U.S. Department of Health and Human Services (HHS)
Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* Privacy Report
Semi-Annual Report for Calendar Year 2019
Covering January 1, 2019–June 30, 2019

Table of Contents

1. Introduction

As required by Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, Pub. L. No. 110-53 (Section 803), this *Report* provides information about privacy activities at the U.S. Department of Health and Human Services (HHS) during the reporting period January 1, 2019 through June 30, 2019.

2. Legislative Language

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*[1], as amended, sets forth the following requirements:

"(f) Periodic Reports-

(1) In General –

The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than semiannually, submit a report on the activities of such officers—

(A)(i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;

(ii) to the head of such department, agency, or element; and

(iii) to the Privacy and Civil Liberties Oversight Board; and

(B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) Contents –

Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including—

[1] 42 U.S.C. § 2000ee-1(f).

(A) information on the number and types of reviews undertaken;

(B) the type of advice provided and the response given to such advice;

(C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and

(D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer."

3. Department and Operating Division Privacy Programs

3.1 HHS Senior Official for Privacy (SAOP) and the Office of Privacy & Information Management (PIM)

At HHS, the Chief Information Officer serves as the Senior Agency Official for Privacy (SAOP). The HHS SAOP is responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks consistent with the agency's mission.

The HHS Office of Privacy & Information Management (PIM), housed within the Office of the Chief Information Officer (OCIO), includes the Department and Office of the Secretary-level (OS) Privacy, Records Management, and Paperwork Reduction Act (PRA) functions. The Deputy Director of PIM manages PIM operations. OS has its own Senior Official for Privacy (SOP), and the OS privacy office operates independently within and under the guidance of PIM.

Within PIM's Privacy function, there are two distinct work streams: (1) Compliance and (2) Policy and Strategy. Compliance encompasses a broad range of activities including Privacy Impact Assessments (PIA), breach response, Federal Information Security Modernization Act (FISMA) reporting, website privacy, High Value Assets, and other ad hoc tasks related to system privacy. PIM Compliance reviews and approves all HHS PIAs and reviews HHS breaches prior to closure. PIM Policy and Strategy focuses on developing HHS privacy policy, including policies related to federal mandates and initiatives, and broader strategic initiatives, including privacy continuous monitoring efforts, as well as leading outreach events. Additionally, both the Compliance and Policy and Strategy work streams develop training and awareness materials.

HHS also has the following outward-facing privacy regulatory components:

3.1.1 Office for Civil Rights (OCR)

OCR is the Department's civil rights and health privacy rights law enforcement agency. OCR enforces federal civil rights laws; conscience and religious freedom laws; the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules; and the Patient Safety Act and Rule, which together protect the nation's fundamental rights of nondiscrimination, conscience, religious freedom, and health information privacy.

3.1.2 Office of the National Coordinator (ONC)

The Office of the Chief Privacy Officer within ONC is responsible for: (1) advising the National Coordinator, the Secretary, or other HHS leadership when indicated on privacy, security, and data stewardship of electronic health information; (2) overseeing privacy and security of the consumer use of electronic personal health information; and (3) coordinating ONC efforts with equivalent privacy officers in other federal, state and regional agencies, and foreign nations with regard to the privacy, security, and data stewardship of electronic individually identifiable health information.

3.2 Additional HHS Privacy Components

HHS has eleven Operating Divisions (OpDivs),[2] which administer a wide variety of health and human services and conduct life-saving activities for the nation, protecting and serving all Americans. Each OpDiv maintains its own privacy program, led by an SOP, to manage the implementation of privacy requirements within its organization. PIM collaborates closely with OpDiv privacy programs to ensure the effective implementation of federal and HHS privacy requirements; assist with emerging privacy issues; and facilitate the sharing of information and best practices among OpDivs. Additionally, PIM leads the Privacy Compliance Working Group, a venue for sharing information and resources, made up of representatives from the OpDivs and Department stakeholders.

The following OpDivs provided program descriptions for the reporting period:

Administration for Children and Families (ACF)

The Administration for Children and Families (ACF) privacy office resides within ACF Office of the Chief Information Officer (OCIO). The team consists of the SOP, a privacy manager, and two team members.

[2] HHS OpDivs include: Administration for Children and Families (ACF); Administration for Community Living (ACL); Agency for Healthcare Research and Quality (AHRQ); Agency for Toxic Substances and Disease Registry (ATSDR); Centers for Disease Control and Prevention (CDC); Centers for Medicare & Medicaid Services (CMS); Food and Drug Administration (FDA); Health Resources and Services Administration (HRSA); Indian Health Service (IHS); National Institutes of Health (NIH); and the Substance Abuse and Mental Health Services Administration (SAMHSA).

The primary activities carried out by these assigned resources include managing the ACF Incident Response Team (IRT) and serving as subject matter experts on the team by evaluating and responding to privacy incidents and complaints. The ACF Incident Response policy requires ACF personnel to report not only security incidents but any suspected or confirmed privacy incidents to their supervisor and the ACF IRT. As appropriate, the privacy team develops corrective action plans to remediate privacy concerns, which most often involves retaking training or a review of policies and procedures. The ACF privacy office also develops procedural guides/standard operating procedures (e.g. how to encrypt an email) to assist ACF personnel in practicing better privacy and security practices. All ACF privacy incidents and complaints are also reported to the HHS Computer and Security Incident Response Center (CSIRC). The ACF IRT and SOP are responsible for coordinating with HHS to ensure that law enforcement, Office of the Inspectors General (OIG), and Office of the General Counsel (OGC) receive report of the incident in a timely manner.

The ACF privacy office is also responsible for conducting privacy threshold analyses (PTA) and PIAs, updating system of record notices (SORNs) as applicable, and audit support for FISMA and the Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management Internal Control*. The ACF privacy office's engagement with PIM usually consists of communication related to closing out incidents and completing PIAs.

Agency for Healthcare Research and Quality (AHRQ)

The office of the Agency for Healthcare Research and Quality (AHRQ) SOP is located within the AHRQ Information Security and Privacy Program within the Division of Information Technology (DIT). The AHRQ Information Security and Privacy Program strives to provide the secure, private environment necessary to support the enhancement of healthcare safety and quality. The SOP coordinates with the AHRQ Privacy Act Officer, the AHRQ Records Manager, and system and information owners to ensure that privacy policy is implemented and enforced within AHRQ systems and applications. General activities include implementing privacy policy, ensuring compliance with federal privacy law and guidance, completing and reviewing PIAs, and assessing the applicability of Privacy Act SORNs for information collections. The SOP also reviews new systems and applications to determine what privacy controls are required for the protection of information collection and use. In these roles the AHRQ SOP coordinates with the HHS Privacy Act Officer and PIM for interpretations of Privacy Act applicability and PIA approval, respectively. The SOP also attends monthly HHS Privacy Compliance Monthly Working Group meetings.

Centers for Disease Control and Prevention (CDC)

The CDC Privacy Unit is organizationally located under the CDC Office of the Chief Information Officer (OCIO) and within the CDC Office of the Chief Information Security Officer (OCISO). The Privacy Unit is led by the SOP (aka Chief Privacy Officer), and the staff includes the Associate Chief Privacy Officer, two Privacy/IT analysts, and two Government Information/Data Specialists. The Privacy Unit oversees privacy compliance for all of the CDC Centers/Institutes/Offices.

The CDC Privacy Program is broken into four functional areas: Privacy Policy and Compliance Management, Privacy Training and Awareness, Privacy Breach Response, and Privacy Act Compliance.

The general services provided by the CDC Privacy Unit include: PIAs and PTAs, SORNs, privacy incident response, Privacy Act reviews for contracts, Privacy Act requests, regulatory reviews for privacy impact, privacy policy, web policy review, and privacy outreach.

Centers for Medicare & Medicaid Services (CMS)

The Centers for Medicare & Medicaid Services (CMS) Acting SOP resides in the Office of Information Technology's (OIT) Information Security and Privacy Group (ISPG) and is the director of the Division of Security, Privacy Policy and Governance (DSPPG). The OpDiv SOP works closely with the PIM Deputy Director. All CMS PIAs are submitted through CMS' SOP to PIM for review and approval. There were no changes made to the privacy office during this reporting period. As a covered entity subject to HIPAA Privacy and Security regulations, as well as a federal agency subject to the Privacy Act, the CMS SOP is responsible for the following:

- Developing, implementing, and disseminating OpDiv-wide information privacy policies, procedures, and standards for the information and information systems that support the operations and assets of CMS, including those provided or managed by other agencies, contractors, or other source;
- Administering and implementing the Privacy Act of 1974 through the development, publication, and maintenance of SORNs and Computer Matching Agreements (CMAs);
- Developing and administering Information Exchange Agreements (IEAs) and PIAs;
- Reviewing privacy notices annually including Medicare's Notice of Privacy Practices, CMS' website privacy policy, SORNs, and Privacy Act statements;
- Providing leadership in the development of CMS privacy policy, including development of regulations and sub-regulatory policy and operations guidance;
- Reviewing all legislation and regulations for privacy implications to ensure that enterprise development complies with privacy requirements;
- Providing CMS senior leadership and information technology (IT) governance boards with pertinent privacy requirements for new and ongoing IT investments/projects to ensure informed decision making;
- Serving on the CMS Privacy Board, providing staff support to the National Committee for Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality, and Security; and participating on HHS committees;
- Facilitating monthly data guardian meetings to ensure cyber hygiene enterprise wide; and
- Evaluating risk for privacy breach and incident response and preparing breach notifications as needed.

Food and Drug Administration (FDA)

The FDA Privacy Office is a single centralized office consisting of four full-time employees (SOP and Privacy Act Officer/Chief Privacy Officer, Privacy Coordinator, and two Privacy Analysts), as well as three to five contractors supporting privacy program activities.

During the reporting period, FDA filled vacant Privacy Analyst positions – which were vacant for much of 2018 – and elevated the positions from GS 11/12 to GS 12/13. Additionally, as part of a broader reorganization, in March 2019 FDA's Privacy Program was shifted to a new organization that also includes privacy partners such FDA's Paperwork Reduction Act and Records Management Programs.

The roles and responsibilities of the Privacy Office include the following: FDA compliance with the E-Government Act and FISMA, including administering the execution of PTAs/PIAs for IT systems and information collections, third-party website and applications, and mobile applications developed by or on behalf of the FDA; enterprise performance life cycle (EPLC) stage/project, program technology request, and mobile technology request approvals; directing and developing FDA privacy policy; overseeing and coordinating agency responses to privacy breaches; privacy training and awareness; reviewing FDA PRA Information Collection Requests (ICR) prior to submission to OMB; FDA compliance with the Privacy Act of 1974, including processing FDA Privacy Act requests and drafting and updating SORNs; reviewing IT and information-related acquisitions; responding to privacy-related reporting requirements and data calls; administering internal councils and working groups, including the FDA Privacy Council and FDA Precision Medicine Initiative (PMI) Working Group; and serving as a point of contact for HHS, OMB, and other agencies for privacy matters.

The FDA Privacy Office engages with PIM in all privacy areas indicated above and provides review/comment input to HHS on draft policies, procedures, legislative comments, Department-level ad hoc working groups, HHS Privacy Compliance Working Group, HHS Privacy Committee, and the HHS Privacy Act Officer functions.

Health Resources and Services Administration (HRSA)

The HRSA Chief Information Security Officer also serves as the HRSA SOP. A member of his team serves as Privacy Officer. Coverage includes PIAs, privacy incidents, and privacy awareness training. HRSA's engagement with PIM includes PIA reviews, privacy incidents, and the Privacy Compliance Working Group Monthly meeting.

The HRSA Privacy Act Officer resides in the HRSA Office of Planning, Analysis and Evaluation. Specific coverage includes the Privacy Act, Routine Uses, SORNs and OMB clearance. The HRSA Privacy Act Officer engages with the HHS Department-level privacy staff to conduct SORN reviews and participate in HHS Privacy Committee Meetings.

The HRSA Privacy Officer and Privacy Act Officer collaborate on a regular basis.

National Institutes of Health (NIH)

The NIH Privacy Program is under the direction of the NIH SOP within the Office of the Senior Official for Privacy (OSOP), Division of Management Support, Office of Management Assessment, Office of Management, Office of the Director, NIH. The OSOP collaborates with the NIH OCIO, Office of General Counsel and other key stakeholders (i.e., Information System Security Officers, System Owners/Managers, Record Liaisons, Risk

Management Officers, OMB Project Clearance Liaisons, Web Managers, Communication Directors, and Training Coordinators) to ensure the highest level of scientific integrity, public accountability, and social responsibility in the area of privacy management. NIH Institute and Center (IC) Privacy Coordinators serve as the liaisons between staff and the OSOP on general privacy issues that affect their respective IC. The Privacy Program's mission is supported through the development of privacy policy and privacy awareness training; management of PIAs for information technology systems and third-party websites and applications; communication of emerging areas of privacy compliance; processing requests for records under the Privacy Act; support of annual report submissions and audit responses to OMB, HHS, Congress, and the Government Accountability Office; and support of privacy-related breach response reporting.

Office of the Secretary (OS)

OS is an independent functioning OpDiv that resides within HHS. Although OS must adhere to all HHS privacy and data security policies, the OS Privacy and Data Protection Division functions separately and follows the OS Privacy Program framework, processes, and procedures. The OS Privacy and Data Protection Division's general activities include: privacy policy and compliance management, privacy risk management and data protection, privacy training and awareness, and privacy breach response. OS Privacy resides within PIM.

Substance Abuse and Mental Health Services Administration (SAMHSA)

There are two main privacy contacts within the SAMHSA Security Office: the SOP and a Privacy Officer. The SOP's responsibilities include reporting to the HHS CISO on the effectiveness of the SAMHSA's information privacy program, including progress of remedial actions for corrections (if any); managing internal privacy reviews of the SAMHSA's business cases, alternatives analyses, and other specific investment documents; obtaining contractual assurances from third parties to ensure that the third party will protect personally identifiable information (PII) in a manner consistent with the privacy practices of the Department and applicable laws before enabling access to PII; and ensuring that all employees and contractors comply with SAMHSA's privacy practices and applicable laws. Additionally, the SOP is responsible for establishing a framework to facilitate the development and maintenance of PIAs for all systems; managing and certifying an inventory of all current and proposed investments that contain a privacy control component; coordinating privacy reporting activities as mandated by federal privacy legislation and OMB guidance; and supporting general privacy awareness and role-based training activities for all personnel using, operating, supervising, or managing information technology (IT) systems.

The Privacy Officer is responsible for serving as a point of contact for issues related to the Privacy Act of 1974 within SAMHSA; maintaining awareness of privacy laws, regulations, and issues within SAMHSA; maintaining a SAMHSA SORN website to post current SORNs per HHS Privacy Act Officer guidance; and supporting the SAMHSA SOP and SAMHSA CISO in completing required reviews, as defined by OMB Circular A-130, *Managing Information as a Strategic Resource.*

4. HHS Privacy Reviews

HHS conducts privacy reviews of information systems and programs to ensure that privacy issues are identified and analyzed in accordance with federal privacy laws such as the Privacy Act of 1974, 5 U.S.C. § 552a (2012); the privacy provisions of the E-Government Act of 2002, 44 U.S.C. § 3501 (2012); and federal privacy policies set forth in OMB guidance.

4.1 Privacy Impact Assessments

The PIA process is one of the Department's key mechanisms to ensure that HHS programs and technologies sustain, and do not erode, privacy protections. The PIA process also ensures that the Department considers and mitigates privacy risks early in system development and throughout the system life cycle.

During the reporting period, the Department SAOP signed 409 PIAs and 12 Third Party Websites and Applications (TPWA) PIAs. PIAs are available at https://www.hhs.gov/pia/.

The following OpDivs provided narrative descriptions of PIAs that cited privacy concerns or sensitivities during the reporting period:

Administration for Children and Families (ACF)

The Refugee Arrivals Data System (RADS) PIA was approved on May 7, 2019 and describes a system that collects and stores information on asylees, refugees, entrants, and other populations received from government agencies, case management agencies, and volunteer agencies (VOLAGs). The system uses this information to provide reports to the Office of Refugees and Resettlement (ORR) leadership and Congress. The system is covered by SORN (09-80-0325) which inherently requires additional controls to help protect those individuals described in the SORN. Per the Privacy Act of 1974, agencies must keep a record of the date, nature, and purpose of each disclosure of a record to any person or to another agency.

Centers for Medicare & Medicaid Services (CMS)

CMS created the Comprised Number Checklist (CNC) as an efficient and accurate system for identifying, tracking, and implementing edits to prevent Medicare Fraud, Waste and Abuse (FWA). CMS created a database/compilation of these numbers that allows designated Medicare direct contractors to routinely obtain access to the numbers and to share any associated corrective actions they may have taken. PII is collected for investigative purposes. The PII of Beneficiaries or Providers is used to carry out investigations. For example, the address of a Provider who has been identified as a Medicare Perpetrator in the CNC system can be used to determine their exact location of operation or even as a lead to their address of operation. Access to the systems is given based on 'need to know' and job responsibilities. Systems grant or deny access to data based upon 'need to know' roles. External audits also verify these controls. Technical controls used include user identification, passwords, security tokens, firewalls, virtual private networks,

and intrusion detection systems. Physical controls used include guards, identification badges, key cards, cipher locks, and closed circuit televisions.

Food and Drug Administration (FDA)

FDA Center for Tobacco Products (CTP) Research and Evaluation of the Public Education Campaign on Tobacco (RESPECT) among Lesbian, Gay, Bisexual, and Transgender (LGBT) is a study that conducts research and evaluation of tobacco public education campaigns targeted at a vulnerable population, extending privacy protection to this population. The purpose of the study is to evaluate the "This Free Life" tobacco public education campaign being conducted by CTP in support of its mandate to positively impact public health by reducing and preventing tobacco use. The "This Free Life" campaign targets LGBT young adults between the ages of 18 and 24 who are occasional tobacco users. This is a cross-sectional study with an embedded longitudinal cohort consisting of seven waves of data collection: a baseline wave and six follow-up waves. An average of 3,461 young adults complete outcome evaluation questionnaires at each wave.

4.2 System of Records Notices

The Department publishes System of Records Notices (SORN) consistent with the requirements outlined in the Privacy Act of 1974. During the reporting period, the Department published five SORNs (five new, zero revised). There were no SORNs implicating privacy concerns which identified particularly significant privacy risks or mitigations. All HHS SORNs are available at https://www.hhs.gov/foia/privacy/sorns/index.html.

5. Complaints

As required by Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, as amended, the HHS is required to provide semi-annual reports to Congress with the number and nature of the complaints received by the Department for alleged violations, and a summary of the disposition of such complaints, when available. For purposes of the Section 803 Report for this reporting period, HHS considers privacy complaints to include breaches of PII.

5.1 HHS Privacy and Incident Response Team (PIRT)

HHS handles significant amounts of PII—information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual—in the course of carrying out its mission. When privacy and security controls break down, PII can be compromised, potentially resulting in harm to individuals and the Department. The principal purpose of the HHS PIRT is to convene members in response to a suspected or confirmed breach of PII; engage in a risk analysis to determine if the breach poses problems related to identity theft or any applicable federal laws and policies, and, if so, identify the level of such risk; and tailor the Department's response to the nature and scope of the risk presented, as appropriate. The HHS PIRT also engages in advanced planning to refine and improve the Department's response to the potential loss of control of PII. The PIRT, led by the SAOP, is composed of stakeholders from across the Department.

During the reporting period, the two most common types of reported privacy breaches were documents mailed to the wrong address and unintended electronic disclosures. Pertinent narrative examples are set forth below.

Example: Documents Mailed to the Wrong Address

An HHS office mistakenly sent a case file to an administrative qualified independent contractor, an unintended recipient. The case file contained three individuals' medical records, home addresses, Health Insurance Claim Numbers, and phone numbers. The unintended recipient returned the case file. HHS reviewed current policies and procedures to prevent these types of breaches from reoccurring and concluded that there was a low risk of the breached information being used impermissibly. The employees responsible completed HHS Cybersecurity Awareness Training and Records Management Training, and received an individualized counseling session from their OpDiv privacy office. The HHS PIRT reviewed and closed the incident.

Example: Unintended Electronic Disclosure

An HHS employee sent an unencrypted email containing two patients' PII to his or her supervisor, an intended recipient. The types of PII included in the email were names, dates of birth, medication names, work addresses, phone numbers, and names of hospitals where treatments were administered. The OpDiv's IT office performed a scrub of the email server to

ensure all copies of the unencrypted email were deleted. The employee was then retrained on proper PII handling procedures. The HHS PIRT reviewed and closed the incident.

The following OpDivs provided descriptions of complaints that their OpDiv received from individuals alleging that HHS violated their privacy during the reporting period:

Centers for Medicare & Medicaid Services (CMS)

The CMS Privacy Office has not received any complaints from individuals alleging that HHS has violated their privacy. The CMS Information Security & Privacy Group receives inquiries from individuals regarding privacy questions, concerns, and requests, and provides answers or referrals to the appropriate contacts for addressing these questions, concerns, and requests. However, during the specified reporting period, none of the questions, concerns, or requests received alleged that an individual's privacy was violated.

During the reporting period, CMS received two requests from individuals for Medicare to facilitate opting out of third-party solicitations from non-government service providers. These requests were resolved by informing the requestors that Medicare does not currently have a process for facilitating an opt-out from third party solicitations, that Medicare does not provide prospective beneficiary lists to third parties, and by referring the requestors to the Medicare help desk for further information.

Food and Drug Administration (FDA)

FDA received two privacy complaints during the reporting period.

The first concerned an employee of a regulated entity, who contacted FDA Privacy to discuss concerns about his anonymity/confidentiality and FDA's potential disclosure of identifying information to an alleged corporate wrongdoer. FDA's SOP spoke to the individual by phone and reviewed email from the individual. In response to questions, the SOP described the protections that are applied to identifying information and the restrictions against disclosure, e.g., review and redaction of record content by FDA disclosure officials and experts before records are released. The individual expressed no further concerns, and to support FDA efforts he provided his contact information to FDA officials involved in the relevant disclosure process.

The second complaint involved an FDA employee, who contacted the FDA SOP with concerns about internal PII sharing and PII duplication/storage. The SOP provided guidance to the individual about appropriate PII use and related HHS/FDA policies, advised the individual of avenues to report policy violations, and offered to meet with program management and/or provide training to the individual's office/organization. The individual has made no further reports or contacts with FDA Privacy.

6. Notable Department-level Updates

6.1 Advice

PIM provides significant, ongoing privacy leadership on a wide range of topics. Advice provided includes written issuance of policies, procedures, or guidance pertaining to privacy.

6.1.1 Existing Privacy Policies, Procedures, and Guidance

A list of HHS OCIO information security and privacy policies, standards, memoranda, and guidance is currently available on the HHS intranet. Information Security and Privacy Program resources are also available at http://www.hhs.gov/ocio/securityprivacy/. Additional HHS OCIO Policies, Standards, and Charters are available at https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/index.html.

6.1.2 Policies, Procedures, and Guidance Updated During the Reporting Period

- Revised and republished the *HHS Policy for Privacy Impact Assessments (PIA)*
- Drafted the *HHS Policy for Social Security Number (SSN) Reduction and Elimination*
- Drafted the *HHS Policy for the Use of Personally Identifiable Information for Testing, Training, and Research*
- Updated the HHS Privacy Program Plan in accordance with OMB Circular A-130, *Managing Information as a Strategic Resource*, which provides an overview of HHS's privacy program, including goals and objectives, structure and resources, privacy requirements, and roles and responsibilities
- Updated the *PIM Policy Glossary*

6.1.3 Leadership and Engagement During the Reporting Period

- PIM helped coordinate a number of strategic activities, including:
    - conducting inventories of PIAs, SORNs, and DLP tools;
    - enhancing the Department's privacy, security, and records management training programs and offerings;
    - analyzing OpDiv and Staff Division (StaffDiv) privacy programs and any actions OpDivs and StaffDivs are taking to strengthen their privacy programs;
    - incorporating National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Appendix J privacy controls into the enterprise-wide Assessment & Authorization (A&A) process, through RSA Archer;

    - leading implementation of RSA Archer privacy modules (e.g., A&A (PIA), and breach response); and
    - reviewing and revising as necessary the *HHS Privacy Program Plan* and *HHS Privacy Continuous Monitoring (PCM) Strategy*.
- The PIM Deputy Director chaired the HHS Privacy Compliance Working Group.
- PIM led the HHS Precision Medicine Initiative Privacy and Security Working Group.

6.2 Department-level Privacy Training and Awareness

6.2.1 Mandatory Training

HHS personnel completed a mandatory security and privacy awareness training course called Cybersecurity Awareness Training. The course is required for all personnel when they join the Department, and annually thereafter. HHS ensures that all Department employees and contractors receive annual information security awareness training, privacy awareness training, and role-based training in compliance with OMB Circular A-130, FISMA, and National Institute of Standards and Technology (NIST) guidance. The Cybersecurity Awareness Training course identifies important guidelines that define the sensitivity levels of information, including information residing on national security systems and PII, and the role a user plays in protecting this information. Also explained are the threats associated with identity theft, social engineering, phishing, spyware, and the insider threat. This course provides computer security tips and practices that may be used at work and at home.

Additionally, all employees and contractors with access to HHS information systems are required to sign the HHS Rules of Behavior annually. The Rules of Behavior informs employees and contractors of their privacy requirements for using HHS information systems and the consequences of violating those requirements.

6.2.2 Classroom Training

PIM staff led a privacy-specific training with the Cybersecurity team entitled “Privacy Requirements Awareness Training for Information and Information Technology Procurements” to assist the HHS acquisitions community in the implementation of standard security and privacy contract language.

6.2.3 Additional Trainings Offered

A number of role-based trainings—including for personnel with significant security responsibilities, executives, managers, IT administrators, SOPs, and Authorizing Officials—are available to HHS employees and contractors. Network accounts are disabled for personnel who fail to satisfy this requirement by the deadline. Examples of available role-based trainings include:

- Senior Officials for Privacy (SOP) Roles & Responsibilities Training

- Authorizing Official/Authorizing Official Designated Representative Roles and Responsibilities Training
- PII Handler Framework

Topic-based trainings—including trainings on email encryption, PII Handler framework, specialized PII training, and third-party websites and applications—are available to HHS personnel. Examples of available topic-based trainings include:

- Privacy Awareness Training
- PIA Training
- TPWA PIA Training
- Mobile Applications Privacy Training
- Sensitive PII Training
- Email Encryption Course

6.3 External Privacy Reporting

PIM also develops content and compiles OpDiv responses for the annual SAOP FISMA report. The report includes information about HHS's privacy program and activities and compliance with federal requirements, including PIAs and SORNs.

6.4 Outreach

- PIM distributed an agency-wide email commemorating International Data Privacy Day (January 28, 2019).
- The Deputy Director of PIM presented the "HHS Privacy Incident Response Team Annual Report to the HHS Risk Management and Financial Oversight Board" (June 24, 2019).
- PIM staff participated on the Federal Privacy Summit Committee, including the planning, development, and execution of the annual federal-wide privacy conference.

7. HHS OpDiv-level Advice, Training, and Outreach Activities

The Department requested input from HHS OpDivs about their privacy activities during the January 1, 2019 to June 30, 2019 reporting period. Activities include advice provided, training and awareness initiatives, and outreach activities. Responses to this inquiry are summarized below:

7.1 Administration for Children and Families (ACF)

Advice provided by ACF: During the reporting period, ACF has provided comment to the Department on the following policies which pertain to privacy:

- HHS Policy for Mobile Devices and Removable Media
- HHS Social Security Number (SSN) Reduction and Elimination Policy

Training and Awareness provided by ACF: The ACF privacy team developed and provided a classroom-style privacy training, specifically around safeguarding PII, for ACF employees. This training was provided routinely to ACF Headquarters personnel from October 2018 to June 2019. Personnel included Federal staff, direct contractors, and third-party contractors. A second version has been created to provide training online with narration and built-in checkpoints. OCIO is now working to confirm the process for tracking completion and disseminating the training to the remaining personnel. Scheduled timeline for dissemination is by end of CY19.

Outreach Activities: The ACF privacy team created and disseminated (2/15/19) the "ACF Security and Privacy Tips", a quick desk reference intended for ACF personnel to print and keep handy in their workspaces. The guide sheet includes tips such as identifying phishing email red-flags, a how-to for encrypting emails and reporting incidents, and password do's and don'ts.

7.2 Agency for Healthcare Research and Quality (AHRQ)

Advice provided by AHRQ: AHRQ documents privacy policies in the *AHRQ Management Operations Manual (MOM).*

Training and Awareness provided by AHRQ: AHRQ provides role-based training, Security and Privacy Awareness training, and Records Management training annually.

Outreach Activities carried out by AHRQ: AHRQ publishes a Tip of the Week that includes security and privacy tips on a wide variety of topics. AHRQ also participates in the HHS Privacy Compliance Working Group and the monthly HHS Privacy Committee meeting. Members of the AHRQ Information Security and Privacy Program are Certified Information Privacy Professionals (CIPP) and attend the annual International Association of Privacy Professionals (IAPP) conference and KnowledgeNet learning sessions.

7.3 Centers for Disease Control and Prevention (CDC)

Advice provided by CDC: N/A

Training and Awareness provided by CDC:

- Mandatory computer-assisted (along with three live sessions) Security and Privacy Awareness training course. This course is required for all personnel when they join CDC, and at least annually thereafter.
- Role-based continuing education training for Information System Security Officers.
- Quarterly privacy trainings: The CDC Privacy Office periodically trains program personnel in compliance best practices, including how to draft PTAs and PIAs.

Outreach Activities carried out by CDC:

- The CDC Privacy Office held privacy briefings for specific programs. Upon request or as needed, the Privacy Office provides customized PIA/PTA briefings to ensure adequate PIAs/PTAs are submitted and to convey the importance of incorporating privacy protections into any new program or system that will collect PII.
- CDC Privacy continued to ensure that CDC leadership, program managers, and system owners are aware of their responsibilities for protecting PII within the context of their position duties through the development and implementation of specialized training for these individuals. Topics of specialized training included information sharing/disclosure, privacy incidents, PIAs/PTAs, and privacy compliance.

7.4 Centers for Medicare & Medicaid Services (CMS)

Advice provided by CMS:

- Update to the CMS Information Systems Security and Privacy Policy (IS2P2) Publication: The CMS IS2P2 defines the framework under which CMS protects and controls access to CMS information and information systems.
- Acceptable Risk Safeguards (ARS) 3.1 Frequently Asked Questions (FAQ): The ARS 3.1 FAQ provides frequently asked questions and answers on the CMS ARS. The ARS provides guidance to CMS and its contractors as to the minimum acceptable level of required security and privacy controls that must be implemented by CMS and CMS contractors to protect CMS' information and information systems, including CMS Sensitive Information.
- CMS PIA Standard Operating Procedure: The CMS PIA Standard Operating Procedure is CMS' detailed guidance for conducting PIA development and maintenance.

Training & Awareness provided by CMS:

- CMS Information Systems Security and Privacy Awareness (ISSPA) Training: This mandatory annual training includes training modules addressing privacy topics, issues, and protections.
- Beneficiary Data Protection Initiative, including monthly Data Guardian meetings and phishing exercises.

- Role Based Training (RBT) is made available through CMS Privacy's Computer Based Training (CBT) website, based on National Initiative for Cybersecurity Education (NICE) role ID assignments.
- Cyberworks: Cyberworks is the CMS Annual Cybersecurity and Privacy Training day. Cybersecurity and privacy professionals from both government and the private sector meet to discuss cybersecurity and privacy priorities, trends, and improvements.
- New Employee Orientation (NEO): NEO instructor-led training includes lessons on privacy topics including PII and Protected Health Information (PHI).
- Information Security & Privacy Catalog: On-line, on-demand training resources include:
  - Your Role in Privacy at CMS
  - Incident Response at CMS
  - CMS Privacy Incident Response: Quick Guide for Business Owners

Outreach Activities carried out by CMS:

- Information System Security Officer (ISSO) Journal Articles on Privacy
- ISSO Forum
- Cyberworks
- Monthly Data Guardian Meetings

7.5 Food and Drug Administration (FDA)

Advice provided by FDA: The FDA Privacy Office did not have occasion to provide advice regarding counterterrorism efforts. The unique regulatory and public health role of the agency does not entail a focus on counterterrorism. The Privacy Office did provide guidance and comments on the following HHS policies pertaining to privacy:

- HHS Policy for Privacy Impact Assessments (PIA) (March 2019)
- HHS Social Security Number (SSN) Reduction and Elimination Policy (June 2019)
- HHS Rules of Behavior for Use of HHS Information and IT Resources Policy (June 2019)
- HHS Plan of Action and Milestones (POAMs) (June 2019)

Guidance to employee/s:

- Information sharing general security practices for drug applications (June 2019)

Training and Awareness provided by FDA: The FDA Privacy Office provides in-person privacy training at the agency's New Employee Orientation (NEO); classes of new hires are onboarded twice a month. FDA Privacy also conducted training sessions on privacy topics for individual FDA offices and divisions. In March and June 2019, organization-specific privacy awareness communications were provided during tax and summer travel seasons on how to protect personally identifiable information (PII).

In May 2019, staff members attended the IAPP Global Summit, which includes training and Continuing Privacy Education (CPE) credits towards privacy certifications.

Outreach Activities carried out by FDA: FDA Privacy staff attended and administered the following meetings and other outreach activities:

- HHS Privacy Committee Meetings
- HHS Privacy Compliance Working Group Meetings
- FDA Privacy Council
- FDA Mobile Applications Privacy Policy Working Group
- Q&A sessions on selected privacy topics
- Management/leadership advisory briefings

7.6 Health Resources and Services Administration (HRSA)

Advice provided by HRSA: N/A

Training and Awareness provided by HRSA:

- The HHS-provided Cybersecurity Awareness Training and Rules of Behavior (required prior to receiving access to HRSA information systems and annually thereafter) contains submodules that include privacy-related information, including information related to safeguarding PII, identifying and reporting suspected and confirmed privacy incidents, and privacy best practices.
- PII specific training for staff involved in PII-related incidents.

Outreach Activities carried out by HRSA:

- Maintained the HRSA Guide to Identifying and Handling Sensitive Information including PII.
- Developed and distributed a pamphlet on how to encrypt sensitive data in emails.
- Developed and leverage for training purposes a video for identifying and emailing sensitive information.
- Some of HRSAs Phishing Awareness campaigns throughout each year are targeted toward the protection of sensitive information.

7.7 National Institutes of Health (NIH)

Advice provided by NIH: N/A

Training and Awareness provided by NIH: NIH OSOP coordinated with the NIH CISO to ensure adequate and appropriate privacy awareness and annual refresher training were provided to NIH employees, contractors, and all other personnel using NIH information systems. Additional trainings included Privacy Coordinator Training on PIA/PTA Tips and Tricks and one-on-one training for Privacy Coordinators, CIO, and stakeholders.

Outreach Activities carried out by NIH: NIH OSOP communicated privacy information to NIH staff via the NIH Privacy Listserv and Institute/Center Privacy Coordinator distribution list. NIH OSOP also developed and disseminated a Privacy Coordinator Brochure and HHS PIA “Tips and

Tricks" handout. NIH OSOP also hosted monthly meetings with privacy staff to communicate evolving privacy requirements.

7.8 Office of the Secretary (OS)

Advice provided by OS: N/A

Training and Awareness provided by OS: OS Privacy provides one-on-one training as a result of a privacy breach, one-on-one PIA training, and privacy best practices training.

In addition, OS Privacy employees attended the following trainings:

- Cybersecurity and Privacy Awareness Training
- HHS Rules of Behavior
- Contracting Officer's Representative Refresher
- IT Audit, Internal Controls, and Risk Management Workshop
- NIST Privacy Framework Workshop
- Archer Security Operations (SecOps) Training
- IAPP Privacy Summit
- Management Concepts Briefing and Presentation training (three-day)
- CIPP/US training (two-day)
- Provided ISSO Privacy Modules Training
- FedStrive: Wellness and Health Promotion

Outreach Activities carried out by OS: N/A

7.9 Substance Abuse and Mental Health Services Administration (SAMHSA)

Advice provided by SAMHSA: N/A

Training and Awareness provided by SAMHSA: New employee security and awareness training, HHS cybersecurity training, and HHS Privacy Compliance Working Group meetings.

Outreach Activities carried out by SAMHSA: Participated in HHS privacy program-wide activities.