SMG 3297.8

FDA Staff Manual Guides, Volume III - General Administration

Information Resources Management - Privacy Program

Policy for Implementation of the Privacy Act and the FDA Privacy Program:

Privacy Act System of Records Notices and Rulemaking

Effective Date: September 16, 2015
Changed: May 2, 2023

NOTE: This is not guidance for industry or the public.

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 a Privacy Act system of records notice (SORN) and any related rulemaking actions.

2. Background

The Privacy Act (5 U.S.C. 552a(e)(4)) and related FDA regulations (21 CFR 21.20) require that the Agency publish a notice in the Federal Register prior to operating a system of records. A Privacy Act "system of records" is a group of agency records from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying characteristic assigned to the individual. A collection of records does not have to be co-located (all stored in a single location) to be subject to the Privacy Act. Records may be subject to the Privacy Act regardless of form or format; they may be hard copy (paper) or electronic. Designating a set of records as a system of records is another way of saying that such records are subject to the Privacy Act.

A SORN is a public document, published in the Federal Register and on the Food and Drug Administration (FDA) website. It notifies the public of the existence of the system of records and describes the records and information collected and how the Agency will use this information. Prior to implementing any system of records[1] (e.g.,

[1] These procedures also apply to amendments to a system of records (e.g., adding new routine uses).

moving a new database into production status, initiating the use of a new tool that includes a system of records), FDA is required to publish a SORN in the Federal Register to inform the public of the existence of an FDA system of records and describe the purpose and character of the information the system contains. Notices must be published in the Federal Register for comment at least 30 days prior to implementation of the new system. (21 CFR 21.21(d)). In addition, before the SORN is published or concurrently, FDA must provide a copy of the Federal Register version of the SORN to the Office of Management and Budget (OMB), and Congress.[2] Reports to OMB and Congress regarding a new system of records must be transmitted at least 40 days prior to the operation of the new system of records. At the end of these time frames, if FDA has no changes to the SORN, the SORN is considered final and FDA posts a copy of the SORN on the Agency's publicly accessible website.

Publication of the SORN is a method of providing notice and transparency to the public. It provides an opportunity for the public to comment and inquire about a system of records before FDA begins to operate the information system. SORNs are also a useful resource for individuals interested in learning whether FDA holds records about themselves and/or who are considering submitting a Privacy Act request. Internally, SORNs provide management with a governance tool and serve as guidance for employees who handle information in a system of records (the SORN outlines the authorized uses and disclosures of information held in a system of records).

3. Policy

A. General Policy

At times, FDA will need to operate a system of records, and HHS and/or other Operating Divisions (OpDivs) within HHS will need to operate a system of records to serve a similar or identical purpose. Likewise, OpDivs and/or HHS may share or jointly operate and use a system. Under those circumstances, FDA may coordinate with OpDivs and/or HHS to develop a single SORN that will be applicable to all such systems of records. Concurrent with the internal development, clearance, and subsequent publication of a shared SORN, FDA provides appropriate documentation and information to the relevant OpDivs and/or HHS.

Prior to implementing a system of records, FDA is required to publish a Privacy Act system of records notice (SORN) in the Federal Register to inform the public of the existence of FDA systems of records and describe the purpose and character of the information the system contains. As noted below, existing SORNs may apply to a system of records and sufficiently cover the records such that a new SORN is not required. Therefore, assessing whether one or more existing SORNs apply to an information system (or a collection of information) is typically

[2] Chair of the House Committee on Oversight and Government Reform, and Chair of the Senate Committee on Homeland Security and Governmental Affairs.

the first step after that system is determined to be subject to the Privacy Act. This assessment is conducted jointly by the SOP, system owner, program management and Office of Chief Counsel.

A SORN describes the information about individuals that an FDA system collects and how FDA will use and disclose records in the system, i.e., it details the permissible and appropriate disclosures by Agency personnel of information from the system of records. The SORN includes:

- System of records number (assigned by the SOP)
- Privacy Act system of records name
- Location(s) of the records in the system of records
- Categories of individuals who are the subjects of the records
- Categories of records/information in the system of records
- Authority for the collection of information
- Purpose of the collection
- “Routine uses” of records in the system of records (discretionary disclosures to recipients outside HHS, see the Privacy Act, 5 U.S.C. 552a(c))
- Storage
- Retrievability (the manner in which records are indexed and retrieved)
- Safeguards (security and access restrictions)
- Retention and disposal
- System manager name and contact information
- Notification procedures
- Record access procedures
- Contesting record procedures
- Record source categories
- Exemptions claimed for the system (if any)

Concurrent with the internal development, clearance, and subsequent publication of the SORN, FDA provides appropriate documentation and information to HHS, OMB, and Congress.

Following publication of the SORN in the Federal Register, HHS and FDA make FDA SORNs available to the public in electronic form on HHS.gov (https://www.hhs.gov/foia/privacy/sorns/fda-sorns.html) and FDA.gov (https://www.fda.gov/regulatory-information/freedom-information/privacy-act) and internal intranet pages.

B. Government-wide and Department-wide Records & SORNs

Not every FDA system that is subject to the Privacy Act will require publication of a new SORN. FDA systems of records that are common to federal agencies may fall under SORNs that are government-wide and/or HHS-wide in scope. For example, the Office of Personnel Management (OPM) issues SORNs for certain personnel record systems common to agencies across the federal landscape. Likewise, HHS publishes SORNs concerning certain Department-wide personnel and administrative management records. HHS makes all HHS SORNs available on HHS.gov (https://www.hhs.gov/foia/privacy/sorns/index.html).

FDA organizations should consult the relevant government-wide and HHS-wide SORNs for guidance on the collection, use and disclosure of information in systems of records covered by such SORNs. Links to these SORNs are available on FDA's intranet page for the Agency's Privacy Office.

Where appropriate, a single SORN may cover multiple instances of the retention of records in separate agencies or offices. In some instances, FDA maintains central records systems, and FDA offices that feed information into the central system also maintain copies of their submissions. In other cases, another government agency or HHS Operating Division, (e.g., the Office of Personnel Management or the National Institutes of Health) maintains a central records system and FDA maintains copies of records supplied to, or kept in, those systems. In either case, such an arrangement is regarded as a single system of records. The SORN is prepared and kept up to date by the system owner subject to the guidance and approval of FDA's SOP.

In keeping with OMB guidance against the publication of duplicative SORNs, FDA does not publish SORNs for FDA systems covered by existing government- wide or HHS-wide SORNs.

C. Exempt Records

Some systems of records, such as those that include investigatory or law enforcement records, may be appropriate for exemption from the access, amendment, or other provisions of the Privacy Act. The Privacy Act specifies that its provisions do not allow an individual access to any information compiled in

reasonable anticipation of a civil action or proceeding. 5 U.S.C. 552a(d)(5). In addition, the Privacy Act provides "general" and "specific" exemptions.[3] To exempt a system of records based on these other exemptions in the Privacy Act, the Agency must promulgate a final rule – in addition to publishing the SORN (which also specifies the exemption) in the Federal Register. A rulemaking typically requires formal clearance within FDA and HHS.

It is FDA policy[4] that systems of records should be exempted from certain provisions of the Privacy Act if they are essential to the performance of a law enforcement function. Law enforcement functions include enforcement of laws that are administered and enforced by FDA as well as enforcement of laws that govern the FDA.

Any exemptions for a system of records are required to be identified in the Privacy Act SORN for the system. FDA identifies exempted Privacy Act systems of records in its privacy regulations (HHS also lists FDA's exempt systems of records in its privacy regulations), and on public-facing and internal webpages. HHS also lists FDA's exempt systems of records in its privacy regulations.

Prior to publication of the SORN, Agency organizations may not implement (go into a production or operating status) a system of records. Agency organizations may not employ or rely on any exemptions identified in the SORN until it has promulgated a final rule specifying the exemptions.

4. Responsibilities

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

A. System Owner

- Prepare the initial draft of a SORN and companion submissions to Congress and OMB for their system(s). System Owners are uniquely positioned to prepare an accurate and complete draft as they have in-depth, system-specific knowledge about their system and related data collection, use, and sharing.

- Submit the draft SORN to the Senior Official for Privacy.

- For systems of records which are proposed to be exempt from provisions of

[3] 5 U.S.C. 552a(j) and (k). For example, 552a(j) states that agencies can exempt SORs from requirements of the Act if the SOR contains information (1) maintained by the Central Intelligence Agency, or (2) maintained by a principal function criminal law enforcement agency and compiled for criminal law enforcement purposes.
[4] 21 CFR 21.60.

the Privacy Act under 5 U.S.C. 552a(j) or (k)[5], the System Owner will, when preparing the initial draft SORN and accompanying materials (or subsequently if exemptions become necessary after FDA has published a SORN for the system) as noted above, provide a rationale for the exemption and prepare an initial draft of the required rulemaking notice in tandem with the SORN and in keeping with the SORN process outlined in this document.

Templates and guidance are available from the staff of the Senior Official for Privacy (SOP).

B. Staff of the SOP

- Provide subject matter expertise and guidance on SORN development and the formal clearance process to System Owners.

- Coordinate review and revision to finalize the draft SORN, including engaging with System Owner, the Chief Information Security Officer (CISO), the Chief Information Officer (CIO) and/or relevant offices under the CIO, the Office of Legislation, Regulations Policy Management, and Departmental counterparts (e.g., HHS Privacy Act Officer) as necessary based on the nature of the information system and the offices that use, operate or disseminate records held in the system.

- Following review and revision by relevant offices as described above, provide a draft of each SORN to, or otherwise coordinate with, the Office of Chief Counsel (OCC) for review.

- Manage the formal clearance process. The process typically requires formal clearance by senior level management in multiple offices including the home organization for the system, stakeholder organizations outside the home organization (e.g., system data is used by other organization/Centers), CIO, CISO, OCC, and the Office of the Executive Secretariat (OES). Whenever feasible, the staff of the SOP will coordinate concurrent (rather than consecutive) clearance by these offices.

- On an as-needed basis, submit the final, FDA-approved SORN to the Department of Health and Human Services (HHS) for their awareness and/or review, comment, and concurrence. This coordination with HHS is particularly appropriate with SORNs that entail a parallel rulemaking,

[5] U.S.C. 552a(k) states that agencies can exempt SORs from requirements of the Act if the SOR contains (1) classified information, (2) investigatory material compiled for law enforcement purposes (other than material within the scope of (j)(2)), (3) information maintained in connection with providing protective services to the President of the United States or other individuals, (4) information required by statute to be maintained and used solely as statistical records, (5) information that reveals a source provided an express promise of confidentiality in the context of background investigatory material, and (6) testing material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing process.

such as for a system of records that FDA proposes should be exempt from requirements of the Privacy Act for law enforcement purposes.

C. Senior Official for Privacy

- Administer FDA's SORN process.
- Provide programmatic direction, aligning FDA's Privacy program and SORNs with that of the Department.
- Determine whether a new or newly documented system of records is fully covered by existing SORN(s).
- Approve and clear SORNs on behalf of FDA.
- Following completion of the formal clearance process, provide the final SORN, proposed rule, and narrative statement to: (1) FDA's Office of Legislation within the Office of the Commissioner (OC), which will in turn submit these required materials to certain Congressional committees; and (2) to the Regulations Policy and Management Staff (RPMS) within the Office of Policy and Planning (OPP), which will submit materials for publication in the Federal Register and to the Office of Management and Budget (OMB)[6].

5. Effective Date

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

6. Document History - SMG 3297.8, "Privacy Act System of Records Notices and Rulemaking"

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
Change	04/26/2023	organizational information and cited authorities	OEMS/DIG/ Privacy	Tiffany Branch, Director, OEMS

[6] The timing and content and other details regarding the submissions to OMB and the Congressional Committee Chairs are described in OMB Circular A-130, Appendix I.

APPENDIX A

References and Authorities

Statutes

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

Regulations

- HHS Privacy Act Regulations, 45 CFR Part 5b
- FDA Public Information and Privacy Act Regulations, 21 CFR Parts 20 and 21

OMB Issuances

- OMB Circular A-130, Managing Information as a Strategic Resource (Revised July 27, 2016; Appendix I, Federal Agency Responsibilities for Maintaining Records about Individuals)
- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (December 27, 2016)

HHS & FDA Policies, Procedures, and other Materials

- HHS Rules of Behavior for the Use of HHS Information and IT Resources Policy (June 7, 2019)
- HHS Policy for Rules of Behavior for Use of Information and IT Resources (February 2023)
- FDA Staff Manual Guides for Information Technology Security (series 3250)