SMG 3297.4

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: OVERVIEW

Effective Date: September 16, 2015

1. Purpose
2. References
3. Background
4. Policy
5. Additional Privacy Act Considerations
6. Responsibilities
7. Effective Date
8. History

Appendix A (References and Authorities)

1. PURPOSE

The purpose of the overall Agency-wide Policy for Implementation of the Privacy Act and the FDA Privacy Program is to provide an overview of the basic privacy mandates contained in the Privacy Act of 1974 (the Privacy Act), the Federal Information Security Management Act of 2002 (FISMA)[1], and the Federal Information Security Modernization Act of 2014 (FISMA 2014), Office of Management and Budget (OMB) directives, National Institutes of Standards and Technology (NIST) guidance, and associated FDA and Department of Health and Human Services (HHS or the Department) policies and procedures.

This Purpose section of the overall Privacy Staff Manual Guide (SMG) generally describes the attributes, requirements and organizational roles in relation to the Food and Drug Administration's (FDA or the Agency[2]) privacy program. Subsequent separate sections of this SMG provide more detailed descriptions of specific privacy program requirements and roles, including:

- FDA Privacy Council (see SMG 2010 series)
- Privacy Impact Assessments (PIAs)

[1] FISMA was enacted as Title III of the E-Government Act of 2002.
[2] Note that "Agency" will be capitalized to refer to the FDA and "agency" will refer to any given government agency.

- Incident Reporting and Breach Response
- Privacy Act Requests and Appeals
- Privacy Act System of Record Notices (SORNs)
- Accounting of Disclosures under the Privacy Act

2. REFERENCES

This Guide supplements privacy related statutes, regulations, policies and procedures set forth in directives, policies, statutory sources and other reference materials such as those listed in Appendix A.

3. BACKGROUND

The federal government maintains information about individuals in order to carry out its diverse activities and programs. Privacy related laws, Executive Orders, regulations, policies, and procedures generally seek to balance the information requirements and needs of the government against the privacy interests and concerns of the individual.

A. Definition of Privacy; Fair Information Practice Principles

The term “privacy” has no singular meaning. It has varying definitions and uses among nations, states, regions, cultures and industries, and the meaning may evolve over time due to technological advances and changing social and moral values. One common working definition states that privacy is the set of concerns about how information about individuals is collected, used, maintained, shared, disclosed, and destroyed, and how these actions align with law and the reasonable expectations of the subjects of the information.

Consistent concepts and principles embodied in privacy are described in the Fair Information Practice Principles (FIPPs). These principles are the foundation of federal privacy mandates and policies. The FIPPs were first generated by the US Department of Health, Education, and Welfare in 1973. Government agencies should strive to continuously and consistently adhere to the FIPPs whenever collecting or handling personally identifiable information (PII).

The FIPPs as adopted to apply to the FDA’s structure and mission:

- **Accountability and Auditing**: Strive to be accountable for complying with these principles and the legal and policy requirements flowing therefrom, support accountable behavior at all levels by providing training to employees

and contractors who use or handle PII, and when appropriate audit organizational use of PII to demonstrate compliance and manage risk.

- **Purpose and Authority Specification**: Articulate the authority that permits the collection of PII and the purpose or purposes for which the PII is intended to be used.

- **Transparency**: Exhibit transparency; provide notice regarding the collection, use, dissemination, and maintenance of PII.

- **Use Limitation**: Use and share PII only to the extent necessary to perform official agency work and only for purposes that are compatible with the purpose for which the PII was collected.

- **Data Minimization**: Collect only PII that is directly relevant and necessary to accomplish the purpose(s) authorized by statute, regulation, or Executive Order and retain PII only for as long as is necessary to fulfill the specified purpose(s). In keeping with applicable Paperwork Reduction Act (PRA) and record keeping requirements, document disposal actions.

- **Individual Participation and Redress**: Collect PII directly from the subject individual when possible and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Safeguard individual interests by providing mechanisms for appropriate access, correction, and redress regarding the Agency's use of PII and the accuracy, timeliness and completeness of the PII.

- **Data Quality and Integrity**: To the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

- **Security**: Protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

B. Definition of Personally Identifiable Information

The federal government has adopted a broad definition of "personally identifiable information."[3] PII refers to any information which can be used to distinguish or

[3] "The term 'PII,' as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual." OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010) at page 8, referencing OMB Memorandum M-07-16,

trace an individual's identity (e.g., name, Social Security number (SSN), passport number, patient number, telephone number, email address, biometric records, etc.), either standing alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual. For example, many individuals may share a date of birth, place of birth, or last name, but if there were a way to connect all three of these elements held in separate records to a single individual, the three items together would most likely identify a single individual. Also, there are some items of information that may not at first consideration seem to identify an individual, but may be easily used to do so. A website visited, for example, would not seem to identify an individual, but if that website linked to an individual's social media page it could be used, alone or in combination, to identify the individual.

The definition of PII is not anchored to any single category of information or technology. It calls for a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, recognize that non-PII can become PII whenever additional identifying information is added—in any medium and from any source.

Personal information that could be used to identify any individual is PII. Neither the manner in which the information is collected, nor the nature of its connection to the individual determines whether information is PII. Information that is PII remains so whether the PII is publicly available, provided voluntarily, or collected by mandate. PII remains PII whether it pertains to employees, the public, research subjects, business partners or other individuals. Data that identifies or is linkable to an individual in his/her personal or professional/work capacity is PII. For example, business contact information about FDA employees which the Agency makes available to the public is PII, although it seems obvious that this information requires a lower standard of protection than more sensitive PII such as health records, human resources and personnel records, investigatory files, and financial account information.

C. Privacy Mandates

Privacy mandates imposed on FDA and other federal agencies are numerous but do not uniformly apply to all PII. For example, not all FDA records containing PII are subject to the Privacy Act and the requirements imposed by the Act. Only those records that are "about a person" and that are maintained in a system of records from which these records are retrieved by an individual's name or personal identifier are subject to the Privacy Act. The Privacy Act and related FDA activities and procedures are discussed in detail in separate sections of this Privacy SMG.

Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007).

The privacy provisions of the FISMA and the related Office of Management and Budget (OMB) directives and HHS implementing policies require that FDA conduct a Privacy Impact Assessment (PIA) for each FDA use of Information Technology (IT) to collect information, and, a separate PIA for each Agency use of a Third-Party Website or Application (TPWA)[4] conducted for the purpose of engaging with the public. PIAs are important risk management tools that are employed to implement privacy controls for relevant FDA information collections, IT systems and Agency uses of third-party websites and applications. FDA conducts a PIA for each Agency IT system and TPWA whether or not it is designed to collect PII. The PIA serves as a tool to identify the extent to which individual systems handle PII, whether a system is subject the Privacy Act, and to identify and implement appropriate privacy protections.

PIAs, their purpose and related operational responsibilities are discussed in detail in separate sections of this Privacy SMG.

D. FDA Privacy Program Mission

FDA recognizes the significance of maintaining the trust of the public through the protection of privacy and the safeguarding of PII. It is FDA policy[5] to collect, maintain, use and disseminate records in a manner which protects individual privacy to the fullest possible extent consistent with laws relating to disclosure of information, the law enforcement responsibilities of FDA, and administration and program management needs. It is FDA's intent to take all reasonable action to align FDA policies, procedures and activities with the Fair Information Practice Principles (FIPPs) as set forth above.

FDA recognizes the inherent importance of information security as an essential element of a successful privacy program. Security and privacy share the goal of protecting the confidentiality and integrity of information about individuals (although each discipline has additional goals as well). FDA's Senior Official for Privacy (SOP) and the Chief Information Security Officer (CISO), and their staff, must maintain a close working relationship and effectively coordinate overlapping activities.

System Owners[6] must apply sound judgment when considering whether to engage in the collection, use or sharing of PII. The unnecessary or unauthorized collection of PII is poor risk management, and can result in the inefficient dedication of security, budgetary, and other resources, or even violations of the

[4] Examples of TPWAs include FDA's use of Facebook, LinkedIn, Twitter accounts, and YouTube as well as individual public-private partnerships employing non-government websites, mobile applications, or similar public outreach and engagement tools.
[5] FDA's privacy regulations, policy concerning records about individuals, 21 C.F.R. 21.10
[6] "Information System Owner (or Program Manager): Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system." National Institute of Standards and Technology Special Publication 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, Appendix B (April 2013).

law. Data minimization (one of the FIPPs) is therefore necessary for breach prevention as well as savvy financial planning.

FDA must decide what information about individuals is relevant and necessary to accomplish a purpose authorized by statute or Executive Order. There must be a deliberate determination that the information to be collected is indeed required to meet the needs of the program concerned. In addition, consideration should be given to whether identifiable data is necessary or whether non-identifiable data would suffice. If the records use IT and/or third-party websites or applications, the Agency must conduct an assessment of the privacy impact as required by FISMA and the E-Government Act.

4. POLICY

In addition to the general policies and principles described above, the following elements of FDA's privacy program policies are described in distinct sections of this policy (SMG). Please review the following sections for more detailed information:

- FDA Privacy Council
- Privacy Impact Assessments (PIAs)
- Incident Reporting and Breach Response
- Privacy Act Requests and Appeals
- Privacy Act System of Record Notices (SORNs)
- Accounting of Disclosures under the Privacy Act

5. ADDITIONAL PRIVACY ACT CONSIDERATIONS

A. Computer Matching

The Computer Matching and Privacy Protection Act of 1988 and the Computer Matching and Privacy Protection Amendments of 1990 are incorporated into the Privacy Act to provide procedural requirements that agencies must follow when performing computer matching activities.

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act to add procedural requirements for agencies to follow when engaging in computer matching activities. As amended, the Privacy Act defines a matching program as one in which any computerized comparison of two or more systems of records established for certain purposes regarding federal benefits programs or personnel or payroll systems. This definition includes comparisons of two or

more federal systems of records and of federal systems of records and non-federal records.

To constitute a computer matching program under this section of the Privacy Act, the matching activity must have as its purpose one or more of the following:

- Establishing or verifying initial or continuing eligibility for federal benefits programs;

- Verifying compliance with the requirements of such programs; or

- Recouping payments or delinquent debts under such federal benefits programs.

Examples of federal initiatives incorporating computer matching programs include Food Stamps, Aid to Families with Dependent Children, and Medicaid.

Currently, FDA does not engage in any computer matching programs. If your Center is exploring such activities, please contact the Privacy Act Coordinator in the office of the SOP for guidance before moving forward.

B. Penalties for Privacy Act Violations

In addition to penalties imposed under other applicable civil and criminal laws and administrative policies, the Privacy Act permits individuals to sue the Agency for certain violations of the Act[7], and subjects permanent and contract personnel[8] to a misdemeanor charge and a fine of not more than $5,000 for willfully or knowingly:

- Disclosing Privacy Act records to any person or agency not entitled to access to such records;

- Maintaining a Privacy Act system of records without first publishing the prescribed public notice (system of records notice or “SORN”) in the Federal Register; and

- Requesting or obtaining any record from any system of records under false pretenses. Such persons may also be subject to prosecution under the False Reports to the Government Act, 18 U.S.C. 1001.

[7] 5 U.S.C. 552a(g)(1) Civil remedies.
[8] 5 U.S.C. 552a(i)(1) Criminal penalties; 5 U.S.C. 552a(m) Government contractors.

6. RESPONSIBILITIES

The following sets out the general roles and responsibilities for Agency personnel with regard to privacy policies, procedures, programs and activities. These roles and responsibilities are largely drawn from and intended to align with HHS policy. Note that more specific duties are set out in FDA and HHS policies and procedures implementing relevant statutes, Executive Orders, and OMB guidance and directives.

A. Senior Official for Privacy (SOP)

FDA's SOP currently serves as the Deputy Director of FDA's Division of Freedom of Information (DFOI).

The SOP occupies a lead role in overseeing, coordinating, and facilitating the Agency's privacy compliance efforts.[9] The SOP serves in a central policy-making capacity in the Agency's development and evaluation of legislative, regulatory, and other internal or public-facing policy proposals which implicate information privacy. Among other duties, the SOP is responsible for Agency compliance with the Privacy Act of 1974 and the privacy requirements of the Federal Information Security Management Act (FISMA).

The SOP is also responsible for implementing Appendix J of the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." The SOP is the approving authority for the selection and assessment of the NIST privacy controls (hereinafter "controls" or "privacy controls") as applied at the system, program and agency-wide level. The SOP typically selects and approves Appendix J privacy controls as part of the Agency's Privacy Impact Assessment (PIA) program, and approves of all FDA PIAs immediately before they are sent to the HHS Senior Agency Official for Privacy (SAOP) for final approval.

Specific responsibilities of the SOP include:

- Implement policy and provide programmatic direction to the FDA Privacy Office and its staff;

- Promote a culture of privacy and executive accountability for ensuring activities are compliant with all privacy requirements;

- Ensure the Agency's information privacy procedures are comprehensive, up-to-date, and consistent with Department privacy requirements, laws, regulations, and adopted guidance;

[9] The SOP role and authority is also detailed in OMB M-14-04 at p22-24; HHS Information System Security and Privacy Policy (July 2014) at p24-26.

- In coordination with the CISO, verify that appropriate privacy controls protect PII held in information systems and record collections;

- Provide expertise and guidance in addressing the Agency's responses to privacy incidents to include coordinating with the FDA CISO, FDA Computer Security Incident Response Team (CSIRT), the HHS Computer Security Incident Response Center (CSIRC), and HHS Privacy Incident Response Team (PIRT); and

- Support internal reporting as needed to ensure compliance, meaningful program analysis and accountability, and accuracy of Agency reports.

The FDA SOP also plays key roles in establishing and maintaining FDA's Privacy Council, ensuring the maintenance of privacy training activities, and, coordinating with stakeholders in responding to data breaches involving PII. The SOP will consult with the Office of Chief Counsel (OCC) to seek legal advice as appropriate.

The staff of the SOP support Agency-wide implementation of the Privacy Act and Agency information privacy policies and procedures at the direction of the SOP, including addressing:

- Privacy Act requests;

- Other Agency actions required by the Privacy Act;

- PIA program needs;

- Documentation of privacy compliance for information systems and records collections, such as those required by the Privacy Act and e-Government Act of 2002;

- Privacy requirements in contracts, memoranda of understanding, statements of work, and other written agreements;

- Privacy incidents; and

- Serving as privacy subject matter experts and points of contact for Agency personnel, including for the purposes of conducting education, awareness and training on privacy issues.

B. Key Internal Privacy Partners

Given the relationship between privacy, security, records management, contracting and legal activities that apply to data held and used across the

Agency, it is crucial that the SOP maintain close working relationships with the following Agency programs:

- Office of Information Management and Technology (OIMT)
    - Chief Information Security Officer (CISO)
        - Information System Security Officers (ISSOs)
        - Policy, Awareness, and Training Team Advanced Forensics & Insider Threat Team; Computer Security Incident Response Team (CSIRT)
    - Office of Information Management (OIM)
        - Center Information Technology Liaisons (CITLs)
    - Office of Informatics and Technology Innovation (OITI) and the Chief Health Informatics Officer (CHIO)
- The Office of Chief Counsel
- Center Freedom of Information Act Offices
- Records, eDiscovery and Risk Management
- Paperwork Reduction Act experts
- Office of Acquisitions and Grants Services (OAGS)
- Office of Criminal Investigations; Internal Affairs; Trusted Workforce and Insider Threat
- Privacy Council members, and Center/Organization privacy contacts
- Center and Organizational Level PIA Reviewers
- Social Media Working Group

C. Chief Information Security Officer

- Foster communication and collaboration among the Agency's security and privacy stakeholders to share knowledge and to better understand threats to FDA information;
- Advise the SOP of reported privacy incidents and coordinate with the SOP on incident response plans and activities; and

- Coordinate with the SOP on the Federal Information Security Management Act (FISMA), the 2014 Federal Information Security Modernization Act and other overlapping reporting requirements; and

- Provide insight regarding potential automated solutions regarding privacy controls, compliance actions and reporting requirements.

D. Center/Component-Designated Privacy Contacts

- Support SOP privacy program activities to ensure effectiveness Agency-wide;

- Participate in the SOP's privacy policy development activities;

- Provide privacy guidance within the Center;

- Serve as or designate PIA Reviewers for system owner drafts of PIAs for Center programs, certify accuracy and completeness of PIAs, and recommend SOP approval or non-approval of PIAs;

- Support Agency responses to Privacy Act requests for records used or maintained within their Center;

- Participate in the preparation of SORNs for Center systems subject to the Privacy Act;

- Support SOP validation of PIA responses at the system level;

- Contribute to the development and implementation of PII disposal procedures at the system level in accordance with applicable National Archives and Records Administration (NARA) - approved records retention schedules, and, consistent documentation of PII disposal actions;

- Participate in Privacy Council activities; and

- Assist the SOP in dissemination of privacy guidance to personnel.

E. Paperwork Reduction Act (PRA) Team/Officer

- Respond to Program Management and System Owner requests for guidance on potential PRA requirements such as preparing an Information Collection Request (ICR) for OMB approval prior to engaging in the collection Support program and system personnel efforts to identify existing OMB ICRs and associated approval numbers for PIA purposes; and

- Provide guidance on whether the use of third-party websites or applications creates information collection activities subject to OMB clearance under the PRA.

F. Records Management

- Provide subject matter expertise and support the SOP, Chief Information Security Officer (CISO), program management and system owners to ensure record maintenance in accordance with NARA requirements, relevant laws and regulations, and Agency policy;

- Support activities for the timely destruction of records containing PII;

- Assist relevant Agency organizations on the applicability of records management to uses of third-party websites and applications; and

- Support SOP and CISO efforts to develop policies and procedures to enable the manual or automated documentation of PII destruction.

G. Acquisitions & Grants Services; Contracting Officers[10]

- Maintain a working relationship with and consult the Office of the SOP (also referred to as the Privacy Office or staff of the SOP) for guidance and assistance as needed;

- When a Program Office's requisition package (submitted to OAGS) identifies Privacy Act implications (e.g., contract requires a contractor to operate an information system subject to the Privacy Act), ensure contracts contain appropriate HHS and Federal Acquisition Regulation Privacy Act clauses[11], related FDA regulation clauses (21 CFR 21.30(e)), and other appropriate provisions concerning privacy[12]; and

[10] See HHS Information System Security and Privacy Policy (July 2014) at p37.

[11] Federal Acquisition Regulations (FAR) are at Title 48 of the Code of Federal Regulations including 48 CFR 52.224-1 (Privacy Act Notification); 48 CFR 52.224-2 (Privacy Act); and 48 CFR 52.239-1 (Privacy or Security Safeguards). HHS Acquisition Regulations (HHSAR) are also within Title 48 of the Code of Federal Regulations including privacy clauses at 48 CFR 352.224-70 (Privacy Act); 48 CFR 352.239-72 (Security Requirements for Federal Information Technology Resources); 48 CFR 324.1 (Protection of Individual Privacy); and 48 CFR 324.2 (Freedom of Information Act). HHS Privacy Act regulations also have relevant content, e.g., 45 CFR 5b.12 (Contractors) and 48 CFR 5b at Appendix A(e) (Standards of Employee Conduct – Contracting officers).

[12] The Privacy Act directs agencies to cause the requirements of the Act to be applied to contractors operating a system of records on behalf of the agency. 5 U.S.C. 552a(m)(1). FDA regulations require the Agency to review all contracts before award to determine if the contractor will operate a system of records from which information will be retrieved by individual names or other personal identifiers in order to accomplish an FDA function, and, if so, to include certain clauses in the solicitation and contract. 21 CFR 21.30(e). HHS regulations require Contracting Officers (COs) to review all proposed contracts for the operation of a Privacy Act system of records and take certain steps to ensure compliance. 45 CFR 5b, Appendix A, section (e). HHS policy identifies COs as responsible for coordinating with other offices to

- As permitted by law, regulation and policy, provide copies of contract materials to the SOP upon request or otherwise assist in providing relevant information to the SOP and/or permitting the SOP to access proposed or existing contract materials.

H. Program Management, System Owners[13] and Project Officers

- Ensure system security breaches are reported in accordance with Agency security policies and support the Agency's privacy incident response activities;

- Seek to incorporate privacy-by-design: actively identify potential PII collection and privacy issues at the earliest possible project stage (e.g., initiation, concept, predesign) and obtain appropriate guidance from the SOP and Counsel;

- Identify program activities, processes and systems that may require compliance with privacy requirements such as the completion of a PIA or SORN and hold process or system owners accountable for addressing these requirements;

- Proactively identify and inform the SOP of the potential need to address privacy issues in contracts, solicitations, or other documents reflecting agreements with parties outside of the FDA, such as program plans for the acquisition of services and products that involve third-party handling of PII entrusted to FDA;

- Effectively apply privacy protections and controls to systems as directed by the SOP as a precondition to the Agency's issuance of an authorization to operate (ATO) a system;

- Ensure timely completion of PIAs and SORNs as part of the Enterprise Performance Lifecycle (EPLC), ATO, IT Investment Management (ITIM) processes or otherwise;

- Identify additional resources needed to complete PIAs and SORNs and/or to effectively implement selected controls;

---

ensure appropriate privacy language is incorporated into each IT contract, determining applicability of the Privacy Act, advising contractors who develop or maintain a system of records that the Act applies to them, monitoring contract performance and deliverables for conformance with privacy-related contract requirements, and enforcing the requirements of privacy clauses. HHS Information System Security and Privacy Policy (July 2014) at 13, 37-38.

[13] HHS Information System Security and Privacy Policy (July 2014) at 31-33.

- Support responses to HHS and FDA issued data calls, audits, contract review initiatives, privacy controls assessments and other SOP actions;

- Inform the SOP of planned new collections or uses of PII in existing or in-development systems;

- Conduct timely disposal of PII in accordance with applicable NARA-approved records retention schedules and maintain consistent documentation of PII disposal actions;

- Ensure personnel receive general and role-based privacy training commensurate with their duties in relation to PII and Privacy Act records;

- Contact the SOP as needed for guidance in order to ensure appropriate privacy clauses are included in contracts, Memoranda of Understanding (MOU) and Information Sharing Agreements (ISAs);

- Review applicable SORNs and/or consult the Office of the SOP before engaging in new internal or external uses of PII;

- Assist the Agency in responding to Privacy Act requests;

- Provide system knowledge and support Agency activities to respond to requests to amend Privacy Act records;

- Disseminate amended Privacy Act records to internal and external partners (recipients of the records prior to amendment) as necessary; and

- Obtain guidance from the SOP and implement effective procedures for the creation and maintenance of an "accounting" of disclosures for systems subject to the Privacy Act, and support SOP validation of accounting.

I. Website Owner/Administrator

- Coordinate website privacy practices and compliance activities with the SOP;

- Ensure that any FDA website that employs a multi-session web measurement and tracking technology that collects PII is approved by the appropriate FDA and HHS officials (e.g., the FDA SOP, the HHS Senior Agency Official for Privacy (SAOP)) prior to its use[14]; and

[14] See HHS Memorandum "Implementation of OMB M-10-22 and M-10-23" (issued by the HHS CIO/SAOP December 21, 2010).

- Ensure that FDA websites or Agency uses of a third-party website or application includes applicable privacy policies, privacy notices, and machine-readable privacy policies and that the content is accurate.

J. General Agency Personnel (permanent and contract employees)

- Support a consistent culture of privacy within FDA;
- Adhere to the HHS Rules of Behavior and FDA information policies;
- Assist in Agency efforts to identify, report, and respond to any privacy incident/breach; and
- Protect and disclose PII and Privacy Act records in accordance with the law, regulations and Agency policy.

7. EFFECTIVE DATE

This guide is effective September 16, 2015, and supersedes SMG 3297.4 "Procedures for Implementation of the Privacy Act", issued August 14, 1981.

8. Document History – SMG 3297.4, Implementation of the Privacy Act and the FDA Privacy Program: Overview

STATUS (I, R, C)	DATE APPROVED	LOCATION OF CHANGE HISTORY	CONTACT	APPROVING OFFICIAL
Change	09/25/2014	Attachment A	OC/OES/DFOI	Frederick Sadler, Director, DFOI
Revision	09/16/2015	N/a	OC/OES/ DFOI/Privacy	Sarah Kotler, Director, DFOI

APPENDIX A

References and Authorities

Statutes:

- 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. N. 113-283 (Dec. 18, 2014)

Regulations:

- HHS Privacy Act Regulations, 45 CFR Part 5b
- FDA Public Information and Privacy Act Regulations, 21 CFR Parts 20 and 21
- Federal Acquisition Regulation (FAR), Title 48 of the Code of Federal Regulations including 48 CFR 52.224-1 (Privacy Act Notification); 48 CFR 52.224-2 (Privacy Act); and 48 CFR 52.239-1 (Privacy or Security Safeguards)
- HHS Acquisition Regulations(HHSAR), Title 48 of the Code of Federal Regulations including privacy clauses at 48 CFR 352.224-70 (Privacy Act); 48 CFR 352.239-72 (Security Requirements for Federal Information Technology Resources); 48 CFR 324.1 (Protection of Individual Privacy); 324.2 (Freedom of Information Act)

National Institute of Standards and Technology Special Publications:

- NIST Special Publication 800-53, rev 4, Security and Privacy Controls for Federal Information Systems and Organizations (April, 2013)

OMB Issuances:

- OMB M-14-04, FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (November 18, 2013)
- OMB M-11-02, Sharing Data while Protecting Privacy
- 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)

- OMB M-07-16, Safeguarding Against and Responding tthe Breach of Personally Identifiable Information (May 22, 2007)

- OMB M-06-19, Reporting Incidents Involving Personally identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006)

- OMB M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006)

- OMB Circular A-130, Management of Federal Information Resources (Revised November 28, 2000)

HHS & FDA Policies, Procedures and other Materials:

- Rules of Behavior for Use of HHS Information Resources (July 24, 2013)

- HHS-OCIPolicy for Information Systems Security and Privacy (July 2014)

- HHS-OCIPolicy for Information Systems Security and Privacy Handbook (July 7, 2011)

- 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)

- HHS Privacy Incident Response Team (PIRT) Standard Operating Procedures (January 27, 2012)

- FDA Staff Manual Guides for Information Technology Security (series 3250)