SMG 3297.5

FDA STAFF MANUAL GUIDES, VOLUME III - GENERAL ADMINISTRATION

INFORMATION RESOURCES MANAGEMENT

FREEDOM OF INFORMATION ACT AND PRIVACY PROGRAM

IMPLEMENTATION OF THE PRIVACY ACT AND THE FDA PRIVACY PROGRAM

PRIVACY IMPACT ASSESSMENTS (PIAs)

Effective Date: September 16, 2015

1. PURPOSE

The purpose of this Staff Manual Guide (SMG) is to provide an overview of the policies and procedures that govern the creation and maintenance of Privacy Impact Assessments (PIAs), which generally refer to both: information technology (IT) system PIAs and Third-Party Website/Application uses (TPWA) PIAs. PIAs are important risk management tools that are employed to implement privacy controls for Food and Drug Administration (FDA) information collections, IT systems and Agency uses of third-party websites and applications. PIAs are public documents that are published on FDA and Department of Health and Human Services (HHS) websites.

This SMG about PIAs applies to all FDA organizations.

2. REFERENCES

Instructional documents that will aid authors in the preparation of PIAs are available through the office of the Senior Official for Privacy (SOP).

- Privacy Act of 1974, 5 U.S.C. 552a

- Federal Information Security Management Act of 2002, 44 U.S.C. 3541 et seq (FISMA, Title III of the E-Government Act of 2002, 44 U.S.C. 101)

- Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (Dec. 18, 2014)

- National Institutes of Standards and Technology Special Publication 800-53, revision 4, Security and Privacy Controls for Federal Information Systems and Organizations (April 2013)

- OMB M-10-06, Open Government Directive (Dec. 8, 2009)

- OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010)

- OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010)

- HHS Standard Operating Procedures for Completing a Privacy Impact Assessment (August 11, 2010)

- HHS Third-Party Websites and Applications Privacy Impact Assessment Standard Operating Procedures (April 20, 2011)

- HHS Memorandum: Implementation of OMB M-10-22 and M-10-23 (December 21, 2010)

3. BACKGROUND

A. Purpose of Privacy Impact Assessments

A PIA is an analysis of how information is handled to:

- Ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

- Determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and

- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

For systems subject to the Privacy Act, much of the required content of the PIA will be the same as for its Privacy Act System of Records Notice (SORN, the subject of a separate part of this SMG series). For example, both documents contain information regarding the categories of records and PII maintained in the system, FDA uses and disclosures of the records, and the policies and practices for handling system information. In addition, when either the PIA or the SORN is amended, System Owners must review both documents to assess whether the other document needs to be revised or amended.

B. Importance of Privacy Impact Assessments

The PIA is a critical tool for spotting privacy risks and compliance needs, tracking implementation of privacy controls, identifying instances where the Agency collects or handles personally identifiable information (PII) and for identifying FDA systems subject to the Privacy Act. PIAs are also a key source of data required for FDA's regular reporting activities (e.g., the privacy section of Federal Information Security Management Act (FISMA) reports), responding to audits and data calls, mapping FDA's PII holdings, and other agency activities.

4. POLICY

A. Overall Policy

It is the current policy of the Department of Health and Human Services (HHS) to conduct a PIA for all information technology (IT) systems and electronic information collections regardless of the presence of personally identifiable information (PII)[1], and without qualification in relation to the subjects of the PII. It is also HHS policy to conduct a PIA for Agency uses of third-party websites and/or applications. HHS has developed two different analytical questionnaires for use in conducting the PIAs for these activities.[2]

The PIA serves numerous purposes, including to:

- Analyze the use of PII in relation to the subject system;

- Identify and address privacy risks, and select appropriate privacy controls to apply to the system;

- Ensure non-security issues are addressed such as notice, choice, consent, access, redress, and use and disclosure practices; and

- Ensure compliance with privacy-related laws and requirements, such as:

    - Authority to Collect (required by the e-Government Act)

[1] Where a system does not handle PII, a shorter version of the PIA, known as a Privacy Threshold Analysis (PTA) is used.

[2] HHS Information Systems Security and Privacy Policy (July 2014). In addition, the E-Government Act requires agencies to conduct PIAs when (1) developing or procuring IT systems or projects that collect, maintain, or disseminate PII from or about members of the public, or (2) when initiating a new electronic collection of PII for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government), consistent with the Paperwork Reduction Act (PRA). OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (M-03-22, September 26, 2003).

- SORN Completion (required by the Privacy Act)

- OMB Information Collection Approval (required by the Paperwork Reduction Act)

- Records retention and disposal (required by records managements laws and regulations)

B. Agency Information Systems

FDA must conduct a “standard PIA” for each Agency information system. These include systems operated by FDA personnel, contract employees, and systems operated by an external party on behalf of FDA. Each PIA must be completed and approved by the SOP prior to putting the system into operation (i.e., as a prerequisite to obtaining an Authorization to Operate (ATO)). This sequence is necessary in order to ensure the Agency does not operate a system without satisfying applicable requirements of law, regulation and policy.

C. Agency Uses of Third-Party Websites and Applications (TPWA)

TPWA uses include technologies such as social media websites that the Agency uses to communicate with and engage the public for the purpose of implementing principles of the Open Government Directive. The Office of Management and Budget (OMB) defines TPWAs as “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.[3] Often these technologies are located on a ‘.com’ Website or 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.”

As use of TPWAs expands, federal agencies are required to take specific steps to protect individual privacy whenever they use TPWAs to engage with the public (e.g., LinkedIn, Twitter, Flickr, Facebook, Instagram, blog/microblogging tools, YouTube, etc.).

Under OMB directive and HHS policy, FDA must conduct a PIA for each such use of a TPWA. The purposes of the TPWA, and the procedures and responsibilities mirror those of the standard IT system PIA described above.

When using a TPWA, the relevant FDA program management, system developer, system owner, or other person responsible for completing the PIA should adhere to the following requirements:

- Contact the staff of the SOP for guidance and materials as needed;

[3] OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications.

- Examine the third party’s privacy policy to evaluate the risks and determine whether the website or application is appropriate for FDA’s use;

- Prepare a TPWA PIA when the public will be engaging with the FDA through the use of a TPWA. That is, TPWAs that do not interact with the public do not require the completion of a TPWA PIA. Tools used for internal administration do not need a TPWA PIA, but are still subject to other listed standards and policies;

- Use an external link notice when visitors are directed to a nongovernment website;

- Review FDA’s web privacy policy (on FDA.gov) and contact the SOP as needed to ensure the TPWA use is appropriate and/or that the Agency policy is accurate in view of the TPWA use; and

- Prominently post a Privacy Notice on the third-party website or application itself, to the extent feasible. Required elements of the Privacy Notice are set out in OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010). Notice requirements are further described in HHS Memorandum: Implementation of OMB M-10-22 and M-10-23 (December 21, 2010) and the HHS-OCIO Policy for Information Systems Security and Privacy (July 2014).

5. RESPONSIBILITIES

The following sets out the general roles and responsibilities for Agency personnel with regard to PIAs. These roles and responsibilities are largely drawn from and intended to align with HHS policy.

A. System Owner or Program Manager

Individuals holding these positions are critical to the PIA process. The Agency as a whole and the Senior Official for Privacy (SOP) rely on their unique in-depth knowledge of their systems and projects when assessing compliance posture and privacy risks, selecting appropriate privacy controls, and implementing security and privacy controls.

Their roles and responsibilities regarding PIAs include:

- Ensure the accuracy and completeness of each PIA prepared.

- Prepare the standard PIA for an information system or information collection and/or the Third-Party Website/Application use (TPWA) PIA if necessary (collectively referred to as PIAs) for a new system/project before or during the concept stage of the mandatory Enterprise Performance Lifecycle (EPLC) process.

- Promptly submit the completed PIA to the Center PIA Reviewer for review and make any necessary changes in accordance with guidance provided.

- Promptly submit to the Center PIA Reviewer an updated PIA for each existing system/project at least every 36 months and at any time when planning or implementing a system change that creates new privacy risks or compliance issues.

- Obtain approval and signature of the PIA from the FDA's SOP.

- When a Plan of Action and Milestone (POA&M) is entered because of a lack of an SOP-approved PIA or when the SOP has approved a PIA and at the same time entered a POAM for remaining weaknesses to be remedied, the System Owner or Program Manager is responsible for completing the PIA, obtaining approval for the PIA, and removing the POA&M.

B. Information System Security Officer (ISSO)

FDA's ISSOs have particularly valuable technical expertise and are organizationally positioned to provide important input and guidance in relation to FDA's PIA program.

- Support the office of the SOP to ensure System Owners and program management are aware of the requirement to complete a PIA.

- Assist System Owners, Program Managers, Center PIA Reviewers, and SOP staff in identifying potential privacy risks for each system.

- Provide input and guidance as needed regarding security and technical content of PIAs.

- Recommend efficient approaches to PIA preparation and PIA inventory maintenance for maximum efficiency at the system, program and agency levels.

- Provide input and guidance on methods to implement privacy controls at the system program and agency levels.

- Cooperatively engage with System Owners, Program Management, Center PIA Reviewers and the staff of the SOP as needed to ensure consistency of operations and privacy compliance documentation.

- Advise SOP staff of planned, new or existing systems that require a new PIA.

- Support SOP staff as needed with regard to POAM procedures and management.

C. Center PIA Reviewer

Each Center has one or more PIA Reviewers. These Reviewers are typically designated by Center members of the Privacy Council. The SOP coordinates the drafting and review process with the PIA Reviewer, who provides initial guidance and assistance to the person authoring the initial PIA (see section 5.A. above). SOP staff will inform System Owners or other persons completing the PIA of who their Center PIA Reviewer is, if they are not already aware.

- Review PIAs as submitted by System Owners.

- Provide feedback and guidance to System Owners to ensure the questions in the PIA are answered correctly to account for all privacy issues present in the system.

- Confirm completeness of each PIA.

- Approve PIAs on behalf of their Center and submit PIAs to the SOP for approval.

- Assist System Owners, Program Management and SOP staff in identifying potential privacy risks for each system or project.

- Support the office of the SOP to ensure System Owners and program management are aware of the requirement to complete a PIA.

- Advise SOP staff in a timely manner of new or existing Center systems/projects that require a new PIA.

D. Staff of the SOP

- Maintain an inventory of all FDA PIAs.

- Provide general support to PIA authors and Reviewers.

- Notify System Owners, Program Managers, ISSOs, and Center PIA Reviewers of PIA due dates and status.

- Review PIAs that are submitted by Center PIA Reviewers for approval; assess the PIA for accuracy and completeness and recommend approval/disapproval to the SOP.

- Assess each PIA and verify whether the system addressed by the PIA may require preparation of additional materials such as:
  - a System of Records Notice (SORN) under the Privacy Act;
  - an Office of Management and Budget (OMB) Information Collection Request under the Paperwork Reduction Act (PRA);
  - an information retention schedule per the National Archives and Records Center guidance; or
  - any other compliance document or activity required to be reflected in the PIA.
- Provide feedback and instruction to Center PIA Reviewers and, when needed, directly to System Owners and Program Managers.
- Serve as PIA Reviewer for systems and projects operated within or organizationally owned by the Office of the Commissioner.
- Forward the SOP-approved PIA to HHS for Departmental review/approval.

E. Senior Official for Privacy

- Administers FDA’s PIA process; oversees selection and implementation of privacy controls.
- Provides programmatic direction, aligning FDA’s Privacy program with that recommended by the Department.
- Approves PIAs on behalf of FDA.

6. EFFECTIVE DATE

The effective date of this guide is September 16, 2015.

7. Document History – SMG 3297.5, Privacy Act Assessments (PIAs)

STATUS (I, R, C)	DATE APPROVED	LOCATION OF CHANGE HISTORY	CONTACT	APPROVING OFFICIAL
Initial	09/16/2015	N/a	OC/OES/ DFOI/Privacy	Sarah Kotler, Director, DFOI