hosted on a NIH.gov Website and does not utilize a third-party blogging platform, a TPWA PIA is not required.

E-mail Subscription Management Services?

If you created a means (e.g., GovDelivery) to allow visitors to provide a personal e-mail address and indicate their subscription preference in order to receive e-newsletters, alerts and other messages, including the items they want to receive, you must complete a TPWA PIA.

Internal Agency Activities *(i.e., SharePoint and Intranet Websites used by employees only)?*

No. Interactions that do not involve the public, or any activity that is part of authorized law enforcement, national security, or intelligence activities, do not need to be assessed with a PIA.

Micro blogs?

If you are using Twitter, Yammer, Posterous, etc. to engage the public, individuals can make personally identifiable information (PII) available or cause it to be accessible to NIH. Therefore, you must complete a TPWA PIA.

Mobile Applications?

Mobile applications installed on a user's device (e.g., iPhone, iPad, iPod) and used to communicate NIH content through an NIH-owned or operated portable, handheld device are not TPWAs. However, you will need to assess the NIH account in the location where the mobile application is downloaded (e.g., iTunes Apps Store, Android Market or other channel where the application resides). Considering NIH is directing the visitor to go to a Website where the privacy settings are not within its control or subject to the same requirements as a Government Website, NIH should review the practices of the Website and exercise due diligence to inform users, to the extent possible and practical, of those practices.

Online Survey Tools *(i.e., SurveyMonkey, SurveyGizmo, Project Implicit, etc.)?*

Yes. If they engage the public, they are third-party Websites/applications. If they are used to survey NIH employees, you would not conduct a TPWA PIA. The frequency or lifespan of TPWA use is not a factor. Therefore, a PIA would need to be conducted for each use of the survey tool that makes PII available, or could potentially make PII available to NIH.

Podcasts?

If the Podcast is hosted on an intranet site owned by NIH, it does not require the completion of a TPWA PIA. However, if the Podcast is hosted on a third-party Website, or if another music/sound sharing tool owned by a third-party is used to play the podcast, then a TPWA PIA will need to be completed.

RSS Feeds?

If the RSS feed (e.g., Feedburner) is produced by NIH or is hosted on or "lives on" a NIH.gov Website, then a TPWA PIA does not need to be completed. The key is to determine whether the RSS feed uses NIH technology or NIH has contractual control over it. If the RSS feed takes a user to a third-party web feed management provider that provides media distribution and audience engagement services, a TPWA PIA must be completed.

Systems developed by GSA for use by Federal agencies to advertise contests *(i.e., Challenge.gov which goes through Challengepost.com)?*

If the Web address and language indicate the Website is an official U.S. Government Website and NIH does not have control over how information is managed (i.e., no contractual control), you do not need to conduct a TPWA PIA.

Systems developed for use by Federal agencies?

If the Web address and language indicate the Website is not an official U.S. Government Website and NIH has control over how information is managed (i.e., contractual control), you must conduct a TPWA PIA.

Vodcasts?

If the vodcast is hosted on an intranet site owned by NIH, it does not require the completion of a TPWA PIA. However, if the vodcast is hosted on a third-party Website such as YouTube, or if another video sharing tool owned by a third-party is used to play the vodcast, then a TPWA PIA is required.

Widgets?

It depends. The functionality of the widget is to allow users to share .gov content on their Facebook, iGoogle or Windows and OS X desktops. If the widget (e.g., AddThis) is used to engage with the public for the purposes of implementing the principles of the Open Government Directive you will need to complete a TPWA PIA.

Wikis?

Wikis are not used by the government to engage with the public for the purpose of implementing the Open Government principles of transparency, participation, or collaboration. In some cases, the government may make contributions to the content, but since the messaging is not controlled by the government, it is not used by the Department to implement the principles of the Open Government Directive. Therefore, Wikis (e.g., Mixed Ink) do not qualify as a TPWA.

7. Are personal e-mail addresses considered to be personally identifiable?

If you create a means for an individual to provide a personal e-mail address (i.e., GovDelivery e-mail subscription service) you should consider that to be personally identifiable (e.g., firstnamelastname@verizon.net). Therefore, Websites and applications that cause an individual to provide an e-mail address, in order to subscribe to a service, should be assessed with a TPWA PIA.

8. Is a personal e-mail address by itself (without a name) considered to be PII?

OMB (M) 07-16 states that PII refers to "**information which can be used to distinguish or trace an individual's identity**, such as their name, social security number, biometric records, etc. **alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual**, such as date and place of birth, mother's maiden name, etc." Therefore, if you can use the information to contact someone, you must consider it to be PII.

9. If we assessed our internet website previously with the IT System PIA and have now modified the system to provide a link to enable the public to download a mobile application from the Apple store, must we now prepare a TPWA PIA on the use of iTunes?

If the public can access the mobile application directly from the iTunes Apps Store (Android Market or other) channel without having to visit the NIH or IC Website, a TPWA PIA must be completed.

10. If we partner with institutions to stand up websites on our behalf for the purpose of registering the public to attend training courses, is the use of the institution website considered to be a third-party?

Yes. If the institution uses a registration service owned by a third-party, or if the Website is not owned or controlled by NIH, it is a third-party Website or application. A TPWA PIA must be completed.

11. If our IC or office has multiple Twitter accounts, do we need to report each use?

Yes. If a NIH office/IC has 12 different *Twitter* (*Facebook*, etc.) accounts, a TPWA PIA must be completed for each account because each represents a unique use of the third-party Website.

NIH Web Measurement and Customization Technologies

1. What is a web measurement and customization technology?

Technologies used to remember a user's online interaction with a Website or online application in order to conduct measurement and analysis of usage or to customize the user's experience

2. What are some examples?

Web bugs, web beacons, and the most common mechanism to track use behavior or customize a Website, session, and persistent cookies.

3. What is the difference between Tier 1, 2, and 3 technologies?

TIER 1

Any use of a ***single-session*** Web measurement and customization technology.

TIER 2

Any use of ***multi-session*** Web measurement and customization technology **w*hen no PII is collected*** (including when the agency is unable to identify an individual as a result of its use of such technologies).

TIER 3

Any use of a ***multi-session*** Web measurement and customization technology ***when PII is collected*** (including when an agency is able to identify an individual as a result of its use).

4. What is meant by a single session technology?

They are technologies that remember a user's online interactions within a single session or visit. Any identifier correlated to a particular user is used only within that session, is not reused, and is deleted immediately after the session ends. An example is a normal web server log that maintains session-only information (whether personally identifiable or not). This includes the collection of an IP address, which the Department views as PII.

5. What is meant by a multi-session technology?

They are technologies that remember a user's online interactions through multiple sessions. This approach requires the use of a persistent identifier for each user, which lasts across multiple sessions or visits.

6. Do I have to conduct a TPWA PIA on Tier 1 usage technologies?

No TPWA PIA is required.

7. Do I have to conduct a TPWA PIA on Tier 2 usage technologies?

No TPWA PIA is required.

8. Do I have to conduct a TPWA PIA on Tier 3 usage technologies?

Yes, you must complete a TPWA PIA on the use of Tier 3 technologies.

9. Do I need to complete a TPWA PIA on all websites?

No. First, consider whether the Website is public-facing. OMB M-10-22 applies to web technologies that are used on government-owned or operated Websites, which face the public and collect information from the public. If the web measurement and customization technologies are on a public government Website and collecting information from the public, then M-10-22 will apply. If the uses are not on government-owned or operated Websites that face the public, M-10-22 does not apply.

If so, determine if web measurement/customization technologies are used on the Website. If so, determine if the technologies are collecting personally identifiable information (PII) belonging to an individual.

10. Do I have to conduct a TPWA PIA on persistent cookies used to block repeated delivery of surveys (e.g., ACSI customer satisfaction surveys)?

No, not unless they are used on a government-owned or operated Website that faces the public and are used to collect PII.

11. Do I have to conduct a TPWA PIA on persistent cookies used to measure repeat visitors (e.g., WebTrends, Omniture, SiteCatalyst, CrazyEgg, etc.)?

No, not unless they are used on a government-owned or operated Website that faces the public and are used to collect PII.

12. Do I have to conduct a TPWA PIA on tools designed to examine Web traffic and market effectiveness (e.g., Google Analytics, Woopra, etc.)?

These tools are not used to engage the public or convey NIH content to the public. Therefore, you most likely will not have to conduct a PIA. However, depending upon the use of settings, they may qualify as a web measurement or customization technology.