Centers for Medicare & Medicaid Services
Information Security and Privacy Group

CMS Information Systems Security and Privacy Policy

Final

Version 2.0

Document Number: CMS-CIO-POL-SEC-2019-0001

May 21, 2019

Record of Changes

This policy supersedes the *CMS Information Systems Security and Privacy Policy v 1.0* , April 26, 2016. This policy consolidates existing laws, regulations, and other drivers of information security and privacy into a single volume and directly integrates the enforcement of information security and privacy through the CMS Chief Information Officer, Chief Information Security Officer, and Senior Official for Privacy.

Version	Date	Author/Owner	Description of Change	CR #
1.0	3/15/2016	FGS – MITRE	Initial Publication	
2.0	05/17/2019	ISPG	Edits addressing the HIPAA Privacy Rule, some Roles and Responsibilities, Role-Based Training/NICE, High Value Assets, and references,	

CR: Change Request

Effective Date/Approval

This policy becomes effective on the date that CMS's Chief Information Officer (CIO) signs it and remains in effect until it is rescinded, modified, or superseded by another policy.

This policy will not be implemented in any recognized bargaining unit until the union has been provided notice of the proposed changes and given an opportunity to fully exercise its representational rights.

Signature: /S/ Date: 05/21/19

Rajiv Uppal
Chief Information Officer

Policy Owner's Review Certification

This document will be reviewed in accordance with the established review schedule located on the CMS website.

Signature: /S/ Date: 05/21/19

George Hoffmann
Acting CMS Chief Information Security Officer

Table of Contents

List of Figures

1. Purpose

The Centers for Medicare & Medicaid Services (CMS) *Information Systems Security and Privacy Policy (IS2P2)*[1] (hereafter "Policy") applies to all users who access CMS information and information systems. As required under the Federal Information Security Modernization Act of 2014 (FISMA), this Policy defines the framework under which CMS protects and controls access to CMS information and information systems. This Policy provides direction to all CMS employees, contractors, and any individual who receives authorization to access CMS information technology (IT) systems; systems maintained on behalf of CMS; and other collections of information to assure the confidentiality, integrity, and availability of CMS information and systems. As the federal agency responsible for administering the Medicare, Medicaid, Children's Health Insurance Program (CHIP), and Health Insurance Marketplace (HIM), CMS collects, creates, uses, discloses, maintains, and stores personal, healthcare, and other sensitive information[2] subject to federal law, regulation, and guidance. This Policy requires all CMS stakeholders, including Business Owners and Information System Security Officers (ISSO), to implement adequate information security and privacy safeguards to protect all CMS sensitive information.

The CMS Chief Information Officer (CIO), the CMS Chief Information Security Officer (CISO), and the CMS Senior Official for Privacy (SOP) jointly develop and maintain this document.

1.1 Authority

The Office of Management and Budget (OMB) designated the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) as authorities to provide guidance to federal agencies for implementing information security and privacy laws and regulations, including FISMA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Privacy Act of 1974 ("Privacy Act"). This Policy addresses CMS applicable information security and privacy requirements arising from federal legislation, mandates, directives, executive orders, and Department of Health and Human Services (HHS) policy by integrating NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, with the *Department of Health and Human Services Information Systems Security and Privacy Policy* (IS2P) and specific programmatic legislation and CMS regulations. Appendix B lists these authoritative references.

In accordance with HHS IS2P Appendix A Section 10.2, the CMS CIO designates the CISO as the CMS authority for implementing the CMS-wide information security program. HHS IS2P

---

1 CMS maintains an Information Security and Privacy Library that contains a comprehensive listing of policy guidance, standards, regulations, laws, and other documentation related to the CMS Information Security and Privacy Program. The library is available at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html.

2 This Policy uses the term "CMS Sensitive Information" as defined in the *Risk Management Handbook (RMH)* Volume I Chapter 10, *CMS Risk Management Terms, Definitions, and Acronyms* (http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_V_I_10_Terms_Defs_Acronyms.pdf) and subject to Executive Order 13556, *Controlled Unclassified Information* (https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information). This definition includes all data that require protection due to the risk and magnitude of loss or harm, such as Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI).

Appendix A Section 15 designates the SOP as the appropriate system authority for implementing the CMS-wide privacy program. Through this Policy, the CIO delegates authority and responsibility to specific organizations and officials within CMS to develop and administer defined aspects of the CMS Information Security and Privacy Program as appropriate. All CMS stakeholders must comply with and support this Policy to ensure compliance with federal requirements and programmatic policies, standards, procedures, and information security and privacy controls.

If a CMS stakeholder is unable to comply with any of the requirements in this Policy, an appropriate authority (Business Owner, Information System Owner [ISO], Division Manager, or other stakeholder) must write a justification for noncompliance, and the CMS CISO or SOP must review this justification and make appropriate recommendations to the CIO for risk acceptance. This risk acceptance is internal to CMS. If, however, the requirement is also a requirement of the HHS IS2P, CMS must provide the documentation of justification and the appropriate HHS form and request the waiver from HHS. Stakeholders must contact their Cyber Risk Advisors for information about the waiver process.

1.2 Scope

This Policy defines the authoritative information security and privacy policies that apply to all CMS centers, components, offices, and programs, as well as all personnel conducting business directly for or on behalf of CMS through contractual relationships.[3] This Policy does not supersede any other applicable law, higher-level agency directive, or existing labor management agreement in place. Any contract, agreement, or other arrangement that collects, creates, uses, discloses, or maintains sensitive information, including but not limited to Personally Identifiable Information (PII) and Protected Health Information (PHI), must comply with this Policy. In some cases, other external agency policies may also apply (e.g., if a system processes, stores, or transmits Federal Tax Information [FTI]).

This Policy does not apply to any network or system that processes, stores, or transmits foreign intelligence or national security information under the cognizance of the Special Assistant to the Secretary (National Security) pursuant to Executive Order (E.O.) 12333, *United States Intelligence Activities*, or subsequent orders. The Special Assistant to the Secretary (National Security) is the point of contact (POC) for issuing IT security and privacy policy and guidance for these systems.

1.3 Policy Structure

The CMS CIO, CISO, and SOP designed this Policy to comply with the NIST Program Management (PM) control family. This Policy integrates information security and privacy roles, responsibilities, and controls into the CMS Information Security and Privacy Program by way of the following structure:

[3] This includes all management, users, information system owners and managers, information owners and stewards, system maintainers and system developers, operators, and administrators, including contractors and third parties, of CMS information systems, facilities, communications networks, and information.

- Section 2 describes the CMS Information Security and Privacy Program.
- Section 3 defines specific information security and privacy responsibilities for relevant stakeholders.
- Section 4 defines CMS's information security and privacy policies, first by HHS- and CMS-specific policies and then by NIST SP 800-53 control families.
- Appendix A presents the acronym terms used in this document.
- Appendix B.1 lists all references in this Policy by order of appearance in the document. Each reference is numbered within brackets [#].
- Appendix B.2 presents by "order of precedence" the authoritative references, statutes, orders, directives, policies, and guidance. Each numbered reference appears in order of authoritative precedence.

The *CMS Acceptable Risk Safeguards* (*ARS*) includes additional, detailed policy traceability statements within each security and privacy control description. The *CMS ARS* provides CMS requirements for all of the detailed information security and privacy controls.

The *Risk Management Handbook* (*RMH*) compiles CMS standards, requirements, directives, practices, and procedures for protecting CMS information and information systems.

CMS updates this Policy at least every three years (36 months). In cases where existing policy is insufficient to address changes in governance (e.g., legislation, directives, mandates, executive orders, or HHS policy) or emerging technology, the CMS CISO or CMS SOP may publish ad hoc or specialized interim policies to address the area of concern. As appropriate, the interim policies may be integrated into future releases of or incorporated as an appendix to this Policy.

2. Information Security and Privacy Program Summary

The CMS CISO and SOP are responsible for managing the Information Security and Privacy Program (henceforth "Program"). This section describes how specific functional areas of the Program help CMS stakeholders apply this Policy to secure and protect CMS information and information systems.

CMS information security and privacy disciplines are now integrated into a single Program. Each discipline has unique requirements. Privacy policies apply to CMS programs and activities at their inception, even before information systems are identified or defined. Business Owners must engage to identify privacy requirements (including the selection of privacy controls), privacy compliance documentation, and privacy contract requirements prior to system acquisition and development.

Privacy policies apply to the collection, creation, use, disclosure retention, and disposal of information that identifies an individual (i.e., PII, including PHI) in electronic or physical form. CMS's responsibility for protecting the privacy interests of individuals applies to all types of information, regardless of its form. All CMS standards, regulations, directives, practices, and procedures must clearly state that all forms of information must be protected.

2.1 Policy and Governance

The policy and governance functional area develops and updates the information security and privacy policies, standards, requirements, directives, practices, and procedures. Responsibilities include developing, implementing, and disseminating this Policy to align with HHS policies, federal legislation, and best practices.

2.2 Risk Management and Compliance

The risk management and compliance functional area oversees Security Assessment and Authorization (SA&A), FISMA reporting, and other external audits. Responsibilities include developing and updating risk management and compliance processes and procedures to align with HHS policies, federal legislation, and best practices.

2.3 Awareness and Training

The awareness and training functional area provides awareness training and role-based training (RBT) for all CMS stakeholders. Responsibilities include developing curriculum, delivering training, tracking training status, and reporting.

2.4 Cyber Threat and Incident Handling

The cyber threat and incident handling functional area supports CMS's cyber threat intelligence, information sharing, and incident handling, including breach response. Responsibilities include developing, updating, and disseminating processes and procedures to coordinate information sharing and incidents across CMS.

2.5 Continuity of Operations

The continuity of operations functional area provides plans and procedures to ensure continuity of operations for information systems that support CMS operations and assets. Responsibilities include developing processes and procedures for system contingency planning, disaster recovery, and participation in federal continuity exercises.

3. Roles and Responsibilities

This section details significant information security and privacy roles and responsibilities for CMS stakeholders. Responsibilities, defined by role rather than position, are derived from the HHS IS2P, RBT requirements, and CMS-specific responsibilities. This section enhances the responsibilities defined within the HHS IS2P to address CMS's needs. Therefore, CMS stakeholders must also refer to the IS2P for additional detail.

A current version of the HHS IS2P may be requested via the HHS FISMA Mailbox at fisma@hhs.gov.

Figure 1, which does not reflect organizational structures, shows the roles grouped by functional area described in this section. Many of the roles are restricted to federal employees and labeled with "Fed" at the lower right corner of the boxes in the figure. Roles that may be filled by either a federal employee or a contractor are labeled with "Mix" at the lower right corner. The subsection that discusses each role is listed at the lower left of each box.

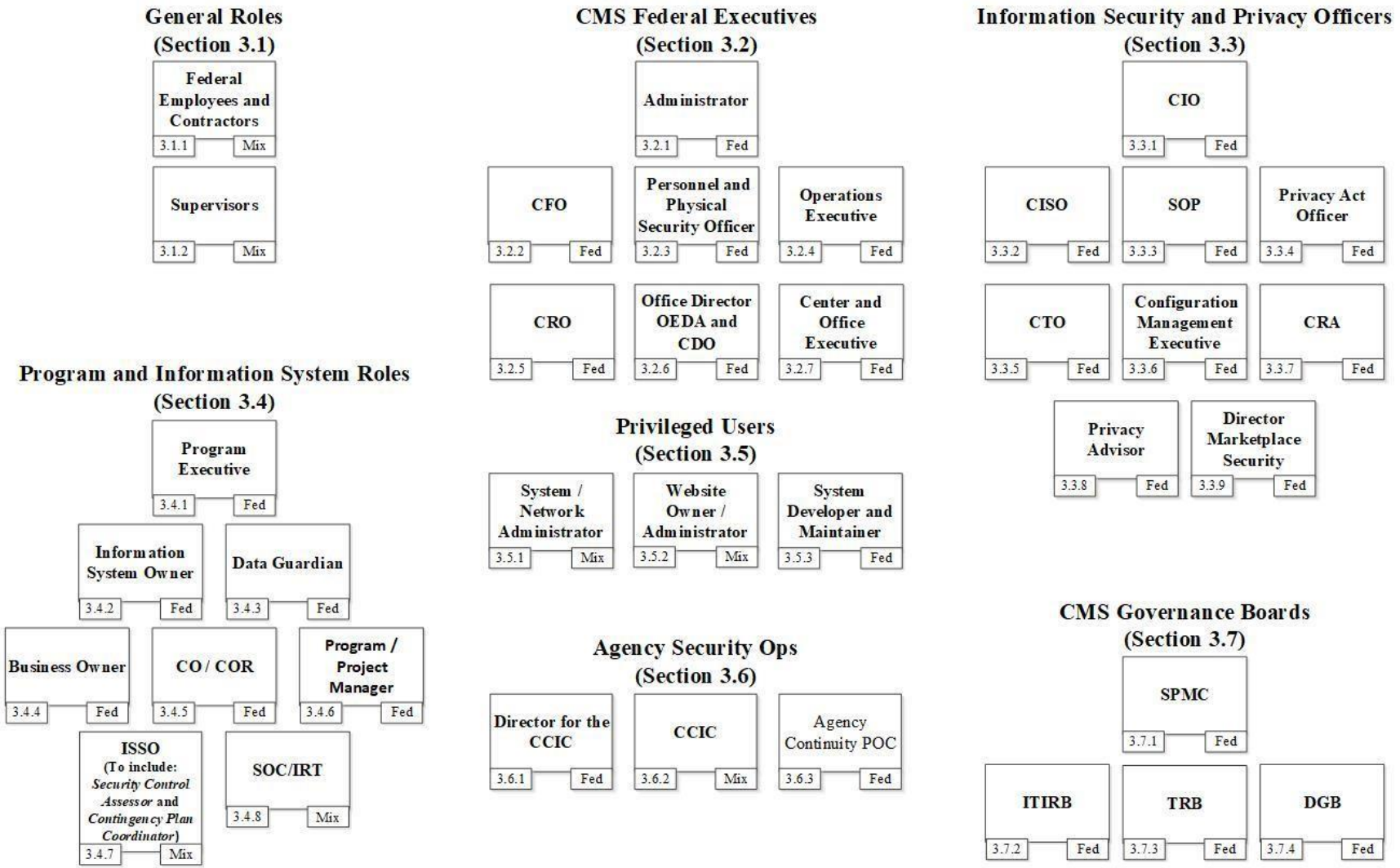

Figure 1. CMSInformation Security and Privacy Roles

3.1 General Roles

All CMS personnel, whether federal employee or contractor (including subcontractors), must adhere to the information security and privacy responsibilities defined within this section. This subsection describes CMS-specific responsibilities for the roles "All Users" and "Supervisors."

3.1.1 Federal Employees and Contractors (All Users)

All CMS federal employees and contractors (including subcontractors) must fulfill all the responsibilities identified in the HHS IS2P, Appendix A Section 31, *All Users*. All users have the responsibility to protect CMS's information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction by complying with the information security and privacy requirements maintained in this Policy.

In addition to the HHS IS2P the responsibilities of the CMS federal employees and contractors must include, but are not limited to, the following:

- Consider all browsing activity private and sensitive [2].
- Notify the CMS CISO and SOP of actual or suspected information security and privacy incidents and breaches, including CMS sensitive data, using procedures specified in the RMH and applicable Rules of Behavior (RoB).
- Complete mandatory security and privacy awareness training before accessing CMS information systems and annually thereafter [3, 4].
- For all newly hired personnel and staff, and those who transfer into a new position with significant security and/or privacy responsibilities, complete specialized security or privacy RBT as appropriate for assigned roles within 60 days of entry on duty or upon assuming new responsibilities. Thereafter, they must complete RBT at least annually.
- For contractors with significant security and/or privacy responsibilities, complete specialized RBT within 60 days of beginning work on a contract. Thereafter, they must complete RBT at least annually.
- Report anomalies when CMS programs, systems, or applications are collecting, creating, using, disclosing, or retaining more than the minimum data necessary. [5, 6]

3.1.2 Supervisors

Supervisors may be federal employees or contractors[4] and must fulfill all responsibilities identified in the HHS IS2P Appendix A Section 30, *Supervisors*.

In addition to the HHS IS2P, the responsibilities of Supervisors include, but are not limited to, the following:

- Notify the appropriate ISSO (or the CMS CISO if the ISSO is not available) within one hour of any unexpected departure or separation of a CMS employee or contractor [7]
- Ensure personnel under their direct report complete all required information security training, including privacy and RBT, within the mandated time [4]

[4] Contractor supervisors must work through the Contracting Officer's Representative to complete the stated responsibilities.

- Ensure background checks are conducted on all individuals identified by system owners with access to CMS information systems in accordance with position sensitivity designation as derived by the use of the appropriate CMS tool

3.2 CMS Federal Executives

This subsection describes the information security and privacy responsibilities of CMS Federal Executives, including the Administrator, Chief Financial Officer (CFO), Personnel and Physical Security Officers (PPSO), and Operations Executive (OE). Only agency officials (federal government employees) are authorized to fill these roles.

3.2.1 Administrator

The Administrator must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 2, *OpDiv Heads,* including "Delegating responsibility and authority for management of HHS Operating Division (OpDiv) IT security and privacy programs to the OpDiv CIOs," and those identified in the *HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)* [8]. These responsibilities include:

- Delegating responsibility and authority for making final decisions regarding external breach notification and issuing written notification to individuals affected by a privacy breach [9, 10]
- Receiving inquiries, investigations, or audits from enforcement authorities, such as any initiated by the HHS Office for Civil Rights related to compliance with HIPAA or the HIPAA Privacy and Security Rules, and coordinating responses with the Chief Information Officer and other appropriate staff.

HHS's Continuity of Operations Program Policy [11] also requires that the Administrator must:

- Incorporate continuity of operations requirements into all CMS activities and operations
- Designate in writing an accountable official as the Agency Continuity Point of Contact, who is directly responsible to the Administrator for management oversight of the CMS continuity program and who is the single point of contact for coordination within CMS for continuity matters.

3.2.2 Chief Financial Officer

The CFO must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 3, *Assistant Secretary for Financial Resources (ASFR)/CFO*.

3.2.3 Personnel and Physical Security Officer

The PPSO must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 5, *OSSI*.

The general and incident response responsibilities of the PPSO must include but are not limited to:

General

- Protect employees, visitors, and CMS-owned and -occupied critical infrastructure [12, 13]
- Coordinate national security information services to all components within the Office of the Administrator (OA)
- Coordinate with appropriate CMS CIO POCs and HHS Office of Security and Strategic Information (OSSI) POCs to ensure background checks are conducted on all individuals identified by system owners with access to CMS information systems in accordance with position sensitivity designation as derived by the use of the appropriate CMS tool
- Ensure relevant paperwork, interviews, and notifications are sent to the appropriate CMS CIO personnel when personnel join, transfer within, or leave the organization, either permanently or on detail

Incident Response

- Participate at the request of law enforcement, the HHS Computer Security Incident Response Center (CSIRC), the HHS Office of the Inspector General (OIG), and/or the CMS Cybersecurity Integration Center (CCIC) in investigating security and privacy incidents and breaches involving federal employees and/or CMS contractor personnel [14]
- Participate at the request of the HHS Privacy Incident Response Team (PIRT) and/or the CMS Breach Analysis Team (BAT) in investigating incidents and/or violations involving federal employees, PII, PHI, and/or Federal Tax Information (FTI)
- Notify the CMS CISO and SOP of actual or suspected information security and privacy incidents and breaches, including CMS sensitive data, using procedures specified in the relevant *RMH* Chapter.

3.2.4 Operations Executive

The Operations Executive must fulfill the responsibilities that include, but are not limited to, the following:

- Oversee day-to-day information security and privacy operations for CMS employees [7]
- Develop and maintain, in coordination with the CISO and SOP, the *HHS Rules of Behavior for Use of HHS Information and IT Resources Policy* [15], to address, at a minimum, the following Acceptable Use standards:
  - Privacy requirements must be identified in contracts and acquisition-related documents.
  - Personal use of CMS IT resources must comply with *HHS Policy for Personal Use of Information Technology Resources*, such that personal use of CMS IT resources does not put CMS data at risk of unauthorized disclosure or dissemination.
- Ensure all CMS system users annually read and sign the *HHS Rules of Behavior for Use of HHS Information Resources*, which governs the appropriate use of CMS IT resources [15].

- Inform CMS employees and contractors that use of CMS information resources, other than for authorized purposes, is a violation of the HHS RoB and Article 35 of the Master Labor Agreement and is grounds for disciplinary action, up to and including removal from federal service, monetary fines, and/or criminal charges that could result in imprisonment. CMS bargaining unit employees must also adhere to Article 35 of the Master Labor Agreement.
- Ensure CMS employees and contractors encrypt CMS sensitive information transmitted to a non-CMS controlled environment,[5] including but not limited to email, using only CMS-approved Federal Information Processing Standard (FIPS) 140-2 compliant encryption solutions [16].
- Ensure CMS employees and contractors are prohibited from transmitting sensitive CMS information using any non-CMS approved, Internet-based mechanism, including but not limited to, personal email, file-sharing, file transfer, or backup services [15].
- Ensure that any CMS contractor, other person, or organization that performs functions or activities that involve the use or disclosure of PHI on behalf of CMS have Business Associate Agreement provisions in their contracts or agreements [17].
- Ensure CMS uses PII internally only for the purpose(s) that are authorized by statute, regulation, or Executive Order; and when the PII is also considered PHI for treatment, payment, healthcare operations, or as permitted under HIPAA (e.g., for research as permitted under 45 CFR §164.512) [15, 17].

3.2.5 Chief Risk Officer

The Chief Risk Officer (CRO) [6] must be an agency official (federal government employee). The Administrator may designate specific responsibilities to the CRO as necessary. [7]

3.2.6 Office Director, Office of Enterprise Data and Analytics and Chief Data Officer

The Office Director of the Office of Enterprise Data and Analytics (OEDA) also serves as the CMS Chief Data Officer (CDO). The CDO must be an agency official (federal government employee). The CDO must establish and implement policies, practices, and standards for maximizing the value and impact of CMS data for internal and external stakeholders.

OEDA develops and implements a data services strategy to maximize use of data on all CMS programs, including issue papers, chart books, dashboards, interactive reports, data enclave services, public use files, and research identifiable files. OEDA oversees the creation of data sets that do not identify individuals and makes these data sets publicly available when there is legal authority permitting their creation. Methods for creating these data sets may include:

[5] Contact the Enterprise Infrastructure Operations Group (EIOG) for organizations that have enforced Transport Layer Security (TLS) in place with CMS.

[6] The Chief Risk Officer is defined within the HHS IS2P as a function in Section 10 (OpDiv CIO)

- The methodology set out at 45 CFR §164.514(b)(2) (the "Safe Harbor Rule") [17].
- The methodology set out at 45 CFR §164.514(b)(1) (the "Expert Determination Rule") [17] .

OEDA also oversees the creation of "limited data sets" (LDS), which are data sets to be used or disclosed for purposes of research, public health, or healthcare operations, using the methodology set out at 45 CFR §164.514(e) [17].

The Administrator may designate other specific responsibilities to the CDO as necessary.

3.2.7 Center and Office Executive

Each CMS Center and Office Executive must nominate an appropriately qualified Data Guardian to the SOP for approval. The executive must ensure the Data Guardian meets the following qualifications:

- Be a proficient consumer advocate
- Have experience identifying information security and privacy requirements
- Be trained in using the *CMS Risk Management Framework* (*RMF*)
- Understand the CMS Center/Office business processes and operations
- Have respect for the role and impact PII and PHI play within the Center/Office and across the CMS enterprise.

3.3 Information Security and Privacy Officers

This subsection describes the information security and privacy responsibilities of those federal employees with roles related to establishing this Policy and the associated Program designed to protect CMS information and information systems, including the CIO, CISO, SOP, Privacy Act Officer, Chief Technology Officer (CTO), Configuration Management Executive, Cyber Risk Advisor (CRA), Privacy Advisor, and Director for Marketplace Security.

3.3.1 Chief Information Officer

The CIO must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 10, *OpDiv CIOs*, including serving as the Authorizing Official (AO) for all CMS FISMA systems. There is only one AO for all CMS FISMA systems.

The responsibilities of the CIO must also include, but are not limited to, the following: [12, 18, 19, 20, 21]

- Designate the CISO as the authority for managing CMS incident response activities identified in HHS IS2P Appendix A Sections 7 and 10
- Define minimum ISSO qualifications commensurate with CMS information sensitivity
- Define mandatory information security and privacy training, education, and awareness activities undertaken by all personnel, including contractors, commensurate with identified roles and responsibilities

- Share threat information as mandated by the Cybersecurity Enhancement Act of 2014
- Coordinate with the CISO to establish configuration management processes and procedures
- Create and manage the review and approval of changes through the appropriate change control bodies/boards
- Coordinate with the CISO, SOP, Data Guardian, ISSO, and Website Owner/Administrator to ensure compliance with control family requirements on website usage, web measurement and customization technologies, and third-party websites and applications
- Respond to any inquiries, investigations, or audits the CIO receives from enforcement authorities, such as any initiated by the HHS Office for Civil Rights related to compliance with HIPAA or the HIPAA Privacy and Security Rules [17]
- Ensure that all CMS key stakeholders, including the CFO; Chief Acquisition Officer (CAO); SOP; mission, business, and policy owners; as well as the CISO organizations, are aware of High Value Asset (HVA) risks
- Ensure the establishment and implementation of an HHS- or CMS-specific HVA Policy and HVA Management Program
- Ensure that owners and operators of HVAs are notified of their asset's designation as an HVA
- Designate a primary HVA representative
- Identify all HVAs and implement HVA requirements as mentioned in this Policy
- Have the SOP review HVAs and identify those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII
- Have the SOP ensure that all required privacy documentation and materials are complete, accurate, and up to date
- Provide HHS with all necessary information to complete an evaluation, if its HVA is selected for an HHS HVA Evaluation
- Liaise with HHS for any DHS HVA assessment engagement
- Provide HHS access to HVA-specific Plan of Action and Milestones (POA&M) on a monthly basis via OMB Max Portal
- Ensure that appropriate contract clauses exist with third-party assessment vendors

3.3.2 Chief Information Security Officer

The CISO[7] must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 11, *OpDiv CISOs*. The CISO carries out the CIO's information security responsibilities under federal requirements in conjunction with the SOP.

[7] Some government directives and standards also refer to this position as the Senior Information Security Officer or Senior Agency Information Security Officer.

The responsibilities of the CISO must include, but are not limited to, the following [12, 14, 18, 19, 20, 22, 23]:

- Define information security and privacy control requirements through the *CMS ARS* and standards, requirements, directives, practices, and procedures through the RMH
- Publish CISO Directives as required to augment existing policy
- Review any requested waivers and deviations from this Policy and provide recommendations to the AO for risk acceptance
- Serve as the security official who is responsible for the development and implementation of the policies and procedures that are required by the HIPAA Security Rule (please refer to 45 CFR §164.308(a)(2))
- Delegate the authority to approve system configuration deviations to the CRA and ISSO, where appropriate
- Ensure CMS-wide implementation of HHS and CMS information security and privacy capabilities, policies, and procedures
- Lead the investigation and resolution of information security and privacy incidents and breaches across CMS
- Define and oversee the goals and requirements of Agency Security Operations
- Coordinate incident response and threat information sharing with the HHS CSIRC and/or HHS PIRT, as appropriate
- Ensure the information security continuous monitoring (ISCM) capabilities accomplish the goals identified in the ISCM strategy [24, 25]
- Publish an Ongoing Authorization process as part of the Program
- Approve the appointment of the ISSO by the Program Executive
- Approve the independent security control assessment deliverables
- Coordinate with the CIO, SOP, Data Guardian, ISSO, and Website Owner/Administrator to ensure compliance with control family requirements on website usage, web measurement and customization technologies, and third-party websites and applications
- Authorize the immediate disconnection or suspension of any interconnection by coordinating with the SOP and the CCIC Director to (1) disconnect or suspend interconnections and (2) ensure interconnections remain disconnected or suspended until the AO orders reconnection

3.3.3 Senior Official for Privacy

The SOP must be an agency official (federal government employee) and must fulfill all the responsibilities identified in the HHS IS2P Appendix A Section 15, *OpDiv SOP*. The SOP carries out the CIO's privacy responsibilities under federal requirements in conjunction with the CISO.

The responsibilities of the SOP must include, but are not limited to, the following [7, 12, 14, 21]:

- Lead CMS privacy programs and promote proper information security and privacy practices
- Lead the development and implementation of privacy policies and procedures, including the following actions:
  - Evaluate any new legislation that obligates the Program to create any regulations, policies, procedures, or other documents concerning collecting, creating, using, disclosing, or retaining PII/PHI
  - Ensure an appropriate party will develop all such required policies or other documents
  - Write or review all such required policies or other documents
  - Ensure policies exist to impose criminal penalties and/or other sanctions on CMS employees (consistent with the CMS Master Labor Agreement) and non-employees, including contractors and researchers, for violations of law and policy
- Ensure privacy controls are implemented and enforced
- Serve as the privacy official responsible for developing and implementing policies and procedures, receiving complaints, and providing further information related to the Notice of Privacy Practices, as required by the HIPAA Privacy Rule (please refer to 45 CFR §164.530(a))
- Ensure individuals are able to exercise their rights to access, inspect, request additions or amendments, and obtain copies of their PII/PHI in a designated record set or in a Privacy Act system of records (SOR) [17][59]
- Ensure individuals are able to exercise their right to an accounting of disclosures of their PII/PHI by CMS or its business associates [17]
- Ensure any use or disclosure of PII/PHI that is not for treatment, payment, health operations, or otherwise permitted or required by the HIPAA Privacy Rule or Privacy Act is disclosed only with the individual's authorization [17]
- Ensure the Program develops and documents a Notice of Privacy Practices for all Medicare Fee-for-Service beneficiaries, as required by the HIPAA Privacy Rule, that defines the uses and disclosures of PHI [17]
- Coordinate with the CIO, CISO, Data Guardian, ISSO, and Website Owner / Administrator to ensure compliance with control family requirements on website usage, web measurement and customization technologies, and third-party websites and applications
- Coordinate as the lead and collaborate with the CISO to:
  - Document privacy requirements and manage privacy implementation as CMS information systems are designed, built, operated, or updated
  - Provide recommendations to the CIO regarding the privacy posture of FISMA systems and the use/disclosure of CMS information
- Co-chair the CMS Data Governance Board
- Approve the appointment of Data Guardians by the Center or Office Executive

- Provide overall direction for incident handling, which includes all incidents involving PII/PHI
- Authorize the immediate disconnection or suspension of any interconnection
  - Coordinate with the CISO and the CCIC Director to disconnect or suspend interconnections
  - Coordinate with the CISO and the CCIC Director to ensure interconnections remain disconnected or suspended until the AO orders reconnection
  - Review HVAs and identify those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII/PHI
  - Ensure that all required privacy documentation and materials are complete, accurate, and up to date

3.3.4 Privacy Act Officer

The Privacy Act Officer must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 16, *OpDiv Privacy Act Contact*.

The responsibilities of the Privacy Act Officer must include, but not be limited to, the following:

- Develop, implement, and maintain policies and procedures related to the Privacy Act
- Process Privacy Act requests, including requests requiring exceptions to the Privacy Act
- Provide guidance and advice on federal Privacy Act policies and procedures
- Evaluate the impact of the Privacy Act and regulations on the organization's activities
- Coordinate with CMS Offices and staff as needed
- Represent CMS on issues related to the Privacy Act
- Assess Privacy Act-related risks associated with programs, operations, and technology
- Support efforts across CMS to comply with the Privacy Act
- Plan and conduct training sessions on Privacy Act requirements
- Ensure procedures exist to:
  - Authenticate the identity of a person requesting PII/PHI and, as appropriate, the authority of any such person permitted access to PII/PHI [17]
  - Obtain any documentation, statements, or representations, as appropriate, whether oral or written, from the authorized person requesting the PII/PHI [17]
  - In responses to requests for disclosures, limit the PII/PHI disclosed to that which is the minimum amount reasonably necessary to achieve the intended purpose of the disclosure or request, relying (if such reliance is reasonable under the circumstances) on the precise scope of the requested disclosure to determine the minimum necessary information to be included in the disclosure [17]
  - In structuring all CMS processes, ensuring that to the greatest degree practicable each person receives only the PII/PHI data elements and records that the person needs (e.g., the data elements the person needs to perform all tasks within the scope of their

assigned responsibilities); When CMS requests PII/PHI from third parties, ensure the PII/PHI requested is limited to the amount reasonably necessary to accomplish the purpose for which the request is made [17]

3.3.5 Chief Technology Officer

A CTO must be an agency official (federal government employee). The Administrator may designate specific responsibilities to a CTO as necessary.

3.3.6 Configuration Management Executive

The Configuration Management Executive must be an agency official (federal government employee) and must provide executive-level oversight for configuration management and contingency planning.

The associated responsibilities are identified under the following HHS IS2P Appendix A sections: Section 20, *Program Executive;* Appendix A Section 21, *System Owner*; and Appendix A Section 24, *Contingency Planning Coordinator*.

3.3.7 Cyber Risk Advisor

The CRA must be an agency official (federal government employee).

The responsibilities of the CRA must include, but are not limited to, the following [26]:

General

- Act as the subject matter expert in all areas of the *CMS RMF*
- Evaluate, maintain, and communicate the risk posture of each FISMA system to executive leadership and make risk-based recommendations to the AO
- Support the CMS stakeholders in ensuring that all requirements specified by the *CMS ARS* and the procedures and standards of the RMH are implemented and enforced; serve as an active participant in the system development life cycle (SDLC) / Technical Review Board (TRB); provide requirements; and recommend design tradeoffs considering security, functionality, and cost
- For each FISMA system or collection of PII/PHI, coordinate with the Data Guardian, Information System Owner (ISO), Business Owner, and ISSO to:
  - Identify the types of information processed
  - Assign the appropriate security categorizations to the information systems
  - Ensure that CMS has the legal authority, either under a statute or an executive order, to conduct activities involving the collection, use, and disclosure of PII/PHI
  - Determine the privacy impacts and manage information security and privacy risk
- Ensure information security and privacy testing is performed throughout the SDLC as appropriate and results are considered during the development phase of the SDLC
- Monitor system security posture by reviewing all proposed information security and privacy artifacts to provide recommendations to the ISSO

- Provide guidance to CMS stakeholders on required actions, potential strategies, and best practices for closure of identified weaknesses
- Upload findings spreadsheets to the CMS FISMA Controls Tracking System (CFACTS)
- Ensure AO-issued authorization is updated in CFACTS
- Serve as the authority to approve selected system configuration deviations from the required baseline
- Upload signed ISSO appointment letter(s) to CFACTS

3.3.8 Privacy Advisor

Privacy Advisors must be federal government employees.

The Privacy Advisor must fulfill responsibilities that include but are not limited to the following:

- Identify opportunities to integrate Fair Information Practice Principles (FIPP) into CMS business processes and information systems
- Evaluate legislation, regulations, and policies that may affect how CMS collects, uses, stores, discloses, or retires PII; identify their potential impact on CMS; and recommend responsive actions to the CMS management or others that request guidance
- For IT systems, coordinate with the Business Owner, CRA, Data Guardian, ISO, and ISSO to identify the types of information processed, assign the appropriate security categorizations to the information systems, determine the privacy impacts, and manage information security and privacy risk, including:
  - Review the Privacy Impact Assessment (PIA) and existing CFACTS documentation to verify that the PIA follows HHS/CMS guidance and verify that privacy risks have been appropriately documented
  - Evaluate privacy-related agreements (e.g., Computer Matching Agreements [CMA], Information Exchange Agreements [IEAs], and Memoranda of Agreement / Understanding [MOA/MOU]) to verify that privacy requirements are satisfied and privacy risks are adequately addressed, both initially and when periodically reviewed, and provide guidance and advice on these agreements to Business Owners, ISOs, and other CMS staff as needed
  - Continuously monitor all findings of privacy risk or deficiency, including by monitoring progress against privacy-related POA&Ms
  - Track the progress of enterprise privacy risk mitigation activities across portfolios
- Provide ISPG perspective during TRB reviews to assess the impact of changes to IT systems on privacy issues and work to mitigate those impacts
- Work with ISSOs to evaluate system changes to determine whether privacy risks are sufficiently significant to require updates to Authority To Operate (ATO) documents
- Works with CRAs to verify that decommission and disposition plans for IT systems do not create significant privacy risks

- Assist in developing reports on any aspect of privacy requested by CMS senior management, HHS, external auditors, or any other party authorized to request and receive such information
- Provide recommendations concerning the privacy risks and practices relevant to IT systems
- Provide incident handling support for incidents involving PII
- Advise CMS healthcare programs on compliance with privacy and related cybersecurity requirements

3.3.9 Director for Marketplace Security

The Director for Marketplace Security must be an agency official (federal government employee).

The responsibilities of the Director for Marketplace Security must include, but are not limited to, the following:

- Ensure the overall information security and privacy of the HIM by driving integration, collaboration, and innovation across disparate groups under the HIM program
- Represent the interests of the CIO, CISO, and SOP by integrating the work of the managers and staff of multiple units to ensure an acceptable information security and privacy posture through visibility, compatibility, and situational awareness
- Provide technical and policy guidance during all phases of the SDLC to balance risk-based tradeoffs among information security, privacy, functionality, and cost

3.4 Program and Information System Roles

This subsection describes the information security and privacy responsibilities of those with roles related to CMS programs and the associated information systems. Program Executives oversee CMS programs and may also serve as ISOs and/or Business Owners. ISOs, referred to as "System Owners" in the HHS IS2P, take responsibility for the operation of information systems required by the CMS program. Business Owners, referred to in the HHS IS2P as "Data Owners/Business Owners," take primary responsibility for the information and data processed by the CMS program.

This subsection identifies specific information security and privacy responsibilities of the Program Executive, ISOs, Data Guardians, Business Owners, Contracting Officers (CO), Contracting Officer's Representatives (COR), and Program/Project Managers. This subsection also describes the responsibilities of the ISSO, including auxiliary responsibilities of the Security Control Assessor and Contingency Planning Coordinator (CPC) that may be filled by the ISSO. The final subsection describes specific responsibilities of the Security Operations Center/Incident Response Team (SOC/IRT).

3.4.1 Program Executive

The CMS Program Executive must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 20, *Program Executive*.

In coordination with the Data Guardian, ISO, and Business Owner, the responsibilities of the CMS Program Executive must include, but are not limited to, the following [7, 27, 28]:

- Nominate appropriately qualified ISSO appointees, as defined under FISMA,[8] to the CISO for approval
- Ensure that information security and privacy for each information system are planned, documented, and integrated from project inception through all phases the CMS SDLC
- In coordination with the CMS SOP, ensure that PIAs are conducted on their programs and/or system(s) to evaluate and control the collection or creation of PII, PHI, and/or FTI
- Establish interconnection security agreements (ISA) before interconnecting any systems
- Consult and coordinate with the CIO and SOP to identify, negotiate, and execute appropriate governing artifacts and agreements before sharing CMS information
- Identify program or system roles that have significant information security or privacy responsibilities

3.4.2 Information System Owner

The CMS ISO must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 21, *System Owner*.

The responsibilities of the CMS ISO must include, but are not limited to, the following [7, 27]:

- For each FISMA system or collection of PII/PHI, coordinate with the Data Guardian, Business Owner, CRA, and ISSO to:
  - Identify the types of information processed
  - Ensure that CMS or the component of CMS conducting collection of PII/PHI has the legal authority, either under a statute or an executive order, to conduct activities involving the collection, use, and disclosure of PII/PHI
  - Assign the appropriate security categorizations to the information systems
  - Determine the privacy impacts
  - Manage information security and privacy risk
- Ensure each system's Change Control Board (CCB):
  - Is an integral part of the information system change management process
  - Implements applicable governing standards as defined in the *RMH*
  - Supports the creation of baseline configuration documentation to reflect ongoing implementation of operational configuration baseline updates
  - Approves ISSO information security configuration recommendations to address weaknesses and system deficiencies
- Develop, implement, maintain, and oversee system-specific RoB training applicable to system(s) under the ISO's purview

[8] From NIST SP 800.37 Rev 1 D.5, an appropriately qualified ISSO is one who "Possesses professional qualifications, including training and experience, required to administer the information security program functions."

- Ensure employees and contractors receive the appropriate training and education regarding relevant information security and privacy laws, regulations, and policies governing the information assets they are responsible for protecting
- Serve as the AO for approving the common controls provided by the system
- Include the Security Control Assessor or representative from the system as a member of the CCB in all configuration management processes that include the system. If the ISSO or Security Control Assessor acts as a voting member of the CCB, they must be federal employees.
- Maintain change documentation in accordance with the CMS Records Retention Policy [29]

3.4.3 Data Guardian

The Data Guardian must be an agency official (federal government employee) and must fulfill shared responsibilities with the CMS Business Owner identified in the HHS IS2P Appendix A Section 22, *Data Owner/Business Owner*.

The responsibilities of the CMS Data Guardian must include, but are not limited to, the following [7]:

General

- Represent the Center or Office on the Data Guardian Committee under the auspices of the CMS Data Governance Board to ensure a coordinated and consistent approach to protecting PII across the CMS enterprise
- For each FISMA system or collection of PII/PHI, coordinate with the ISO, Business Owner, CRA, and ISSO to:
  - Identify the types of information processed
  - Ensure that CMS has the legal authority, either under a statute or an executive order, to conduct activities involving the collection, use, and disclosure of PII/PHI
  - Assign the appropriate security categorizations to the information systems
  - Determine the privacy impacts
  - Manage information security and privacy risk
- Identify and pursue opportunities to proactively enhance information security and privacy controls and increase awareness of the evolving information security and privacy threats to the information assets of the Center or Office

Privacy [30, 31, 32]

- Safeguard PII by creating an information security and privacy aware culture that adheres to information security and privacy standards and requirements designed to protect CMS data assets as directed by the CISO and SOP
- Gather lessons learned and communicate best practices for protecting PII to their Center or Office

- Participate in incident response activities affecting the Center or Office information security and privacy posture

3.4.4 Business Owner

The CMS Business Owner must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 22, *Data Owner/Business Owner* in coordination with the Data Guardian. CMS Business Owners are the Group Directors or Deputy Group Directors who have the primary business needs that are or will be addressed by CMS IT investments/projects [33].

The responsibilities of the CMS Business Owner must include, but are not limited to, the following [7]:

General

- Comply with the requirements of the CMS Policy for IT Investment Management & Governance or its successor policy [33]
- For each FISMA system and collection of PII/PHI, coordinate with the Data Guardian, ISO, CRA, and ISSO to:
  - Identify the types of information processed
  - Ensure that CMS has the legal authority, either under a statute or an executive order, to conduct activities involving the collection, use, and disclosure of PII/PHI
  - Assign the appropriate security categorizations to the information systems
  - Determine the information security and privacy impacts
  - Manage information security and privacy risk
- Work with the COs and CORs to determine the minimum necessary PII/PHI required to conduct the activity for which the agency is authorized
- Coordinate with the COs and CORs, Data Guardian, Program/Project Manager, the CISO, and the SOP to ensure appropriate information security and privacy contracting language from relevant sources is incorporated into each IT contract. Relevant sources must include, but are not limited to, the following:
  - HHS ASFR
  - HHS Office of Grants and Acquisition Policy and Accountability (OGAPA)
  - CMS Office of Acquisition and Grants Management (OAGM)
- For each FISMA system and collection of PII/PHI, coordinate with the Data Guardian, ISO, CRA, and ISSO to ensure compliance with the *CMS ARS*, and when collecting or using FTI, with Internal Revenue Service (IRS) *Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies* [31]

Privacy [30, 31, 32]

- Document data that are collected and maintained and certify that the data are authorized, relevant, and necessary to CMS's mission

- Own the information stored, processed, or transmitted in CMS's information systems and limit access to the data/information
- Manage and approve all use and disclosure of data from CMS programs or systems that are permitted by routine use under CMS System of Records Notices (SORN) through appropriate vehicles to authorize or deny the release of PII
- Verify that CMS's programs or systems only disclose the minimum data necessary
- Determine and certify that the information security and privacy controls that protect CMS's systems are commensurate with the sensitivity of data being protected
- Establish and revise, in coordination with the Privacy Act Officer, SORNs and computer matching agreements in accordance with the established procedures
- Prepare PIAs for programs or systems in accordance with the direction provided by the CRA
- Support the analysis of incidents involving PII and the determination of the appropriate action to be taken regarding external notification of privacy breaches as well as the reporting, monitoring, tracking, and closure of PII incidents

3.4.5 Contracting Officer and Contracting Officer's Representative

The CMS CO and COR must be agency officials (federal government employees) and must fulfill all the responsibilities identified in the HHS IS2P Appendix A Section 27, *CO and COR*.

The responsibilities of the CMS CO and COR must include, but are not limited to, the following [34, 35]:

- Ensure the CISO, SOP, Privacy Act Officer, and Data Guardian are consulted during contract development and that the latest information security and privacy contract language is included in all contracts, as applicable
- Work with the Business Owner to determine the minimum necessary PII/PHI required to conduct each activity for which the agency is authorized
- Collect training records demonstrating that all CMS contractors with significant security and/or privacy responsibilities complete specialized RBT commensurate with their roles within 60 days of beginning work on a contract, upon commencement of the contractors' work, annually thereafter, and upon request

3.4.6 Program/Project Manager

The CMS Program/Project Manager must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 28, *Project/Program Manager* in coordination with the Data Guardian.

The responsibilities of the CMS Program/Project Manager must include, but are not limited to, the following:

General

- Ensure information security and privacy-related actions identified by the CMS SDLC meet all identified information security and privacy requirements [35]

Privacy [6, 7]

- Ensure contractors follow all required information security and privacy policies, standards, and procedures
- Ensure contractors follow all required procedures and provide all required documentation when requesting/gaining access to PII
- Ensure contractors use the minimum data required to perform approved tasks
- Ensure contractors return data covered by approved information sharing agreements at the end of the contract or task to the COR for proper destruction
- Ensure appropriate notification and corrective actions, as described in the CMS Incident Handling procedure [9], are taken when a privacy breach is declared and involves a contractor or a public-private partnership operating a SOR on behalf of CMS

3.4.7 Information System Security Officer

The CMS ISSO may be either a federal government employee or a contractor and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 19, *ISSO*. The ISSO must ensure the duties of the Security Control Assessor and Contingency Planning Coordinator are completed as described in the HHS IS2P Appendix A Sections 18 and 24 and further elaborated in this subsection.

The responsibilities of the CMS ISSO must include, but are not limited to, the following:

General [7, 27]

- For each FISMA system or collection of PII/PHI, coordinate with the Data Guardian, ISO, Business Owner, and CRA to:
  - Identify the types of information processed
  - Ensure that CMS has the legal authority, either under a statute or an executive order, to conduct activities involving the collection, use, and disclosure of PII/PHI
  - Assign the appropriate security categorizations to the information systems
  - Determine the information security and privacy impacts
  - Manage information security and privacy risk
- Report compliance on secure protocol use in websites periodically as defined within the *CMS ARS* [2]
- Submit recommendations to the CRA for system configuration deviations from the required baseline
- Coordinate with the CIO, CISO, SOP, Data Guardian, and Website Owner/Administrator to ensure compliance with control family requirements on website usage, web measurement and customization technologies, and third-party websites and application
- Coordinate with the System Developer and Maintainer in identifying the information security and privacy controls provided by the applicable infrastructure that are common controls for information systems

- Document the controls in the information security and privacy plan (or equivalent document) to ensure implemented controls meet or exceed the minimal controls defined by CISO guidance

Privacy [6, 7]

- Coordinate with the Data Guardian, ISO, Business Owner, and CRA to meet all collection, creation, use, dissemination, retention, and maintenance requirements for PII, PHI, and FTI in accordance with the *Privacy Act*, *E-Government Act*, the HIPAA Privacy and Security Rules, and all applicable guidance

Assessment and Authorization [26, 36]

- Maintain current system information in CFACTS (such as POCs and artifacts) to support organizational requirements and processes (e.g., communication, contingency planning, training, and data calls)
- Coordinate with the Business Owner, ISO, and CISO to ensure that all requirements specified by the *CMS ARS* and the RMH are implemented and enforced for applicable information and information systems
- Ensure anomalies identified under the CMS Continuous Diagnostics and Mitigation (CDM) program and ISCM activities are addressed and remediated in a manner that is commensurate with the risks posed to the system from the anomalies
- Evaluate the impact of network and system changes using RMH processes

System Development Life Cycle [26]

Initiation

- Review and confirm that contracts include appropriate information security and privacy language
- Coordinate with Enterprise Architecture
- Ensure the system appears in CFACTS
- Generate a draft PIA in coordination with the Business Owner
- Evaluate whether other privacy artifacts are required
- Complete System Security Categorization
- Identify system-specific, information security and privacy training needs
- Participate in governance and project reviews identified in the SDLC

Concept

- Identify and discuss risk with the Program Manager and Business Owner
- Identify any investment needs to ensure each FISMA system meets security and privacy requirements

Planning

- Develop a System Security Plan

- Ensure Security Control Assessment is scheduled
- Identify training needs
- Review or develop a corresponding security architecture diagram
- Participate in governance and project reviews identified in the SDLC

Requirements Analysis

- Conduct formal information security risk assessment (ISRA) as defined in the *RMH*
- Complete documentation activities, including the privacy documents

Design

- Ensure that security architecture ingress/egress points are reviewed to meet CMS security requirements
- Ensure data is transmitted, processed, and stored securely
- Participate in governance and project reviews identified in the SDLC

Development

- Verify software code is developed in accordance with the *CMS TRA* and SDLC information security and privacy guidelines
- Participate in governance and project reviews identified in the SDLC

Test

Schedule internal tests such as penetration testing

- Coordinate with the CCIC to ensure assets are identified within monitoring tools
- Ensure use case security testing is incorporated into system functional testing
- Ensure change control processes are followed in accordance with the system security plan (SSP)
- Ensure auditing logs are appropriately capturing required information
- Participate in governance and project reviews identified in the SDLC

Implementation

- Ensure third-party testing begins and weaknesses are resolved quickly
- Ensure each FISMA system is authorized for operation before the go-live date
- Participate in governance and project reviews identified in the SDLC

Operation and Maintenance

- Address weaknesses and POA&Ms
- Review available reports
- Routinely evaluate risk posture based on change requests
- Conduct Security Impact Analysis (SIA) at the direction of the Business Owner
- Participate in governance and project reviews identified in the SDLC

Disposition

- Verify the proper disposition of hardware and software
- Verify data are archived securely in accordance with the National Archives and Records Administration (NARA) requirements in coordination with the Data Guardian
- Initiate the request to close out the project file in CFACTS
- Participate in governance and project reviews identified in the SDLC

3.4.7.1 Security Control Assessor

The CMS Security Control Assessor (also referred to as Certification Agent) role may be performed by an ISSO. The CMS Security Control Assessor must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 18, *Security Control Assessor* [7, 26].

3.4.7.2 Contingency Planning Coordinator

The CMS Contingency Planning Coordinator role may be performed by an ISSO. The CMS Contingency Planning Coordinator must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 24, *Contingency Planning Coordinator*.

The responsibilities of the CMS Contingency Planning Coordinator must include, but are not limited to, the following [18, 37]:

- Work as part of an integrated project team to ensure contingency plans and related operational procedures accommodate all business resumption priorities and defined applicable Maximum Tolerable Downtimes (MTD)
- Ensure procedures exist that achieve continuity of operations of business objectives within appropriately targeted systems with any applicable Recovery Time Objective (RTO) and Recovery Point Objective (RPO) identified in the Business Impact Assessment
- Ensure that the contingency plan is activated if any computer security incident disrupts the system; if the disruption is not resolved within the system's RTO, implement the system's disaster recovery procedures

3.4.8 Security Operations Center/Incident Response Team

The FISMA system SOC/IRT may consist of federal employees or contractors and must fulfill all of the FISMA system-level responsibilities identified in the HHS IS2P Appendix A Section 13, *OpDiv CSIRT*, and applicable responsibilities under the HHS IS2P Appendix A Section 14, *HHS PIRT*. The FISMA system SOC/IRT reports to the Agency Security Operations, which is responsible for CMS-wide incident management.

The Data Guardian, Business Owner, and ISO, in coordination with the CISO, have ownership of and responsibility for incident response and reporting for the FISMA system. The execution of this function begins at the data center/contractor site housing the FISMA system. Once an incident is declared, the CCIC coordinates with FISMA system SOC/IRT and Agency Security Operations personnel for all incident management activities.

The FISMA system SOC/IRT operates under the direction and authority of the ISSO and the Business Owner/ISO. The FISMA system SOC/IRT monitors for, detects, and responds to information security and privacy incidents within the FISMA system environment. The FISMA system SOC/IRT also provides timely, accurate, and meaningful reporting to the FISMA system stakeholders.

FISMA systems may perform the SOC/IRT capability by using a separate CMS CISO-approved SOC/IRT service provider. Any FISMA system SOC/IRT that is unable to deploy the required capabilities may establish an agreement with the CCIC to provide SOC/IRT services.

The responsibilities of the FISMA system SOC/IRT must include, but are not limited to, the following:

General [10]

- For the FISMA system, perform:
  - Real-time network and system security monitoring and triage
  - Analysis, coordination, and response to information security and privacy incidents and breaches
  - Security sensor tuning and management and infrastructure operations and maintenance (O&M)
- Ensure flaw remediation (e.g., patching and installation of compensating controls), planning, ongoing scanning (e.g., ISCM), help desk, asset management, and ticketing are performed for the FISMA system in a manner that meets or exceeds CMS requirements
- Ensure the SOC/IRT-specific tools are implemented and deployed according to the CCIC and vendor technical guidance
- Ensure SOC/IRT-specific tools/equipment are isolated, as appropriate, from operational networks and systems
- Serve as the FISMA system's information security and privacy lead for CCIC and HHS CSIRC

Incident Response [10, 14]

- Report FISMA system information security and privacy incidents and breaches to CCIC and HHS CSIRC as required by federal law, regulations, mandates, and directives, and as reflected in the *RMH*
- Report cyber threat/intelligence/information to CCIC as required by federal law, regulations, mandates, and directives

3.5 Privileged Users

This subsection describes specific information security and privacy responsibilities of users with privileged access to CMS information systems. For example, a privileged user[9] is any user that

[9] CNSSI 4009 defines a privileged user as a user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. Relevant functions are those actions that potentially defeat security controls put in place to protect the system from non-privileged users.

has sufficient access rights to modify, including disabling, controls that are in place to protect the system.

The responsibilities for all privileged users must include, but are not limited to, the following:

- Limit the use of privileged access to those administrative functions requiring elevated privileges

3.5.1 System/Network Administrator

The CMS System/Network Administrator may be a federal employee or a contractor and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 26, *System/Network Administrator* [7].

3.5.2 Website Owner/Administrator

The CMS Website Owner/Administrator may be a federal employee or contractor and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 23, *Website Owner/Administrator*.

The responsibilities of the CMS Website Owner/Administrator must include, but are not limited to, the following [7, 15, 19]:

- Implement proper system backups and patch management processes
- Assess the performance of security and privacy controls associated with the web service to ensure the residual risk is maintained within an acceptable range
- Coordinate with the CIO, CISO, SOP, Data Guardian, and ISSO to ensure compliance with control family requirements on website usage, web measurement and customization technologies, and third-party websites and applications
- Limit connections to publicly accessible federal websites and web services to approved secure protocols [2]
- Ensure federal websites and web services adhere to Hypertext Transfer Protocol (HTTP) Strict Transport Security (HSTS)[10] practices

3.5.3 System Developer and Maintainer

The CMS System Developer and Maintainer must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 25, *System Developer and Maintainer*.

The responsibilities of the CMS System Developer and Maintainer must include, but are not limited to, the following [7, 20, 26, 31]:

- Identify, tailor, document, and implement information security- and privacy-related functional requirements necessary to protect CMS information, information systems, missions, and business processes, including:

[10] https://https.cio.gov/hsts, "Strict Transport Security."

- Ensure the requirements are effectively integrated into IT component products and information systems through purposeful security architecting, design, development, and configuration in accordance with the CMS SDLC and change management processes
- Ensure the requirements are adequately planned and addressed in all aspects of system architecture, including reference models, segment and solution architectures, and information systems that support the missions and business processes
- Ensure automated information security and privacy capabilities are integrated and deployed as required

- Coordinate with the ISSO to identify the information security and privacy controls provided by the applicable infrastructure that are common controls for information systems
- Follow the CMS SDLC in developing and maintaining a CMS system, including:
  - Understand the relationships among planned and implemented information security and privacy safeguards and the features installed on the system
  - Ensure all development practices comply with the *CMS TRA*
- Execute the RMF tasks listed in NIST SP 800-37 and the *RMH*
- Ensure CMS systems or applications that currently disseminate data for any purpose are capable of extracting data by pre-approved categories
- Share only the minimum PII from CMS systems and applications that is necessary and relevant for the purposes it was originally collected [6]

3.6 Agency Security Operations

Agency Security Operations must fulfill all OpDiv responsibilities identified in the HHS IS2P Appendix A Section 13, *OpDiv CSIRT,* and applicable responsibilities under the HHS IS2P Appendix A Section 14, *HHS PIRT*.

Security operations are a shared responsibility between CMS Agency Security Operations and the ISO's SOC/IRT. For each FISMA system, System Developers and Maintainers are expected to establish, maintain, and operate a SOC/IRT to provide FISMA system situational awareness and incident response. For the CMS enterprise, Agency Security Operations maintains visibility and incident management across all FISMA systems, providing management, information sharing and coordination, unified response (including containment and mitigation approaches), and required reporting across the enterprise to CMS Management.

The responsibilities for Agency Security Operations, both within the CCIC and across all SOC/IRTs, must include, but are not limited to, the following:

Awareness and Training [7, 19, 22]

- Ensure all personnel with responsibilities for incident response complete annual RBT
- Ensure non-federal technical personnel (SOC/IRT and CCIC) obtain and maintain appropriate commercial information assurance certification credentials that have been accredited by the American National Standards Institute (ANSI) or an equivalent

authorized body under the ANSI/International Standards Organization (ISO)/ International Electro Technical Commission (IEC) 17024 Standard

– Personnel who do not hold a commercial information assurance certification credential must obtain an appropriate credential within six months of the individual's start date or the release date of this document, whichever is later.

- Encourage federal oversight personnel (SOC/IRT and CCIC) to obtain and maintain a commercial information assurance certification credential that has been accredited by ANSI or an equivalent authorized body under the ANSI/ISO/IEC 17024 Standard.

3.6.1 Director for the CMS Cybersecurity Integration Center

The CCIC operates under the direction and authority of the CMS CISO, who appoints the Director for the CCIC.

The responsibilities of the Director for the CCIC must include, but are not limited to, the following:

General [10, 14]

- Ensure the operational execution of the CCIC function enables the CMS CISO's strategic vision
- Oversee the operation of the CCIC
- Enable CCIC capabilities (penetration testing, security engineering, etc.) to efficiently and effectively enhance the CMS enterprise security posture by performing their roles across the enterprise in coordination with CMS groups, partners, and contractors
- Support the CISO and SOP when immediate disconnection or suspension of any interconnection is required

Awareness and Training [7, 19, 22]

- Define information security and privacy RBT requirements for CCIC and FISMA system SOC/IRT personnel

3.6.2 CMS Cybersecurity Integration Center

The CCIC monitors, detects, and isolates information security and privacy incidents and breaches across the CMS enterprise IT environment. The CCIC provides continual situational awareness of the risks associated with CMS data and information systems throughout CMS. The CCIC also provides timely, accurate, and meaningful reporting across the technical, operational, and executive spectrum.

The responsibilities of the CCIC must include, but are not limited to, the following:

General [7, 27]

- Serve as the primary entity in CMS responsible for maintaining CMS-wide operational cyber security situational awareness, based on coordinated enterprise ISCM activities and the overall information security and privacy risk posture of CMS

- Serve as the information security and privacy lead organization for coordinating within CMS and identified external organizations for Cyber Threat Intelligence (CTI) sharing, analysis, and response activities, including:
  - Identify enterprise threats and disseminate advisories and guidance
  - Identify and coordinate response with SOC/IRT to ongoing threats to CMS
  - Develop and share Indicators of Compromise (IOC)
  - Develop and disseminate unified containment and mitigation approaches
- Define minimum interoperable defensive technology requirements for CMS systems

Incident Response [10, 14]

- Serve as CMS's primary POC with HHS CSIRC
- Report CMS information security and privacy incidents and breaches to HHS CSIRC
- Perform malware analysis and advanced analytics in support of unified incident response
- Coordinate with the Data Guardian when PII is involved
- Coordinate with the CMS Counterintelligence and Insider Threat Program Office, as appropriate

Assessment and Authorization [26, 27]

- Define enterprise-wide information security and privacy requirements for all phases of the SDLC
- Define an enterprise-wide, continual assessment process that:
  - Validates incident response processes and procedures
  - Meets federal law, regulations, mandates, and directives for continual assessment
  - Defines security data monitored by all SOCs/IRTs and is made available to the CCIC
- Define reporting metrics that are compliant with federal law, regulations, mandates, and directives for:
  - Penetration testing
  - Information security continuous monitoring
  - Information security and privacy incident and breach response
  - Cyber threat intelligence
- Determine risk and impact on the CMS enterprise based on:
  - Real-time monitoring and triage
  - Analysis, coordination, and response to incidents
  - Collection, sharing, and analysis of CTI (i.e., knowing the adversary)
- Develop, in coordination with the CCIC Director, information security and privacy RBT requirements for CCIC and FISMA system SOC/IRT personnel

3.6.3 Agency Continuity Point of Contact

The Agency Continuity Point of Contact must be an agency official (federal government employee) and is the individual the Administrator designates as the accountable official who will:

- Perform the duties and responsibilities of the Agency Continuity Point of Contact, as set out in HHS's Continuity of Operations Program Policy
- Be directly responsible to the Administrator for management oversight of the CMS continuity program
- Serve as the single POC for coordination within CMS for continuity matters

3.7 CMS Governance Boards

CMS Executive Management established multiple governance boards to confirm policy, make strategic decisions, and provide appropriate federal oversight for all investments. These boards promote CMS strategic objectives and enforce federal requirements, including information security and privacy processes.

The primary governance boards relevant to information system security and privacy policy are:

- The **Strategic Planning Management Council (SPMC)**, co-chaired by the Chief Operating Officer (COO) and CIO, manages oversight of all CMS investment-related governance boards.
- The **IT Investment Review Board (ITIRB)** supports the Investment Management and Oversight Boards.
- The **Technical Review Board (TRB)** aligns with the Technical Standards Oversight Boards.
- The **Data Governance Board (DGB)** supports overall agency data governance.

3.7.1 Strategic Planning Management Council

The SPMC provides leadership and support for executing CMS strategic objectives across all CMS investments [38]. The SPMC provides a forum for ongoing collaboration among teams and overall management of the CMS Strategy.

3.7.2 Information Technology Investment Review Board

The CMS ITIRB serves as the executive review and oversight body for CMS IT management by providing enterprise-wide, strategic decision making; shared leadership; transparency; monitoring; and true ownership of major IT decisions, opportunities, and risks. The ITIRB ensures proposed investments comply with departmental objectives and system architectures, while providing the highest return on investment within acceptable project risk thresholds.

3.7.3 Technical Review Board

The TRB provides oversight to ensure IT investments are consistent with CMS's IT strategy. The board manages updates to the *CMS TRA* to promote the CMS IT strategy and assists projects

by ensuring solutions are technically sound and on track to deliver promised capabilities on time and on budget. The TRB:

- Provides technology leadership to deliver business value and anticipate change to meet the current and long-term needs of CMS programs
- Implements and communicates CMS's IT governance that ensures and secures cost-effective, sustainable systems to support the agency's business

3.7.4 Data Governance Board

The CMS Data Governance Board (DGB) provides executive leadership and stewardship of the agency's data assets, including oversight for the development and implementation of the policies and processes which govern the collection or creation, management, use, and disclosure of CMS data. The DGB ensures intra-agency transparency and data stewardship to promote efficient and appropriate use of, and investment into, agency data resources. Transparency and data stewardship include:

- *Openness:* Promoting and facilitating the open sharing of knowledge about CMS data, including an understanding of how and where agency data are collected or created, stored, managed, and made available for analysis.
- *Communication:* Promoting partnerships across the CMS enterprise to eliminate duplication of effort, stove-piping, and one-off solution designs.
- *Accountability:* Ensuring agency-wide compliance with approved data management principles and policies. Understanding the objectives of current and future strategic or programmatic initiatives and how they impact, or are impacted by, existing data management principles and policies as well as current privacy and security protocols.

4. Integrated Information Security and Privacy Policies

This section presents the high-level CMS integrated information security and privacy policies, defined by control statements and organized into three categories. Section 4.1 lists policies specific to CMS, as tailored from the HHS IS2P or created by CMS. Section 4.2 provides the CMS policies aligned with the eighteen (18) security control families identified in NIST SP 800-53 as the Security Control Baseline. Section 4.3 provides the CMS privacy-specific policies, including the eight privacy control families from Appendix J of NIST SP 800-53. Each policy statement is numbered to help users directly reference a specific policy. The *CMS ARS* includes additional detailed information security and privacy control policies.

4.1 CMS Tailored Policies

The HHS IS2P delineates information security and privacy policies, including both mandated security controls and a provision for CMS to develop its own controls for CMS information systems. CMS tailored specific controls to ensure they meet the mission and vision of the organization. This subsection lists the tailored controls, which include:

1. Controls explicitly mandated for CMS by an authoritative agent (e.g., HHS or other federal agency)
2. Controls that have been modified to address the CMS implementation (e.g., CMS architecture, risk framework, and life cycle)
3. Controls that address specialized topics that extend beyond NIST SP 800-53 as amended (e.g., the Federal Risk and Authorization Management Program [FedRAMP])

CMS tailors HHS IS2P policy by requiring the use of CMS standards, requirements, directives, practices, and procedures outlined in the *RMH*. Business Owners and Information System Owners must apply the appropriate baseline based on the security categorization and tailor the controls to the specific circumstances of the information and the information system.

4.1.1 Employee Monitoring/Insider Threat (CMS-EMP)[11]

CMS-EMP-1 The use of warning banners is mandatory on all CMS information systems in accordance with federal and HHS policy and the ARS control requirements. A warning banner states that by accessing a CMS information system, (e.g., logging onto a CMS computer or network), the employee[12] consents to having no reasonable expectation of privacy regarding any communication or data transiting or stored on that system, and the employee understands that, at any time, CMS may monitor the use of CMS IT resources for lawful government purposes [39].

[11] For the purposes of this Policy, any monitoring of employee activities are governed and subject to compliance with the Master Labor Agreement between CMS and the American Federation of Government Employees, Local 1923.

[12] For the purposes of this policy requirement, the term "employee" includes all individuals who have been provided and currently have access to CMS IT resources and who are current employees, contractors, guest researchers, visiting scientists, and fellows. The term excludes individuals who are not or are no longer CMS employees, contractors, guest researchers, visiting scientists, or fellows.

CMS-EMP-2 In accordance with HHS policy [39, 40] the CMS CIO must carry out monitoring in a fashion that protects employee interests and ensures the need for monitoring has been thoroughly vetted and documented.

Computer monitoring[13] of an employee at CMS may be requested by HHS/OSSI, HHS/OIG, CMS Counterintelligence and Insider Threat Program Office, or an outside law enforcement authority.

CMS-EMP-3 All requests from outside law enforcement agencies must be coordinated through the HHS/OIG, except for requests relating to national security or non-criminal insider threat matters. The latter must be coordinated with the Security Management Group, Physical Security and Strategic Information (DPSSI), which in turn coordinates with HHS/OSSI on all requests. Such external computer monitoring requests may be subject to different standards, partly because they are covered by the internal controls of the requesting agency or judicial process.

CMS-EMP-4 No CMS official may initiate computer monitoring without advance written authorization by the CMS Administrator or the CMS CIO. By HHS policy, this authority to authorize monitoring may not be delegated below the CMS CIO. Prior to submission of a monitoring request, the CMS CIO or HHS/OSSI consults with the HHS Office of the General Counsel (OGC). The requesting organization documents the basis for approving any request for computer monitoring.

CMS-EMP-5 Computer monitoring may only be authorized for the following reasons:

1. Monitoring has been requested by the HHS/OSSI, HHS/OIG, CMS Counterintelligence and Insider Threat Program Office, or an outside law enforcement authority in accordance with CMS Administrative Services Group, DPSSI and federally recognized jurisdiction.
2. Reasonable grounds exist to conclude that the individual to be monitored may be responsible for an unauthorized disclosure of legally protected information (e.g., confidential commercial information or *Privacy Act* protected information).
3. Reasonable grounds exist to believe that the individual to be monitored may have violated an applicable law, regulation, or written HHS or CMS policy.

Routine IT equipment examinations are permissible when malware searches are involved. Any unintended discoveries of problematic content and resulting follow-up actions are not subject to this policy except for follow-up actions that involve computer monitoring.

CMS-EMP-6 In circumstances in which HHS/OIG requests computer monitoring for purposes of an HHS/OIG investigation or where HHS/OIG requires assistance in the conduct of computer

[13] For the purposes of this policy, the term "computer monitoring" covers monitoring of CMS IT resources, including real-time or contemporaneous observation, prospective monitoring, (e.g., using monitoring software), and retrospective review and analyses (e.g., of email sent or received, of computer hard-drive contents) focusing on an individual employee. This section of policy does not apply to passive monitoring (computer incident response monitoring) of systems relating to national security or FISMA that perform general system and network monitoring or examinations of computers for malware. Additionally, computer monitoring excludes any review and analysis requested by or approved by the employee(s) being covered. This does not apply to retrospective searches for documents in response to valid information requests in the context of litigation, Congressional oversight, Freedom of Information Act (FOIA) requests, and investigations by the Government Accountability Office (GAO) and the Office of Special Counsel. Such retrospective searches may be conducted with the consent of the employee or the authorization of the CMS CIO.

monitoring, HHS/OIG will provide such information or notification as is consistent with its responsibilities, duties, and obligations under the *Inspector General Act of 1978*.

CMS-EMP-6.1 In concert with the HHS/OGC, the CMS CIO must develop a memorandum of understanding (MOU) or similar written agreement with outside law enforcement agencies as a precondition for approving monitoring requests from these organizations. The MOU must include the following:

- Title and organizational component of the person(s) authorized to make monitoring requests on behalf of the law enforcement agency.
- Documentation of the source of the official request demonstrating approval by an official of the governmental entity that has the authority to request the initiation of such monitoring (e.g., a subpoena [administrative or grand jury], warrant, national security letter [NSL], or other acceptable documented request [e.g., a written law enforcement administrative request that meets applicable requirements of the *Privacy Act* and/or HIPAA requirements for certain disclosures to law enforcement agencies]).
- Any restrictions applicable to the handling and disclosure of confidential information that may be produced by monitoring.
- Other items consistent with this memorandum, including handling sensitive communications, as described in the following bullet (Documentation).
- Documentation – the written authorization for computer monitoring describes the reason for the monitoring. If the monitoring is initiated at the request of outside law enforcement authorities, the authorization documents that the request was approved, consistent with the applicable MOU with that organization by an official of the governmental entity that has the authority to request the initiation of such monitoring.

CMS-EMP-6.2 Except for monitoring initiated at the request of an outside law enforcement authority or the HHS/OIG, the party requesting the monitoring must document the factual basis justifying the request for monitoring and the proposed scope of the request. Requests for such monitoring must include an explanation of how monitoring will be conducted, how the information collected during monitoring will be controlled and protected, and a list of individuals who will have access to the resulting monitoring information.

CMS-EMP-6.3 A record of all requests for monitoring must be maintained by the CMS CIO along with any other summary results or documentation produced during the period of monitoring. The record must also reflect the scope of the monitoring by documenting search terms and techniques. All information collected from monitoring must be controlled and protected with distribution limited to the individuals identified in the request for monitoring and other individuals specifically designated by the CMS Administrator or CMS CIO as having a specific need to know such information.

CMS-EMP-7 The CMS Administrator or CMS CIO must ensure authorized computer monitoring is appropriately narrow in scope and time limited and takes the least invasive approach to accomplish monitoring objectives. The CMS Administrator or CMS CIO, in reviewing requests for monitoring, must consider whether there are alternative information gathering methods that CMS can utilize to address the concern in lieu of monitoring. When the

monitoring request originates from HHS/OIG or outside law enforcement, CMS will grant appropriate deference to a request made in accordance with this policy.

CMS-EMP-8 No monitoring authorized or conducted may target communications with law enforcement entities, the Office of Special Counsel, members of Congress or their staff, employee union officials, or private attorneys. Employee union officials of CMS will be treated, for non-targeted monitoring purposes, as all other employees of CMS when monitoring is necessary. If such protected communications are inadvertently collected or identified from more general searches, they may not be shared with a non-law enforcement party who requested the monitoring or anyone else without express written authorization from the HHS/OGC and other appropriate HHS official(s).

CMS-EMP-9 When a request for computer monitoring is made by a party other than an outside law enforcement authority or the HHS/OSSI, HHS/OIG, CMS Counterintelligence and Insider Threat Program, CMS must consult with the OGC as to whether the monitoring is consistent with all applicable legal requirements, including the *Whistleblower Protection Act* and *HIPAA*, and consider whether there are any additional limits. In addition, except for monitoring initiated at the request of outside law enforcement or the HHS/OIG, parties that receive information derived from monitoring must consult with the OGC as to potential restrictions on the use of such information under applicable law.

CMS-EMP-10 The CMS CIO must review all employee monitoring on a monthly basis and, in consultation with the party who requested the monitoring, assess whether it remains justified or is to be discontinued. The CMS CIO must consider whether or not the decision for ongoing monitoring must be reviewed by the OGC. A decision to continue monitoring must be explained and documented in writing by the CMS CIO, who must report at least monthly to the CMS Administrator regarding the status of any ongoing monitoring.

CMS-EMP-11 The CMS CIO and the OGC may make recommendations to the CMS Administrator for additional procedures, if necessary, to address specific circumstances not addressed in this policy. Insider threat policies and procedures that deviate from the elements of this policy, however, must not be implemented without the written concurrence of the HHS CIO in consultation with the OGC.

4.1.2 Risk Management Framework (CMS-RMF)

CMS-RMF-1 The CMS CISO must develop and maintain within the ARS (*Security Assessment and Authorization* family of controls) minimum controls to ensure information systems: (i) are assessed at least every three years or whenever a significant change occurs[14] (as defined in the RMH) to the information system to determine if security and privacy controls are effective in their application; (ii) have POA&Ms designed to correct deficiencies and reduce or eliminate vulnerabilities; (iii) are authorized for processing (including any associated information system connections) by the CMS CIO; and (iv) are monitored on an ongoing basis to ensure the continued effectiveness of the controls. In addition, the CMS CISO, where necessary to add clarity, provides methods in the form of *Chapters, Procedures,* and/or *Standards* within the

[14] NIST SP 800-37 describes examples of significant changes to an information system that should be reviewed for possible re-authorization.

RMH to facilitate implementation, assurance, and tracking effectiveness of those controls. Minimally, these processes and procedures must address the following [26]:

CMS-RMF-1.1 Ensure all systems and networks receive a system categorization in accordance with the frameworks set forth in FIPS 199, NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, and the RMH.

CMS-RMF-1.2 Ensure CMS Business Owners/ISOs conduct risk assessments on systems and networks and document the result in accordance with NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

CMS-RMF-1.3 Ensure the CMS Business Owners/ISOs review and update risks, as necessary, no less than annually or when significant changes occur to the system/network.

CMS-RMF-1.4 Ensure CMS Business Owners/ISOs implement appropriate information security and privacy controls as documented in an information security and privacy plan for each CMS system and network in accordance with NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, and that CMS Business Owners/ISOs review and update plans as needed but no less than annually or when significant changes occur to the system/network.

CMS-RMF-1.5 Ensure CMS Business Owners/ISOs implement and document information security and privacy controls outlined in NIST SP 800-53 [41].

CMS-RMF-1.6 Assess the controls using the procedures outlined in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.

CMS-RMF-1.7 Develop, disseminate, and review/update: (i) formal, documented security assessment and authorization standards that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.

CMS-RMF-1.8 Determine (i) the required level of Security Control Assessor independence based on the security categorization of the information system and/or the ultimate risk to organizational operations and assets and to individuals; and (ii) if the level of Security Control Assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision.

CMS-RMF-1.9 Ensure all CMS systems and networks are formally assessed and authorized using the methodology outlined in NIST SP 800-37 and in accordance with the minimum content requirements for the creation of security authorization packages, as stated in the ARS and the RMH.

CMS-RMF-1.10 Ensure the Security Control Assessor(s) [15] is identified and assigned prior to applying the RMF tasks to the information system. The AO for the information system (i) is the CMS CIO, (ii) authorizes the information system for processing before commencing operations, and (iii) uses the results of the ISCM process to the maximum extent possible as the basis for rendering a re-authorization decision.

CMS-RMF-1.11 Require SIA and PIA review when any significant change occurs to a CMS system, network, physical environment, etc., to assess the impact of the change on the information security and privacy of the information processed.

CMS-RMF-1.12 Ensure CMS Business Owners/ISOs request to re-authorize all systems at least every three years or when a significant change occurs to the system.

CMS-RMF-1.13 Develop a ISCM strategy and implement a ISCM program that includes: (i) a configuration management process for the information system and its constituent components; (ii) determination of the security impact of changes to the information system and environment of operation; (iii) ongoing information security and privacy control assessments in accordance with the organizational ISCM strategy; and (iv) reporting on the security state of the information system to appropriate organizational officials.

The organization assesses the information security and privacy controls in an information system, at a minimum, as part of (i) security authorization or re-authorization, (ii) meeting the FISMA requirement for annual assessments, (iii) ISCM, and (iv) testing/evaluation of the information system as part of the SDLC process. Those controls that are the most volatile (e.g., controls most affected by ongoing changes to the information system or its environment of operation) or deemed essential to protecting CMS operations and assets, individuals, other organizations, and the nation are assessed more frequently in accordance with the CMS CISO's assessment of risk as defined in the ARS. All other controls are assessed at least once during the information system's three-year authorization cycle.

4.1.3 CMS System Development Life Cycle (CMS-SDLC)

Security Architecture and Engineering (SA&E) activities help CMS Components align with enterprise information security and privacy capabilities, reporting processes, and requirements. SA&E ensures that the information security environment continues to meet business needs and address new and emerging threats by identifying risks and providing adequate information security and privacy protections through testing, implementation, and improvement of new and existing technologies and processes. To help guide a unified enterprise approach to implementing information security and privacy architecture, the risk management and compliance functional area publishes and updates information security and privacy technical guidance and provides input into the development of TRA security-related supplements.[16]

[15] Per NIST SP 800-37 (available at http://csrc.nist.gov/publications/PubsSPs.html), security control assessors may be called certification agents in some organizations. At the discretion of the organization, security control assessors may be given additional duties/responsibilities for the post-processing and analysis of security control assessment findings and results. This may include, for example, making specific determinations for or recommendations to authorizing officials (known in some communities of interest as certification recommendations or certification determinations).

[16] http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/Technical-Reference-Architecture-Standards/

Security Assessment and Authorization (SA&A) processes help CMS Business Owners/ISOs comply with Capital Planning and Investment Control (CPIC) processes and CMS's SDLC processes to incorporate the security requirements of the ARS and the CMS TRA to obtain system authorization, also referred to as Authority to Operate (ATO), prior to operation. The CMS CISO and SOP follow the procedures outlined in the RMF for SA&A in accordance with FISMA and the direction of the CMS CIO.

The SA&A processes help CMS stakeholders identify information security and privacy risks, assess the adequacy of information security and privacy controls, and ensure information security and privacy responsibilities are assigned prior to authorizing systems for operation. These processes incorporate ISCM[17] and periodic manual assessment techniques to appropriately test the ongoing effectiveness of all controls.

The RMH Chapter for Planning [42] describes how CMS implements the CMS RMF in the SDLC processes, including privacy requirements. By following CPIC, SDLC, and RMF, System Developers and Maintainers include information security and privacy requirements from project initiation throughout the life cycle and implement the appropriate controls to manage information security and privacy risk.

The ARS and the RMH provide specific guidance and standards for completing the RMF process and include descriptions of the artifacts required to document information and information system controls. The SA&A processes result in identification of information security and privacy risks that must be managed by the POA&M processes, which are also described in the RMH [20].

CMS-SDLC-1 The CISO must integrate information security and privacy into the CMS life cycle processes. The SDLC provides the processes and practices of the CMS system development life cycle in accordance with the *CMS Policy for Information Technology (IT) Investment Management & Governance* [33]. The CMS CISO maintains the RMH to document the CMS information system life cycle, in accordance with the RMF [26]

CMS-SDLC-2 Program Executives must engage the ISSO, CRA, and privacy team early and throughout the SDLC.

CMS-SDLC-3 The SDLC and the RMH processes and procedures must:

CMS-SDLC-3.1 Integrate information security and privacy requirements into all CMS SDLC activities (i.e., Initiation, Concept, Planning, Requirements Analysis and Design, Development and Test, Implementation, Operations and Maintenance, and Disposition).[18]

CMS-SDLC-3.2 Ensure critical SDLC stage gate reviews are conducted to govern the information security and privacy posture of the system being developed. The TRB must evaluate the information security and privacy risk introduced by the system and provide guidance to improve system architecture and engineering [26, 42, 43].

CMS-SDLC-3.3 Assign information security and privacy roles for the information system [7, 44].

[17] See section 4.1.2 RMF for additional information on ISCM.

[18] RMF tasks are executed concurrently with SDLC processes and are documented (and cross-walked) in the *RMH*.

CMS-SDLC-3.4 Ensure system information security and privacy controls are assessed.

CMS-SDLC-3.5 Ensure system authorization prior to entering the O&M phase of the SDLC.

CMS-SDLC-3.6 Ensure systems undergo ongoing information security and privacy control assessments and vulnerability scanning as defined in information security continuous monitoring plans.

CMS-SDLC-3.7 Ensure systems that no longer have a business need are appropriately retired in accordance with the established System Disposition Plan. Any sensitive information such as PII on the system must be disposed of, destroyed, erased, and/or anonymized, regardless of the method of storage, in accordance with a NARA-approved record retention schedule. Retention and destruction must be done in a manner that prevents loss, theft, misuse, or unauthorized access as identified in any applicable information sharing agreements.

4.1.4 Cloud Computing Policies (CMS-CLD)

This Policy supersedes *CMS Cloud Computing Policy*, dated November 12, 2014.

CMS developed CMS-CLD policies to provide guidance and direction on the acceptable uses of cloud service providers (CSP) and cloud computing services in compliance with the *Federal Cloud Computing Strategy (Cloud-First)* [45]. The CMS-CLD policies define directives concerning the procurement, deployment, and utilization of cloud computing services across the CMS enterprise. The CMS-CLD policies are not a process guide for developing or deploying cloud computing projects at CMS.

This Policy governs only new or legacy computing project implementations that are deemed cloud computing solutions as defined under *Cloud First*. A "cloud computing installation" possesses characteristics consistent with those defined by NIST SP 800-144 and SP 800-145.

In accordance with *Cloud First*,[19] CMS permits cloud services within the CMS environment. CMS established the policies in this section to guide use of cloud services and cloud computing installations.

CMS-CLD-1 All cloud service implementations must have an approved Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) Provisional ATO (P-ATO) or an Agency ATO. FedRAMP authorization ensures the minimum baseline controls are in place. Business Owners must verify the CSP meets additional CMS and HHS security, monitoring, and reporting requirements prior to selecting a cloud service. The designated Business Owner must:

[19] See www.fedramp.gov for more information.

- Comply with FedRAMP controls to meet the FedRAMP baseline for the use case under the stated FedRAMP categorization
- Submit an authorization package to the CMS CISO that includes all documentation required by FedRAMP for an ATO and complete all required templates and processes
- Store FedRAMP documentation on the FedRAMP Program Management Office (PMO) website
- Maintain consistent contact with approved CSP to manage risk

CMS-CLD-2 All FISMA systems and applications deployed on a CSP service must have a CMS-issued ATO.

4.1.5 Information Sharing Agreements (CMS-ISA)

CMS must comply with information security and privacy policies defined by federal organizations external to CMS (e.g., Internal Revenue Service [IRS], DHS) via information sharing agreements. CMS Information Sharing Agreement (CMS-ISA) provides the CMS standards for implementing information security and privacy controls mandated by other federal organizations (i.e., controls not routinely applicable to CMS).

CMS-ISA-1 CMS employees and contractors are prohibited from transmitting sensitive CMS information using any non-CMS approved, Internet-based mechanism, including but not limited to personal email, file-sharing, file transfer, and backup services.

CMS-ISA-2 The Program must develop and document CMS-ISA policies governing information security and privacy requirements defined by federal organizations external to CMS and required under inter-agency agreements. ISA controls apply to all FISMA systems within the CMS enterprise environment or any systems storing, processing, or transmitting CMS information on behalf of CMS and the external federal organization. The Program must:

CMS-ISA-2.1 Develop and maintain an effective implementation of selected controls and control enhancements for all inter-agency information security and privacy controls in the ARS to:

CMS-ISA-2.1.1 Address information security and privacy requirements defined by inter-agency agreements.

CMS-ISA-2.1.2 Address information security and privacy training requirements defined by inter-agency agreements.

CMS-ISA-2.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for all inter-agency information security and privacy controls.

CMS-ISA-2.2.1 Use PII internally only for the authorized purpose(s) identified in the *Privacy Act* and/or in public notices.

CMS-ISA-2.2.2 Share PII externally only for the authorized purposes identified in the *Privacy Act* and/or described in its notice(s) or in a manner compatible with those purposes.

CMS-ISA-2.2.3 Enter into appropriate agreements with third parties (e.g., Data Use Agreement [DUA], CMA, information exchange agreements) that specifically describe the PII covered and enumerate the purposes for which the PII may be used.

CMS-ISA-2.2.4 Monitor, audit, and train staff on the authorized uses and sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

CMS-ISA-2.2.5 Evaluate any proposed new instances of sharing PII with third parties to assess whether the use is authorized and whether additional or new public notice is required.

4.1.6 CMS Email Encryption Requirements (CMS-EMAIL)

CMS must comply with information security and privacy encryption policies defined by federal laws, executive orders, directives, regulations, policies, standards, and guidance (e.g., HIPAA, Health Information Technology for Economic and Clinical Health [HITECH], Privacy Act, and IRS Publication 1075). The CMS Email Encryption Requirements control family provides the CMS standards for implementing information security and privacy controls.

CMS-EMAIL-1 CMS Sensitive Information must be protected and only sent to recipients with a "need to know." Emails containing sensitive information must be protected using one of the following steps:

CMS-EMAIL-1.1 Ensure unencrypted emails containing sensitive information remain within the HHS email shared service environment (i.e.,"jane.doe@opdiv.hhs.gov") or trusted domain.

CMS-EMAIL-1.2 For recipients outside of the HHS email shared service environment or trusted domain:

CMS-EMAIL-1.2.1 Encrypt sensitive email and email attachments using the certificates contained on federally issued Personal Identity Verification (PIV) cards.

CMS-EMAIL-1.2.2 Place the CMS sensitive information in a password-protected, encrypted email attachment using software that meets FIPS 140-2 for encryption software, (e.g., SecureZip) [16].

CMS-EMAIL-1.2.3 Sending passwords for an encrypted attachment via email is prohibited. Instant messaging clients that are integrated with Microsoft Outlook, such as Lync/Skype, must not be used to communicate passwords. Acceptable approaches for sharing passwords include phone conversation , text message, or a shared secret. The method chosen must protect the password from compromise.

4.1.7 CMS High Value Asset Requirements (CMS-HVA)

CMS must comply with the Office of Management and Budget (OMB) Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*; the Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-02, *Securing High Value Assets;* and the *HHS High Value Asset (HVA) Program Policy* (February 2018) [21, 46, 47].

The *HHS HVA Program Policy* defines HVAs as:

> Assets, federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people.

The HHS policy requires CMS to establish appropriate governance of HVA activities across its organization and integrate HVA remediation activities into its planning, programming, budgeting, and execution process. These efforts will align with federal law, regulations, standards, and guidelines, as well as CMS policies, processes, and procedures. To meet the HHS policy, CMS will conduct the following activities:

CMS-HVA-1 The CMS CIO develops a process for creating and maintaining an HVA inventory, consistent with any format and content specified by HHS. Upon request, the Program will complete or update the inventory. HHS may require the inventory to note any or all threats, vulnerabilities, and impacts, and the likelihood of each of these occurring, associated with each system. CMS will share its HVA inventory with HHS upon request, following HHS instructions and consistently with the RMH.

CMS-HVA-2 When creating or updating HVA-related contracts and acquisition requirements, CMS Contracting Officers' Representatives (COR) must incorporate appropriate language from the HHS Security and Privacy Language for Information and Information Technology Procurements [1].

CMS-HVA-3 HVA-related artifacts must be handled as directed by OMB [47] and DHS [46]. These documents include instructions for securing and encrypting all correspondence involving HVA-related information.

CMS-HVA-4 HVAs must have a valid Authority to Operate (ATO). An ATO must reflect that appropriate safeguards have been implemented to protect the HVA, many of which will be specific to HVAs.

CMS-HVA-5 Security assessments must be conducted on HVAs using independent third-party assessment providers at the frequency and rigor stipulated by DHS.

CMS-HVA-6 The CMS CIO must develop a Standard Operating Procedure (SOP) for reviewing CMS's HVAs to identify those HVAs that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.

4.1.8 Federal Tax Information

Systems that collect, maintain, use, or disclose Federal Tax Information (FTI) must follow IRS requirements for protecting FTI. Business Owners of CMS systems, with direction provided by the OIT, must ensure that all applicable information security and privacy controls, whether imposed by an organization or office internal or external to CMS, are incorporated into CMS systems.

The IRS defines Federal Tax Information as federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the

confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. CMS often receives, accesses, and uses FTI in conducting its business processes.

CMS-FTI-1 Business Owners that collect, maintain, use, or disclose FTI must:

CMS-FTI-1.1 Comply with IRS Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*.

CMS-FTI-1.2 Document and certify the incorporated controls in their respective system security plan and identify residual risks in the corresponding risk assessment for their systems.

CMS-FTI-1.3 Disclose FTI to its agents solely for purposes for which there is an appropriate legal authority, and for which IRS has granted an exception permitting its disclosure (see Section 4, Authority and Purpose [AP], section CMS-AP-1.1.1).

CMS-FTI-1.4 Notify the IRS Office of Safeguards prior to re-disclosing FTI to contractors. Notify and obtain written approval from the IRS Office of Safeguards prior to re-disclosing FTI to sub-contractors.

CMS-FTI-1.5 Execute a contract or other agreement with any recipient of the FTI. The contract must require the recipient to abide by IRS Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, including its requirements for providing privacy and security controls for FTI.

4.2 Security Control Families

CMS requires compliance with the security control families described in NIST SP 800-53. For each control family, the first set of controls—often referred to as the "dash one" controls—requires that specific policies be in place, while the remaining controls provide details for implementing the policy. CMS includes the "dash one" controls in this Policy and defers the details for each security control to the ARS. The RMH documents the CMS procedures and standards for implementing these controls. The following subsections present the policies associated with the 18 NIST security control families [48].

4.2.1 Access Control (AC)

AC-1 The Program must develop and document an access control policy that addresses purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance. The Access Control family of controls ensures access to information systems is limited to authorized users, processes acting on behalf of authorized users, and devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. The Program must [7, 31, 48, 5, 49, 50, 51]:

AC-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Access Control family of controls in the ARS.

AC-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Access Control family of controls.

AC-1.3 Review policies, procedures, and standards for the Access Control family of controls periodically, as defined in the ARS and RMH.

AC-1.4 Disseminate policies, procedures, and standards for the Access Control family of controls to all personnel who perform roles defined within this Policy.

AC-1.5 Maintain all policies, procedures, and standards associated with the Access Control family of controls to reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

AC-1.6 Define access control policies and procedures to provide the foundation required to ensure privacy protections are implemented for the identified uses of PII and PHI.

4.2.2 Awareness and Training (AT)

AT-1 The Program must develop and maintain minimum controls to ensure managers and users of information systems are made aware of the information security and privacy risks associated with their activities and of the applicable federal and agency requirements related to the information security and privacy of CMS systems. Through the Program, the CMS CISO must [7, 27]:

AT-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Awareness and Training family of controls in the ARS for CMS to:

AT-1.1.1 Develop topic-based training to explain privacy processes carried out within CMS and update topic-based training courses when significant changes occur to privacy processes.

AT-1.1.2 Develop and implement an information security and privacy education, awareness, and training program for all employees and individuals working on behalf of CMS involved in managing, using, and/or operating information systems.

AT-1.1.2.1 Ensure information security awareness and training is provided to all employees and contractors, and that all employees and contractors review and acknowledge an approved within sixty (60) days from entry on duty (EOD) date, or commencement of work on a contract or subcontract; and ensure and acknowledge the RoB annually thereafter.

AT-1.1.2.2 Ensure privacy awareness and training is provided within sixty (60) days from EOD date, or commencement of work on a contract or subcontract., and annually thereafter, to all employees and contractors to explain the importance and responsibility in safeguarding PII and PHI and ensuring privacy, as established in federal legislation, regulations, and OMB guidance.

AT-1.1.2.3 Ensure system information security and privacy training records are documented in support of annual FISMA reporting.

CMS-AT-1 The Program must develop and maintain minimum controls to ensure those with "significant information security and privacy responsibilities"[20] receive adequate role-based training (RBT) [21] to carry out those responsibilities. Through the Program, the CMS CISO must:

CMS-AT-1.1 Ensure initial and periodic information security and privacy RBT is provided for all individuals in roles that possess significant information security and privacy responsibilities, including those that are CMS federal employees, contractors, and subcontractors. CMS RBT must meet or exceed HHS RBT requirements, as follows:[22]

CMS-AT-1.1.1 CMS must identify all personnel (employees and contractors) and their associated work roles with significant information security and privacy responsibilities, in accordance with the HHS Cybersecurity Coding Guide and the National Initiative for Cybersecurity Education (NICE) Framework.[23] The Program will identify appropriate minimum RBT requirements for each identified role with significant information security and privacy responsibilities.

CMS-AT-1.1.2 All CMS employees, including managers, Senior Executive Service (SES) personnel, and contractors who have significant information security and privacy responsibilities, must complete minimum RBT requirements within sixty (60) days from EOD date, or commencement of work on a contract or subcontract. Thereafter, all personnel with significant information security and privacy responsibilities must complete RBT at least annually, on a schedule that will be set out in the RMH.

CMS-AT-1.1.3 Individuals who change roles within CMS such that they assume new significant information security and privacy responsibilities, or who otherwise assume such responsibilities, must complete RBT within 60 days of assuming those new responsibilities. Thereafter, they must complete RBT at least annually.

CMS-AT-1.1.4 All CMS employees and contractors with significant information security and privacy responsibilities who have not completed the required training within the mandated timeframes will have their user accounts disabled until they have met their RBT requirement.

CMS-AT-1.1.5 All companies/vendors contracting with CMS are responsible for ensuring that their personnel who have significant information security and privacy

---

20 Per HHS IS2P Appendix G, "significant security responsibilities (SSR)" are defined as "the responsibilities associated with a given role or position, which, upon execution, could have the potential to adversely impact the security posture of one or more HHS systems [including OpDiv systems]." CMS adopts this definition, and further notes that by extension, "significant information security and privacy responsibilities" will be defined as " the responsibilities associated with a given role or position, which, upon execution, could have the potential to adversely impact the privacy or security posture of one or more HHS or CMS systems."

21 This section supersedes CMS CIO Directive 12-03, *Annual Role-Based Information Security Training Requirements*, and HHS Memorandum, *Requirements for Role-Based Training of Personnel with Significant Security Responsibilities* (HHS Office of the Chief Information Officer, June 28, 2017). It is intended to follow FISMA; OMB Circular A-130, Appendix II, *Security of Federal Automated Information Resources* ; HHS IS2P, Appendix G; and the Office of Personnel Management (OPM), 5 Code of Federal Regulations (CFR) 930.301, *Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems* .

22 CMS RBT policies must meet or exceed the standards of the cited HHS June 28, 2017 Memorandum.

23 Identification of roles must be consistent with current federal guidance, such as NIST SP 800-181, *The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (National Institute of Standards and Technology, August 2017).

responsibilities have training commensurate with their role. Training records must be submitted to CMS upon commencement of work and annually thereafter (or upon request, whichever comes first).

CMS-AT-1.1.6 The CMS CISO, in coordination with the CMS's Training Coordinator(s) and Contracting Officers/Representatives (CO/COR), must track and maintain RBT records for all personnel with significant information security and privacy responsibilities. All training records must be retained consistently with an appropriately selected records retention schedule.

CMS-AT-1.2 Develop appropriate security and privacy RBT for personnel with significant information security and privacy responsibilities in accordance with all relevant federal laws, regulations, and guidelines. The Program may provide such training in the form of CMS- or HHS-approved courses[24] or professional development training,[25] or in other appropriate formats. Personnel may also request approval for external training, such as certificate programs or college courses, to satisfy their RBT requirements.

CMS-AT-1.3 Require personnel wishing to receive credit for any form of RBT taken from an organization external to CMS, in satisfaction of any CMS or HHS training requirement to first seek review and approval from their supervisor (or for contractors, from their employer. The Program may further require personnel to supply information concerning completion of such external programs (such as grade reports or certificates of completion) before providing personnel with credit or acknowledgment for having satisfied the relevant RBT requirement.[26]

CMS-AT-1.4 In addition to periodically identifying all *roles* of personnel that have significant information security and privacy responsibilities, CMS will also periodically identify all *specific individuals* who serve in roles with significant information security and privacy responsibilities. CMS managers are responsible for cooperating with the Program to identify individuals with significant information security and privacy responsibilities, and for ensuring that the personnel they manage are appropriately categorized in their roles. CMS managers will be required to complete this identification process as a CMS personnel needs assessment.

CMS-AT-1.5 Personnel who assume multiple roles must complete at least one training that addresses the unique responsibilities associated with at least one role. CMS managers must also ensure the personnel they manage complete the appropriate minimum RBT requirements in the required timeframes as established within the CMS RMH.

CMS-AT-1.6 The Program may request verification of completion of RBT of all personnel from CMS managers. The Program may require mangers to supply adequate information, for

---

[24] Recommendations for RBT may be found at the Program's Information Security and Privacy Library at this website: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ISPG-Training-Catalog.html

[25] Professional development training is any training providing the student with an advanced understanding in information security or privacy. This includes coursework in support of receiving any advanced degrees.

In addition to any mandated privacy or security training, the Program encourages personnel to leverage training and educational opportunities, including both those offered by CMS and by external organizations, such as briefings, forums, seminars, professional development workshops, conferences, and professional independent reading and research.

each individual completing RBT, to verify the individual's identity, the content of the RBT, and proof of completion of RBT.

AT-2 The Program must provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Awareness and Training family of controls.

4.2.3 Audit and Accountability (AU)

AU-1 The Program must develop and maintain (within the Audit and Accountability family of controls) minimum controls to ensure information system audit records are created, protected, and retained to the extent needed to: (i) enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure the actions of individual information system users can be uniquely traced to those users so that they can be held accountable for their actions. The Program must [48]:

AU-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Audit and Accountability family of controls in the ARS for CMS to:

AU-1.1.1 Identify which events the organization audits, based on a risk assessment and mission/business needs.

AU-1.1.2 Identify and ensure a subset of auditable events applicable to the information system is chosen, based on threat information and risk assessment.

AU-1.1.3 Identify and ensure the rationale is provided for why the list of auditable events is deemed adequate to support incident investigations.

AU-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Audit and Accountability family of controls.

AU-1.3 Ensure audit record content for all CMS system components includes:

- Date and time of the event
- Component of the information system (e.g., software component, hardware component) where the event occurred
- Type of event
- User/subject identity
- Outcome (success or failure) of the event
- Execution of privileged functions

AU-1.4 Ensure audited events are significant and relevant to the information security and privacy needs associated with the information system.

AU-1.4.1 Auditing must be compliant with the Federal Rules of Evidence[27] as published by US Courts.

AU-1.5 Define CMS processes, procedures, and standards for the maintenance and review of audit logs for indications of inappropriate or unusual activity to ensure:

AU-1.5.1 Findings are reported to the designated CMS officials, including system officials with a need to know (e.g., Business Owner, ISSO).

AU-1.5.2 The level of audit review, analysis, and reporting is adjusted when there is a change in risk.

AU-1.5.3 A uniform time and time protocol is implemented across CMS, based on CMS approved sources.

AU-1.6 Ensure audit and accountability policies, processes, procedures, and standards directly support privacy audit and accountability requirements.

AU-1.7 Coordinate information security- and privacy-related audit functions with other entities that require audit information to enhance mutual support and guide the selection of auditable events.

4.2.4 Security Assessment and Authorization (CA)

CA-1 The Program must develop and document a security assessment and authorization control policy governing the assessment and authorization of FISMA systems within the CMS enterprise environment or any systems storing, processing, or transmitting CMS information on behalf of CMS. The Program must [48]:

CA-1.1 Develop and maintain an effective implementation of selected controls and control enhancements within the Security Assessment and Authorization family of security controls in the ARS to:

CA-1.1.1 Perform security assessments on information systems and the environments in which those systems operate as part of (i) initial and ongoing security authorizations, (ii) FISMA annual assessments, (iii) continuous monitoring, and (iv) system development life cycle activities.

CA-1.1.2 Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements.

CA-1.1.3 Develop and submit a POA&M for the information system as a result of any security assessment findings.

CA-1.1.4 Develop an ISCM strategy and implement a program compliant with Federal Rules of Evidence Section 803(6).

CA-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Security Assessment and Authorization family of controls.

[27] The Federal Rules of Evidence can be found at this website: http://www.uscourts.gov/file/rules-evidence

4.2.5 Configuration Management (CM)

CM-1 The CMS Configuration Management Executive must coordinate with the CMS CISO and the Program to document the configuration management processes and procedures to define configuration items at the system and component level (e.g., hardware, software, workstation); monitor configurations; and track and approve changes prior to implementation, including but not limited to flaw remediation, security patches, and emergency changes (e.g., unscheduled changes such as mitigating newly discovered security vulnerabilities, system crashes, replacement of critical hardware components). Baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) must be established and maintained throughout the respective system life cycles, and security configuration settings for information products employed in information systems must be established and enforced. In coordination with the CMS Configuration Management Executive, the Program must [48]:

CM-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Configuration Management family of controls in the ARS to:

CM-1.1.1 Ensure configuration management procedures are consistent with applicable federal laws, executive orders, mandates, directives, regulations, and HHS and CMS policies and standards.

CM-1.1.2 Ensure scheduled changes to networks or systems are authorized prior to implementation and are not permitted outside of the configuration management process.

CM-1.1.3 Monitor system configurations and changes to ensure configuration management processes and procedures are followed.

CM-1.1.4 Evaluate the configuration management process periodically, as specified in the ARS, as part of the required FISMA reporting process to verify adequacy and effectiveness.

Through the Program the CMS CISO, in coordination with the CMS Configuration Management Executive, defines and develops policies to ensure CMS Business Owner/ISOs:

CM-1.1.5 Implement and enforce configuration management controls for all CMS systems and networks.

CM-1.1.6 Develop, document, and maintain a current baseline configuration of each system and the system's constituent components.

CM-1.1.7 Develop, document, and maintain an inventory of the components, both hardware and software, that includes relevant ownership information.

CM-1.1.8 Test, validate, and document proposed changes prior to implementation to assess the impact to the information security and privacy of data.

CM-1.1.9 Ensure systems categorized as "Moderate" or "High" under FIPS 199:

- Retain older versions of baseline configurations as deemed necessary to support rollback

– Maintain a baseline configuration for development and test environments to ensure development and test environments are managed separately from the operational environment

Through the program, the CMS CISO must ensure:

CM-1.1.10 Current (up-to-date) anti-virus (AV) and host-based intrusion detection system (HIDS) applications are included, as appropriate, on systems connected to the CMS network.

CM-1.1.11 AV software is configured to automatically perform periodic virus scanning.

CM-1.1.12 HIDS software is configured to automatically scan all inbound and outbound network traffic.

The CMS Configuration Management Executive must ensure:

CM-1.1.13 All systems and system components adhere to *HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications*.

CM-1.1.14 Appropriate CCBs are created and managed for the review and approval of changes.

CM-1.1.15 Configuration management includes a representative from the system as a member of the CCB. Participation on the CCB is at the Security Control Assessor's discretion. If the ISSO or Security Control Assessor acts as a voting member of the CCB, they must be a federal employee.

CM-1.1.16 Personnel with configuration management responsibilities are trained on CMS configuration management processes.

CM-1.1.17 Change documentation is maintained for no less than 12 months after a change is made.

CM-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Configuration Management family of controls.

CM-1.3 For systems categorized as "High" under FIPS 199, ensure detection of unauthorized information security and privacy relevant configuration changes is incorporated into the incident response capability to ensure events are tracked, monitored, corrected, and available for historical purposes.

4.2.6 Contingency Planning (CP)

CP-1 The Program must develop and maintain the Contingency Planning family of controls to ensure contingency plans for emergency response, backup operations, and disaster recovery for organizational information systems are established, maintained, and effectively implemented. IT Contingency Plans ensure the availability of critical information resources and continuity of operations in emergency situations. The Program must [37, 48]:

CP-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Contingency Planning family of controls in the ARS to:

CP-1.1.1 Work with Business Owners/ISOs to develop and document an IT contingency plan for all information systems in accordance with NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, which documents the following processes and procedures:

- Notification of key personnel
- Activation of the plan
- Recovery of the system
- Reconstitution of the system
- Testing of processes and procedures to ensure the system is fully functional and accessible upon restoration

IT contingency plans must support:

CP-1.1.1.1 Applicable CMS continuity of operations plans (COOP), particularly for information systems supporting the continuity of CMS's essential business functions.

CP-1.1.1.2 Recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

CP-1.1.1.3 Implementation of privacy-applicable requirements to reduce the risk of avoidable information security and privacy incidents and breaches while executing contingency measures.

IT contingency plans, as part of the required FISMA reporting process, must be:

CP-1.1.1.4 Reviewed and updated periodically, as defined in the ARS.

CP-1.1.1.5 Tested periodically, as defined in the ARS.

CP-1.1.2 Ensure systems categorized as "High" or "Moderate" under FIPS 199:

- Implement a transaction recovery system for transaction-based systems
- Perform coordinated contingency testing and/or exercises with organizational elements responsible for related plans

CP-1.1.3 Ensure systems categorized as "High" under FIPS 199 develop an IT contingency plan in coordination with organizational elements responsible for related plans (e.g., incident response).

CP-1.1.3.1 Business Owners/ISOs must develop and document a comprehensive system backup strategy for each system.

CP-1.1.3.1.1 The system backup strategy must document processes to:

- Support the information system recovery
- Store backup copies of the operating system and other critical information system software, as well as copies of the information system inventory, in a physically separate facility or in a fire-rated container not co-located with the operational system
- Meet business continuity needs, including the identified RTO and RPO

CP-1.1.3.1.2 Applicable alternate processing sites must be established that are compliant with FIPS 199 system categorization requirements.

CP-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Contingency Planning family of controls.

CP-1.3 For systems categorized as "High" (or as "Moderate" and supporting essential CMS mission or business functions) under FIPS 199, ensure the CMS Business Owner/ISO establishes and maintains appropriate alternate processing and storage site agreements that require:

CP-1.3.1 Alternate processing sites:

- Be separated from the primary storage site(s) and primary processing site(s)
- Identify potential accessibility problems to the alternate processing site(s) and outline explicit mitigation actions
- Ensure information security measures equivalent to those of the primary processing site(s) are provided
- Be configurable for use as an operational site

CP-1.3.2 Alternate storage sites:

- Be separated from the primary storage site(s)
- Identify potential accessibility problems to the alternate storage site(s) and outline explicit mitigation actions
- Ensure information security measures equivalent to those of the primary storage site(s) are provided

4.2.7 Identification and Authentication (IA)

IA-1 The Program must develop and maintain the Identification and Authentication family of controls to ensure information system users, processes acting on behalf of users, and devices are identified and the identities authenticated (or verified) as a prerequisite to allowing access to information systems. Through the Program, the CISO must [48]:

IA-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Identification and Authorization family of controls in the ARS to:

IA-1.1.1 Establish policy and procedures for the effective implementation of selected security controls and control enhancements in the IA control family.

IA-1.1.2 Ensure policy and procedures reflect applicable federal laws, executive orders, mandates, directives, regulations, and HHS and CMS policies and standards.

IA-1.1.3 Ensure the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) and the organizations meet all the requirements specified by HHS policy and applicable implementation standard(s).

IA-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Identification and Authentication family of controls.

IA-1.3 Ensure all users, including federal employees, contractors, and entities with network access to systems, use multi-factor authentication. External facing applications must offer consumers multi-factor authentication as an option [48].

4.2.8 Incident Response (IR)

IR-1 The Program must develop and maintain the Incident Response family of controls to establish an operational incident handling capability for information systems that includes preparation, detection, analysis, containment, recovery, and user response activities. Incidents must be tracked, documented, and reported. The Program must [14, 18, 48]:

IR-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Incident Response family of controls in the ARS to:

IR-1.1.1 Document, maintain, and communicate policies and procedures in accordance with the *HHS Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response* and the *HHS Policy for Responding to Breaches of PII*, including roles and responsibilities for information security and PII incidents and violation handling.

IR-1.1.2 Ensure CMS and contractor situational awareness through:

IR-1.1.2.1 Receipt of information system security and privacy alerts, advisories, and directives from designated external organizations on an ongoing basis.

IR-1.1.2.2 Generation of internal information security and privacy alerts, advisories, and directives as deemed necessary.

IR-1.1.2.3 Dissemination of information security and privacy alerts, advisories, and directives to personnel (see the ARS for a complementary, CMS-defined process).

IR-1.1.3 Ensure CMS and contractor awareness of privacy-related incidents through:

IR-1.1.3.1 Development and implementation of privacy breach notification and response policies, processes, and standards.

IR-1.1.3.2 Appropriate notification of the SOP for all incidents involving PII or PHI.

IR-1.1.4 Ensure CMS and contractors maintain incident response processes and procedures by:

IR-1.1.4.1 Reviewing and updating Incident Response Plans periodically as defined in the ARS.

IR-1.1.4.2 Testing Incident Response Plans periodically as defined in the ARS.

IR-1.1.4.3 Incorporating lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises.

IR-1.1.5 Ensure CMS and contractors maintain familiarity with incident response processes and procedures through periodic training, as defined in the ARS.

IR-1.2 The CMS CISO, in coordination with the CMS Director of CCIC and Business Owners/ISOs, must establish and maintain an information security and privacy incident and breach response capability that includes preparation, identification, containment, eradication, recovery, and follow-up capabilities to ensure effective recovery from information security and privacy incidents and breaches.

IR-1.2.1 For systems categorized as "Moderate" or "High" under FIPS 199, incident handling activities must be coordinated with contingency planning activities.

IR-1.3 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Incident Response family of controls.

4.2.9 Maintenance (MA)

MA-1 The Program must develop and maintain the System Maintenance family of controls to ensure (i) periodic and timely maintenance on organizational information systems is performed and (ii) effective controls are established for the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. The Program must [6, 28, 48, 5, 52]:

MA-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the System Maintenance family of controls in the ARS to:

MA-1.1.1 Ensure privacy considerations are included in system maintenance policy and procedures, especially when the system contains information subject to the *Privacy Act* and/or HIPAA.

MA-1.1.2 Ensure routine preventative and regular maintenance (including repairs) on the components of all CMS information systems, supporting utilities, and ancillary equipment (e.g., within the data center, used for testing) are scheduled, performed, documented, and reviewed.

MA-1.1.2.1 Maintenance processes and procedures must be compliant with CMS processes and procedures.

MA-1.1.2.2 Maintenance processes and procedures may reference manufacturer or vendor specifications.

MA-1.1.3 Ensure information system maintenance tools are approved, controlled, maintained, and monitored as required.

MA-1.1.4 Ensure only authorized personnel are allowed to perform maintenance on the information system through established processes and procedures.

MA-1.1.4.1 Personnel authorized to perform maintenance must be compliant with requirements defined under the Awareness and Training and Personnel Security sections of this document.

MA-1.1.5 For non-local (e.g., remote) maintenance and diagnostic services ensure:

MA-1.1.5.1 Services are authorized, monitored, and controlled.

MA-1.1.5.2 Tools are consistent with organizational policy and documented in the security plan for the information system.

MA-1.1.5.3 Strong identification and authentication techniques are employed in the establishment of sessions.

MA-1.1.5.4 Activity records are maintained.

MA-1.1.5.5 All sessions and network connections are terminated when non-local maintenance is completed.

MA-1.1.6 Ensure appropriate protection of information systems and/or components being removed:

MA-1.1.6.1 The CMS Business Owner/ISO or designated federal employee must approve removal of information systems and/or system components for offsite maintenance/repairs.

MA-1.1.6.2 The equipment/media must be sanitized in a manner compliant with NIST or Department of Defense (DoD) guidance prior to removal from organizational facilities for offsite maintenance or repairs.

MA-1.1.7 For systems categorized as "Moderate" or "High" under FIPS 199, maintenance records must include:

- Date and time of maintenance
- Name of the individual performing the maintenance
- Name of escort, if necessary
- Description of the maintenance performed
- List of equipment (including components and parts), including the removal and/or replacement of applicable identification numbers

CMS Business Owners/ISOs must:

MA-1.1.7.1 Inspect all maintenance tools carried into a facility by maintenance personnel for improper modifications.

MA-1.1.7.2 Check all media containing diagnostic and test applications and programs for malicious code before the media is used in the information system.

MA-1.1.7.3 Ensure non-local maintenance and diagnostic sessions, including review of the maintenance records of the sessions, are audited by the ISSO.

MA-1.1.7.4 Ensure installation and use of non-local maintenance and diagnostic connections are documented in the security plan for the information system.

MA-1.1.8 For systems categorized as "High" under FIPS 199, CMS Business Owners/ISOs must:

MA-1.1.8.1 Employ automated mechanisms to schedule, conduct, and document any required maintenance and repairs.

MA-1.1.8.2 Produce and maintain up-to-date, accurate, complete, and available records of all maintenance and repair actions that are needed, in process, and completed.

MA-1.1.8.3 Prevent the unauthorized removal of maintenance equipment/media by performing one of the following:

- Verifying there is no CMS sensitive information contained on the equipment/media
- Sanitizing or destroying the equipment/media in a manner compliant with NIST or DoD guidance
- Retaining the equipment/media within the facility
- Documenting the removal of the equipment/media from the facility with an exemption signed by the Business Owner/ISO or designated federal employee

MA-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the System Maintenance family of controls.

4.2.10 Media Protection (MP)

MP-1 The Program must develop and maintain the Media Protection family of controls to ensure information system media containing sensitive information, both digital and non-digital, is protected by (i) limiting access to authorized users and (ii) sanitizing or destroying information system media before disposal or release for reuse. The Program must [28, 48]:

MP-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Media Protection family of controls in the ARS to:

MP-1.1.1 Inform all employees and contractors with potential access to sensitive information, such as PII or PHI, about all policies and procedures to protect any sensitive information residing on the various media types used by CMS.

MP-1.1.2 Ensure procedures exist for protecting information system media during transport, specifically through the use of cryptography and restricting the transport of such media to authorized personnel commensurate with the sensitivity level of the data.

MP-1.1.3 Develop and maintain processes, procedures, and standards to ensure information system media, both digital and non-digital, are properly sanitized and/or disposed of.

MP-1.1.3.1 Ensure sanitization and disposal techniques (i.e., clear, purge, destroy) for digital and non-digital media are in compliance with NIST SP 800-88 Revision 1, *Guidelines for Media Sanitization*,[28] including the media sanitization decision matrix, prior to disposal, release, and transfer of custody for re-use.

[28] Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf .

MP-1.1.4 Ensure all confidential or classified information is sanitized and disposed of in accordance with policy, procedures, and standards established by the National Security Agency (NSA)[29] and DoD.[30]

MP-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Media Protection family of controls.

4.2.11 Physical and Environmental Protection (PE)

Physical controls are important for protecting PII and PHI against unauthorized access, use, and disclosure. Environmental controls can be critical when PII has high availability requirements (e.g., core mission capabilities of an organization rely on consistent and frequent access to PII) [31, 5, 53].

PE-1 The Program must develop and maintain the Physical and Environmental Protection family of controls to ensure physical access to information systems, equipment, and the respective operating environments is limited to authorized individuals. The Program must:

PE-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Physical and Environmental Protection family of controls in the ARS to:

PE-1.1.1 Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals.

PE-1.1.2 Protect the physical plant and support infrastructure for information systems.

PE-1.1.3 Provide supporting utilities for information systems.

PE-1.1.4 Protect against environmental hazards.

PE-1.1.5 Consider the data sensitivity when defining physical and environmental controls for systems.

PE-1.1.6 Maintain an understanding that the sensitivity of information impacts the necessary physical and environmental controls.

PE-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Physical and Environmental Protection family of controls.

4.2.12 Planning (PL)

PL-1 The Program must develop and maintain the Planning family of controls to ensure information security and privacy planning for FISMA systems are performed within the CMS enterprise environment and on any systems storing, processing, or transmitting CMS information on behalf of CMS. The Program must [18, 48, 52]:

[29] NSA Media Destruction Guidance is available at http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance.

[30] DoD 5220.22-M, *National Industrial Security Program Operating Manual* is available at http://www.dss.mil/documents/odaa/nispom2006-5220.pdf .

PL-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Planning family of controls in the ARS to:

PL-1.1.1 Develop, document, and maintain information security and privacy plans for each CMS system and network:

PL-1.1.1.1 Security plans must be in accordance with NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*.

PL-1.1.1.2 Privacy plans must address the privacy requirements for confidentiality, availability, and integrity for the organization and individual information system(s).

PL-1.1.1.3 Business Owners/ISOs must review and update the information security and privacy plans periodically as defined in the ARS or when significant changes[31] occur to the system/network

PL-1.1.2 Develop, document, and maintain an Information Security Architecture to:

PL-1.1.2.1 Document the information security segments of the CMS enterprise architecture in accordance with OMB Circular A-130.

PL-1.1.2.2 Fully integrate information security and privacy into the CMS architecture framework.

PL-1.1.2.3 Provide an architecture framework consistent with HHS's Enterprise Architecture program[32] and based on the taxonomy of the *Federal Enterprise Architecture Framework*.[33]

PL-1.1.3 Review and update the security segments of the CMS enterprise architecture periodically, as defined in the ARS.[34]

PL-1.1.4 Develop, document, and maintain the CMS Acceptable Use standards within the *HHS Rules of Behavior For Use of HHS Information and IT Resources Policy* [15].

PL-1.1.4.1 Privacy requirements must be identified in contracts and acquisition-related documents.

PL-1.1.4.2 CMS employees and contractors (users) must:

PL-1.1.4.2.1 Be informed that the use of CMS IT resources, other than for authorized purposes, is a violation of the *HHS Rules of Behavior for Use of HHS Information and IT Resource Policy* and is grounds for disciplinary action, up to and including removal from federal service, monetary fines, and/or criminal charges, which could result in imprisonment.

---

31 NIST SP 800-37 describes examples of significant changes to an information system that should be reviewed for possible re-authorization.

32 The HHS Enterprise Architecture program can be found at http://www.hhs.gov/ocio/ea/index.html.

33 The OMB Federal Enterprise Architecture Website provides additional guidance.

34 See Federal Enterprise Architecture (FEA) Security and Privacy Profile, Version 3.0, available at https://cio.gov/wp-content/uploads/downloads/2012/09/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf.

PL-1.1.4.2.2 Be prohibited from transmitting sensitive CMS information using any non-CMS approved Internet-based mechanism, including but not limited to personal email, file-sharing, file transfer, and backup services.

PL-1.1.4.2.3 Read and sign the HHS RoB periodically, as defined in the ARS.

PL-1.1.4.3 Personal use of CMS IT resources must comply with *HHS Rules of Behavior for Use of HHS Information and IT Resource Policy*, which governs the appropriate use of CMS IT resources to ensure personal use of those resources does not put CMS data at risk of unauthorized disclosure or dissemination.

PL-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Planning family of controls.

4.2.13 Personnel Security (PS)

PS-1 The Program must develop and maintain the Personnel Security family of controls to ensure (i) CMS information systems employ personnel security controls consistent with applicable laws, executive orders, policies, directives, regulations, standards, and guidelines and (ii) procedures are developed to guide the implementation of personnel security controls. The Program must [31, 48, 5, 54]:

PS-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Personnel Security family of controls in the ARS to ensure:

PS-1.1.1 CMS information systems employ personnel security controls consistent with applicable federal laws, executive orders, mandates, directives, regulations, and HHS and CMS policies and standards.

PS-1.1.2 Processes and procedures are developed to guide the implementation of personnel security controls.

PS-1.1.2.1 Where appropriate, roles that require access to sensitive information (such as PII and PHI) must apply additional personnel security measures.

PS-1.1.3 Individuals occupying positions of responsibility within organizations (i.e., including third-party service providers) are trustworthy and meet established security criteria for the positions of responsibility.

PS-1.1.4 Information and information systems are adequately protected when personnel actions occur such as initial employment, terminations, and transfers.

PS-1.1.5 Formal sanctions for personnel failing to comply with organizational security policies and procedures are employed.

PS-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Personnel Security family of controls.

4.2.14 Risk Assessment (RA)

RA-1 The Program must develop and maintain the Risk Assessment family of controls to [26]:

- Ensure the risk to organizational operations (e.g., mission, functions, image, reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information, is assessed
- Develop, document, implement, and update a risk assessment at least every three years or whenever a significant change occurs to the information system, a change in the threat environment occurs, a significant data breach occurs, or the ATO has expired

The Program must:

RA-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Risk Assessment family of controls as described in the ARS to ensure formal risk assessment processes and policies provide the foundation for protecting sensitive information.

RA-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Risk Assessment family of controls.

4.2.15 System and Services Acquisition (SA)

SA-1 The Program must develop and maintain the System and Services Acquisition family of controls to ensure contracts, especially the Statement of Work (SOW) within the contract, are reviewed for appropriate information security and privacy contracting language specific to the technology or service being acquired. Through the Program, the CMS CISO must [34, 35, 1]:

SA-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the System and Services Acquisition family of controls defined in the ARS to ensure:

SA-1.1.1 Appropriate information security and privacy documentation (i.e., information security and privacy functional requirements/specifications, information security-related and privacy-related documentation requirements, and developmental and evaluation-related assurance requirements) are contractually required for the development or acquisition of new systems.

SA-1.1.2 Appropriate information security and privacy language to protect sensitive information, such as PII and PHI, is contractually required for the development, acquisition, or operation of systems, when applicable.

SA-1.1.3 Documented processes and procedures are developed and implemented effectively to facilitate the acquisition for information security and privacy controls in all system and services acquisitions.

SA-1.1.4 Processes and procedures are consistent with applicable federal laws, executive orders, mandates, directives, regulations, and HHS and CMS policies and standards.

SA-1.1.5 Sufficient resources to adequately protect organizational information systems are allocated by the responsible organization.

SA-1.1.6 System development life cycle processes, as defined under the SDLC, incorporate required information security and privacy considerations.

SA-1.1.7 Software usage and installation restrictions are employed and compliant with CMS policy.

SA-1.1.8 Security specifications, either explicitly or by reference, are included in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal requirements and industry best practices.

SA-1.1.9 Security measures consistent with applicable federal requirements and industry best practices to protect information, applications, and/or services outsourced from the organization are required of third-party vendors and are verified as specified in the ARS.

SA-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the System and Services Acquisition family of controls.

4.2.16 System and Communications Protection (SC)

SC-1 The Program must develop and maintain the System and Communications Protection family of controls to ensure the organization develops, documents, and maintains system and communications protection policy, processes, and procedures. Through the Program the CMS CISO must [48, 55]:

SC-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the System and Communications Protection family of controls in the ARS to ensure CMS Business Owners/ISOs:

SC-1.1.1 Review the *System and Communications Protection Policy* periodically, as defined in the ARS, or when significant changes occur to the system/network.

SC-1.1.2 Protect the system's assets and information while in transmission or at rest with technical controls based on:

- The confidentiality, integrity, and availability of the system
- The sensitivity of information (e.g., PII and PHI) processed or stored by the system

SC-1.1.3 Ensure the information system isolates security functions from non-security functions by means of an isolation boundary compliant with the TRA to:

SC-1.1.3.1 Isolate access and information flow control from non-security functions and from other security functions.

SC-1.1.3.2 Determine if the information system uses underlying hardware separation mechanisms to implement security function isolation.

SC-1.1.3.3 Minimize the number of non-security functions included within the isolation boundary containing security functions by implementing security and privacy functions as:

- Largely independent modules to maximize internal cohesiveness within modules and minimize coupling between modules

- A layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers

SC-1.1.4 Implement information security and privacy controls throughout the SDLC of each system by:

- Implementing usage restrictions based on the potential risk of harm to an information system
- Authorizing, monitoring, and controlling the use of such components within the information system

SC-1.1.5 Operate websites that are within the restrictions stated in federal policies and directives.

SC-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the System and Communications Protection family of controls.

4.2.17 System and Information Integrity (SI)

SI-1 The Program must develop and maintain the System and Information Integrity family of controls to establish and maintain policy and procedures for the effective implementation of selected information security controls and control enhancements. Through the Program, the CMS CISO must [48]:

SI-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the System and Information Integrity family of controls in the ARS to ensure:

SI-1.1.1 Policy, processes, and procedures are consistent with applicable federal laws, executive orders, mandates, directives, regulations, and HHS and CMS policies and standards.

SI-1.1.2 Policy, processes, and procedures are implemented to protect the integrity of systems and information and to meet the *Privacy Act* requirements for protection against any anticipated threats or hazards to the security or integrity of records.

SI-1.1.3 Information and information system flaws are identified, reported, and corrected in a timely manner, as defined within the ARS.

SI-1.1.4 Protection from malicious code is provided at appropriate locations within organizational information systems.

SI-1.1.5 Information system security and privacy alerts and advisories issued are monitored and appropriate action taken in response.

SI-1.1.6 Minimum information security and privacy controls are supplemented, as warranted, based on an assessment of risk and local conditions, including organization-specific security requirements, specific threat information, cost-benefit analysis, and special circumstances.

SI-1.1.7 A monitoring strategy is developed to implement an ISCM program that is compliant with Federal Rules of Evidence Section 803(6).

SI-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness-tracking for the System and Information Integrity family of controls.

4.2.18 Program Management (PM)

PM-1 The Program must develop and maintain the Program Management family of controls to ensure CMS develops an organization-wide information security program and protects the information security plan from unauthorized disclosure and modification. Through the Program, the CMS CISO must [7, 26, 48]:

PM-1.1 Develop and maintain an effective implementation of selected information security and privacy controls and control enhancements in the Program Management family of controls in the ARS to ensure:

PM-1.1.1 Periodic review of the Program Plan as specified in the ARS.

PM-1.1.2 CMS maintains:

PM-1.1.2.1 Information security and privacy policy as an overview of the information security and privacy management controls and common controls.

PM-1.1.2.2 A sound information security program to facilitate a sound and effective privacy program.

PM-1.1.2.3 A privacy program structured to inform the information security program of all privacy-related requirements.

PM-1.1.3 CMS identifies roles, responsibilities, and compliance requirements.

PM-1.1.3.1 CMS must appoint the CISO as the Senior Information Security Officer.

PM-1.1.3.2 CMS must appoint individuals with specific roles and responsibilities.

PM-1.1.4 CMS holds the approved AO accountable for the risk to the operations within CMS, organizational assets, individuals, and the nation.

PM-1.1.5 CMS develops, implements, and maintains a Risk Management Strategy to:

PM-1.1.5.1 Document remediation actions responding to identified risk.

PM-1.1.5.2 Develop and implement a POA&M process to address information security and privacy risks identified in its information systems.

PM-1.1.5.3 Develop and maintain inventory listings of its information systems.

PM-1.1.5.4 Measure the effectiveness of the Program, information security controls, and privacy controls.

PM-1.1.6 CMS develops, implements, and maintains a testing, training, and monitoring program.

PM-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Program Management family of controls.

4.3 Privacy Control Families

Privacy controls implement the privacy protections required by FISMA, the Privacy Act, the HIPAA Privacy Rule, and other federal laws and regulations. Information privacy is distinct from, but highly interrelated with, information security. These interrelations create dependencies that require close coordination and cooperation between the CMS CISO and CMS SOP.

The privacy controls in this subsection provide a structured set of standards based on NIST SP 800-53, revision 4, Appendix J, and are tailored based on best practices. This document will assist the SOP and provide guidance to CMS stakeholders in complying with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

The privacy controls represent CMS's efforts to comply with privacy requirements affecting CMS programs and/or systems that manage PII/PHI.[35] Business Owners of CMS systems, with direction from OIT, must ensure that all applicable information security and privacy assurance controls, whether imposed by an organization or office internal or external to CMS, are appropriately integrated into CMS systems.

The Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to adopt standards regarding the electronic exchange, security, and privacy of PHI. The HIPAA Privacy Rule sets standards with respect to the rights of individuals regarding their PHI, procedures for exercising those rights, and the authorized and required uses and disclosures of such information. CMS's Medicare Fee-for-Service program, also known as "original Medicare," is a HIPAA covered entity. The HHS Office for Civil Rights investigates privacy-related complaints to identify discrimination or violations of the law and acts to correct problems. Therefore, CMS must adhere to the HIPAA Privacy Rule.

4.3.1 Authority and Purpose (AP)

The Authority and Purpose privacy control family addresses the requirements to: (i) identify the legal bases that authorize a particular PII collection or activity that impacts privacy; and (ii) specify in appropriate notices the purpose(s) for which PII is collected [48].

CMS-AP-1 The Program develops and documents an Authority and Purpose control family policy governing the lifespan of PII/PHI. The Program must:

CMS-AP-1.1 Develop and maintain an effective implementation of selected controls and control enhancements within the Authority and Purpose family of privacy controls in the ARS to:

[35] The CMS privacy policies provide high-level policy statements for each of the NIST SP 800-53 Appendix J privacy control families. NIST developed the Appendix J control families to help agencies implement the Fair Information Practice Principles (FIPP) embodied in the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, and OMB policies and memoranda (e.g., M-07-16, M-10-22, M-10-23). The FIPPs (http://www.nist.gov/nstic/NSTIC-FIPPs.pdf) are widely accepted in the United States and internationally as a general framework for privacy and are reflected in other federal and international laws and policies.

CMS-AP-1.1.1 Ensure that each CMS office or component has the legal authority, either under a statute or an executive order, to conduct activities involving the collection, use, and disclosure of PII and PHI.

CMS-AP-1.2 Describe the authority and purpose(s) throughout the lifespan of PII/PHI in its privacy notices.

CMS-AP-1.3 Ensure that the Business Owner publishes and updates Privacy Act Systems of Records Notices (SORN), Privacy Act Notices, and a HIPAA Notice of Privacy Practices that reflect appropriate authority and activities [17].

CMS-AP-1.4 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance and effectiveness tracking for the Authority and Purpose family of privacy controls.

4.3.2 Accountability, Audit, and Risk Management (AR)

The Accountability, Audit, and Risk Management privacy control family enhances public confidence by providing effective controls for governance, monitoring compliance, risk management, and assessment. These controls demonstrate that CMS complies with applicable privacy protection requirements to minimize the overall risk to individual privacy [48].

CMS-AR-1 The Program develops and documents an Accountability, Audit, and Risk Management control family policy providing a comprehensive governance and privacy program supporting organizational accountability for, and a commitment to the protection of, individual privacy. The Program must:

CMS-AR-1.1 Develop and maintain an effective implementation of selected controls and control enhancements in the Accountability, Audit, and Risk Management family of privacy controls in the ARS to:

CMS-AR-1.1.1 Provide organizational accountability for and commitment to the protection of individual privacy. CMS must:

CMS-AR-1.1.1.1 Develop, implement, and maintain an enterprise-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the lifespan of PII by programs and information systems and manage *Privacy Act* systems of records (SOR) in accordance with applicable guidance.

CMS-AR-1.1.1.2 Develop and implement written privacy requirements that are consistent with the HIPAA Privacy Rule, the Privacy Act, and all other authorities that require agencies to conduct privacy-related activities.

CMS-AR-1.1.1.3 Develop and implement CMS privacy performance measures and metrics to evaluate the effectiveness of privacy policies, procedures, and controls and reporting on implementation, efficiency, effectiveness, and impact.

CMS-AR-1.2 Ensure a PIA is conducted on each CMS FISMA system as a method to evaluate inherent privacy risks in accordance with the HHS PIA standard operating procedures.

CMS-AR-1.3 Establish privacy roles and responsibilities for contractors and service providers and include appropriate privacy responsibilities and requirements in their contracts.

CMS-AR-1.4 The SOP or their designee, must ensure a review is conducted every two years of a random sample of agency contracts that provide for the maintenance of a SOR on behalf of CMS to accomplish a CMS function. The review must ensure the wording of each contract makes the provisions of the *Privacy Act* and other appropriate laws and regulations binding on the contractor and their employees in accordance with OMB Circular A-130.

CMS-AR-1.5 CMS will require any person or organization that performs functions or activities that involve the use or disclosure of PHI on behalf of CMS to complete a Business Associate Agreement (BAA). When CMS discloses PHI to a business associate, the Program requires that the parties enter into a contract or agreement that includes BAA language. Examples of functions or activities on behalf of CMS include claims processing, data analysis, and utilization review. The BAA establishes what disclosures of PHI CMS will make to the business associate and whether and to what extent the business associate may use or disclose that PHI. The BAA also provides satisfactory assurance that the business associate will appropriately safeguard the information. Safeguards include administrative, physical, and technical policies and procedures that protect the confidentiality, integrity and availability of data. The BAA also includes clauses addressing how PHI may be used, when and how the business associate must report breaches of PHI and when and how the business associate must return or destroy PHI upon termination of the contract [17].

CMS-AR-1.5.1 Establish privacy RoB based on the HHS *Privacy Act* regulation, 45 CFR 5b Appendix A, *Employee Standards of Conduct*, and require employees and contractors to formally acknowledge the RoB at least annually to ensure any individual with access to CMS computer systems that contain sensitive information abides by the HHS RoB.

CMS-AR-1.5.2 Ensure every CMS employee and CMS contractor that is assigned a CMS User ID completes and signs an "Application for Access to CMS Computer Systems" form.

CMS-AR-1.5.2.1 CMS employees and contractors that have a User ID to access CMS computer systems are required to complete a mandatory information security and privacy training session annually. If this training is not completed, the user's access privileges must be revoked.

CMS-AR-1.5.2.2 Privacy Awareness and Data Dissemination Training must be provided to CMS project officers and other CMS employees who may benefit.

CMS-AR-1.5.2.3 CMS employees and contractor staff must be trained on how to prevent security incidents and privacy breaches and instructed in their roles and responsibilities regarding responding to incidents and breaches when they occur.

CMS-AR-1.5.3 Report to OMB and Congress as required.

CMS-AR-1.5.4 Impose criminal penalties and/or other sanctions on CMS employees (consistent with the CMS Master Labor Agreement) and non-employees, including contractors and researchers, for the following [56]:

CMS-AR-1.5.4.1 Non-compliance with the *Privacy Act*, the *Computer Matching and Privacy Protection Act of 1988*, the HIPAA Privacy Rule, and the requirements established by the Program for the protection of PII and PHI.

CMS-AR-1.5.4.2 Failure to take required steps to prevent a breach from occurring or for failure to take appropriate action upon discovering a breach.

CMS-AR-1.5.4.3 Failure to implement and maintain security and privacy controls for PII, for which an individual is responsible and aware, regardless of whether such action results in the loss of control or unauthorized disclosure of PII [6].

CMS-AR-1.5.5 Expressly state all applicable criminal penalties and/or sanctions in all CMS contracts or agreements with non-CMS employees, contractors, and/or researchers.

CMS-AR-1.4 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness-tracking for the Accountability, Audit, and Risk Management family of privacy controls.

CMS-AR-1.5 Refrain from intimidating, threatening, coercing, discriminating against, or taking retaliatory action against employees or contractors for exercising their rights under the HIPAA Privacy Rule or participating in any process for [17]:

- Filing privacy complaints
- Testifying, assisting, or participating in an investigation
- Conducting a compliance review, proceeding, or hearing related to the HIPAA Privacy Rule or Privacy Act
- Opposing any act or unlawful practice under the HIPAA Privacy Rule or Privacy Act as long as the manner of opposition is reasonable and does not involve a disclosure of PHI not permitted (HIPAA Privacy Rule §164.530(g)(1))

All elements of CMS-AR-1.5 are included in the CMS Master Labor Agreement.

4.3.3 Data Quality and Integrity (DI)

The Data Quality and Integrity privacy control family enhances public confidence that PII collected and maintained by CMS is accurate, relevant, timely, and complete for the purpose for which the information is to be used (i.e., as specified within CMS's public notices). This control family leverages the HHS Data Integrity Board (DIB)[36] to address the computer matching provisions of the *Privacy Act* [48].

CMS-DI-1 The Program must develop and document a Data Quality and Integrity privacy control family policy that ensures compliance with the *Privacy Act* through the collection of accurate, relevant, timely, and complete PII and limiting use of PII to published purposes. The Program must:

CMS-DI-1.1 Develop and maintain an effective implementation of selected privacy controls and control enhancements in the Data Quality privacy controls (within the Data Quality and Integrity privacy control family) in the ARS to:

CMS-DI-1.1.1 Use accurate, relevant, timely, and complete PII to the greatest extent practicable.

CMS-DI-1.1.2 Collect PII directly from the individual to the greatest extent practicable.

[36] See HHS IS2P, control DI-2, *Data Integrity and Data Integrity Board.*

CMS-DI-1.1.3 Provide mechanisms to check for, and correct as necessary, inaccurate or outdated PII no less frequently than specified in the ARS.

CMS-DI-1.1.4 Issue guidelines on ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated PII.

CMS-DI-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Data Quality privacy controls.

CMS-DI-1.3 Develop and maintain an effective implementation of selected privacy controls and control enhancements in the Data Integrity and DIB privacy controls (within the Data Quality and Integrity privacy control family) in the ARS to:

CMS-DI-1.3.1 Document processes to ensure the integrity of PII.

CMS-DI-1.3.2 Leverage the HHS DIB to approve CMAs and ensure that those agreements comply with the computer matching provisions of the *Privacy Act*.

CMS-DI-1.4 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Data Quality and Integrity privacy controls.

CMS-DI-1.5 Prior to any disclosure of PII or PHI, the Business Owner must [17]:

CMS-DI-1.5.1 Authenticate the identity of a person requesting PII/PHI and, as appropriate, the authority of any such person permitted access to PII/PHI.

CMS-DI-1.5.2 Treat a personal representative the same as the individual with respect to uses and disclosures of the individual's PII/PHI as well as the individual's rights under the HIPAA Privacy Rule.

CMS-DI-1.5.3 Obtain any documentation, statements, or representations, as appropriate, whether oral or written, from the authorized person requesting the PII/PHI.

4.3.4 Data Minimization and Retention (DM)

This privacy control family helps implement the CMS data minimization and retention requirements to collect, use, disclose, create, and retain only PII/PHI that is relevant and necessary for the purpose for which it was originally collected. CMS only retains PII/PHI for as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a NARA-approved record retention schedule. The Program must develop and document a data minimization and retention control family policy providing data minimization (i.e., compatible use)[37] and retention requirements governing the collection, use, rights of redress, and disclosure of PII. The CMS Business Owner must determine the minimum necessary PII/PHI required to conduct the activity for which the agency is authorized. Where relevant, a COR will work with the CO and the Business Owner to make the determination. The Business Owner must also consult the Privacy Office and the Office of General Counsel, as necessary.

[37] See the definition of routine use at 5 USC § 552a(a)(7).

CMS-DM-1 The Program must [48]:

CMS-DM-1.1 Develop and maintain an effective implementation of selected controls and control enhancements in the Data Minimization and Retention family of privacy controls in the ARS to:

CMS-DM-1.1.1 Identify the minimum PII/PHI elements relevant and necessary to accomplish the defined purpose of collection, use, or disclosure (such as for payment and health care operations purposes) [17].

CMS-DM-1.1.2 For internal uses, develop and implement procedures that limit access and use of PII/PHI based on the specific roles of its workforce to carry out their duties, the categories of PII/PHI to which access is needed, and any conditions under which the workforce needs the PII/PHI to do their jobs [17].

CMS-DM-1.1.3 Retain PII, PHI, and FTI only to fulfill the purpose(s) identified in the SORN or as required by law or governed under an agreement.

CMS-DM-1.1.4 Implement procedures for conducting routine and recurring disclosures and for responding to requests for disclosures that limit the PII/PHI disclosed to that which is the minimum amount reasonably necessary to achieve the intended purpose of the disclosure or request, relying (if such reliance is reasonable under the circumstances) on the precise scope of the requested disclosure to determine the minimum necessary information to be included in the disclosure [17].

CMS-DM-1.1.5 Dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.

CMS-DM-1.1.6 Minimize the use of PII/PHI commensurate with federal law and regulation to protect PII/PHI when it is used for testing, training, or research.

CMS-DM-1.1.7 Limit collection, use, disclosure, and retention of PII/PHI to the minimum elements identified for purposes described in the notice and for which the individual provided consent.

CMS-DM-1.1.8 When requesting PII/PHI from other covered entities, limit the PII/PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made [17].

CMS- DM-1.1.9 Conduct initial evaluation of PII/PHI holdings and review holdings annually to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete and reduce PII holdings to the minimum necessary for the proper performance of the documented CMS function.

CMS- DM-1.1.10 Ensure the evaluation of the impact of PII/PHI when the characteristics of the lifespan have changed.

CMS-DM-2 CMS will enter into a valid data use agreement (DUA), whenever appropriate, to protect LDSs.

CMS-DM-3 CMS will provide methods, procedures, and standards within the RMH to accept requests for LDSs, determine whether to provide an LDS, draft and execute LDSs, and provide appropriate governance and oversight of LDS-related processes.

CMS-DM-3.1 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Data Minimization and Retention family of privacy controls.

4.3.5 Individual Participation and Redress (IP)

The Individual Participation and Redress privacy control family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in CMS decisions that are based on the PII [48].

CMS-IP-1 The Program must develop and document an Individual Participation and Redress control family policy providing individuals active participation in the decision-making process regarding the collection and use of their PII. The Program must:

CMS-IP-1.1 Develop and maintain an effective implementation of selected controls and control enhancements in the Individual Participation and Redress family of privacy controls in the ARS to:

CMS-IP-1.1.1 Provide the means, where feasible and appropriate, for individuals to authorize the lifespan of PII/PHI prior to its collection.

CMS-IP-1.1.1.1 CMS must provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization for the lifespan of PII.

CMS-IP-1.1.1.2 CMS must obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

CMS-IP-1.1.1.3 CMS must ensure individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

CMS-IP-1.1.1.4 Individuals must be informed of any records that are subject to computer matching via notice in the *Federal Register,* and the CMA must be published on the CMS website.

CMS-IP-1.1.2 Provide a process for individuals to have access to their PII as appropriate.

CMS-IP-1.1.2.1 Provide individuals the ability to access PII maintained in its SOR(s) as published in the *Federal Register*.

CMS-IP-1.1.2.2 Publish rules and regulations governing how individuals may request access to records maintained in a *Privacy Act* SOR.

CMS-IP-1.1.2.3 Ensure CMS supports and maintains *Freedom of Information Act*-(FOIA) and *Privacy Act*-compliant processes that allow individuals to petition the agency to determine what personal information is maintained specific to the individual.

CMS-IP-1.1.2.4 Provide individuals the right to access, inspect, and obtain copies of their PII and PHI in a designated record set or in a Privacy Act system of records [59].

CMS-IP-1.1.3 Provide individuals the right to an accounting of disclosures of their PII and PHI by CMS or its business associates [59].

CMS-IP-1.1.3.1 On request of the individual, provide accountings of disclosures for routine uses, as required under the Privacy Act, and defined for each system of records in its SORN.

CMS-IP-1.1.3.2 At the request of the individual, provide accountings of disclosures as required under the HIPAA Privacy Rule, unless an exception provided for under the Privacy Rule applies.

CMS-IP-1.1.3.3 The Program must create procedures to temporarily suspend individuals' rights to an accounting of disclosures, if a health oversight agency or law enforcement official provides a written request for such a suspension that meets specific requirements for the time period specified in the written request.

CMS-IP-1.1.4 Provide a process for individuals to have inaccurate PII or PHI corrected or amended, as appropriate.

CMS-IP-1.1.4.1 CMS must permit correction of data only in cases where CMS is the source of the data.

CMS-IP-1.1.4.2 CMS must direct the individual to return to the source of the information to request corrections where CMS is not the source of data.

CMS-IP-1.1.4.3 CMS must implement additional redress processes to comply with federal regulations.

CMS-IP-1.1.5 Provide a process for receiving and responding to complaints,[38] concerns, or questions from individuals about the organizational privacy practices.

CMS-IP-1.1.6 Establish a process for disseminating corrections or amendments of PII to affected individuals and other authorized users of the PII, such as external information sharing partners, where feasible and appropriate.

CMS-IP-1.2 Provide methods, procedures, and standards within the RMH that facilitate implementation, assurance, and effectiveness tracking for the Individual Participation and Redress family of privacy controls.

CMS-IP-1.3 Require the individual's written authorization for any use or disclosure of PII or PHI, unless that use or disclosure is permitted or required by the HIPAA Privacy Rule or

[38] Complaints are written questions or concerns regarding appropriate collection, use, or disclosure of PII or allegations of harm or violation of privacy requirements filed with CMS. The Office of the Ombudsman is responsible for receiving complaints. The Office triages complaints and works in coordination with the Office of the SOP to address the complaint.

Privacy Act to be disclosed without an authorization. This includes a situation where an individual wants their information shared with a third party [17].

CMS-IP-1.3.1 The Program must not condition payment, enrollment, or benefits eligibility on an individual granting an authorization.

CMS-IP-1.3.2 CMS's authorization form must be written in plain language and contain specific information, such as the PII/PHI to be used or disclosed, the person disclosing and receiving the information, the expiration of the authorization, and description of an individual's right to revoke the authorization in writing.

CMS-IP-1.3.3 The Program must treat a personal representative the same as the individual with respect to uses and disclosures of the individual's PHI and with respect to the individual's rights under the HIPAA Privacy Rule. A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or of the deceased individual's estate.

CMS-IP-1.4 Provide individuals the right to request that the Program restrict uses or disclosures of PII or PHI about the individual [17].

CMS-IP-1.4.1 The Program is not required to agree to any such restriction; however, if the Program agrees to a restriction, then the Program may not use or disclose PHI in violation of such restriction.

CMS-IP-1.4.2 If the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, the Program may use the restricted PHI or may disclose such information to a health care provider to provide such treatment to the individual. If restricted PHI is disclosed to a health care provider for emergency treatment, the Program will request that such health care provider not further use or disclose the PHI.

CMS-IP-2 The Program must provide individuals the right to request and to receive communication of PHI by alternate means or to an alternate location if the individual makes a request in writing. The Program must accommodate all reasonable requests [17].

4.3.6 Security (SE)

The Security privacy control family supplements the security controls to ensure technical, physical, and administrative safeguards are in place to protect PII and PHI collected or maintained by CMS against loss, unauthorized access, or disclosure and to ensure planning and responses to privacy incidents comply with OMB policies and guidance [48, 17]. Policies and procedures to safeguard PII and PHI are created and implemented in accordance with federal requirements and may apply to information in any medium.

CMS-SE-1 The Program must develop and document a Security privacy control family policy providing technical, physical, and administrative safeguards for the protection of PII and an appropriate response to privacy incidents in a manner compliant with mandates and directives. The Program's Security privacy control family policy is documented in Section 4.2 of this Policy. The Program's Security privacy control family details and procedures are documented in the ARS and RMH.

CMS-SE-2 When the Program becomes aware of the use or disclosure of PII/PHI in violation of applicable federal law, and/or in violation of its policies or procedures, by one or more members of its workforce, contractors, or business associates, the Program follows the procedures found in the Risk Management Handbook Incident Response Plan [17].

4.3.7 Transparency (TR)

The Transparency privacy control family ensures that CMS provides public notice of its information practices and the privacy impact of its programs and activities. This family of controls consists of three control areas that implement the *Privacy Act* requirements to provide individuals a Privacy Act Statement[39] at the time PII is collected and to publish a SORN[40] and a notice of privacy policies on CMS websites that are required under Section 208 of the *E-Government Act*[41] [48].

CMS-TR-1 The Program must develop and document a Privacy Notice control policy that provides appropriate notification of privacy practices to individuals so individuals are enabled to make informed decisions when they decide to provide their PII/PHI to CMS (i.e., provide consent). The Program's Privacy Notice control details and procedures are documented in the ARS and RMH. The Program must:

CMS-TR-1.1 Provide public notice through a variety of means, as required by law or policy, including SORNs, PIAs, or a website privacy policy.

CMS-TR-1.2 Provide direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII or on separate forms that can be retained by the individuals.

CMS-TR-1.3 Provide additional forms of notice when appropriate to the circumstances.

---

39 A *Privacy Act* statement informs an individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual, of the following information: (i) the authority which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (ii) the principal purpose or purposes for which the information is intended to be used; (iii) the routine uses which may be made of the information, as published in the SORN; and (iv) the effects on the individual, if any, of not providing all or any part of the requested information. See 5 USC § 552a(e)(3).

40 The establishment or revision of a SORN must be published that informs the public of the existence and character of the system of records. The notice must include the name and location of the system the categories of individuals on whom records are maintained in the system; the categories of records maintained in the system; each routine use of the records contained in the system, including the categories of users and the purpose of such use; the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; the title and business address of the agency official who is responsible for the system of records; the agency procedures whereby an individual can be notified at their request if the system of records contains a record pertaining to them; the agency procedures whereby an individual can be notified at their request how they can gain access to any record pertaining to them contained in the system of records, and how they can contest its content; and the categories of sources of records in the system. See 5 USC § 552a(e)(4).

41 A privacy notice on an agency website must be consistent with section 552a of title 5, United States Code and must include: (i) what information is to be collected; (ii) why the information is being collected; (iii) the intended use of the agency of the information; (iv) with whom the information will be shared; (v) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; (vi) how the information will be secured; and (vii) the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the *Privacy Act*), and other laws relevant to the protection of the privacy of an individual. See e-Government Act of 2001, Section 208(b)(1).

CMS-TR-2 The Program must develop and document a SORN and Privacy Act Statements control policy that provide appropriate transparency, in advance of collection, use, maintenance, or sharing of PII when in a system that meets the statutory definition of a "system of records" under the *Privacy Act*. The Program's SORN and Privacy Act Statements control procedures are documented in the ARS and RMH. The Program must:

CMS-TR-2.1 Publish a SORN and adjudicate all comments received from the public review process prior to collecting PII that will be maintained in a system that meets the statutory definition of "system of records".[42]

CMS-TR-2.2 Publish final SORNs on a centralized website to improve transparency by providing individuals easier access to information about how their PII will be collected, used, maintained, or shared by CMS [6].

CMS-TR-2.3 Ensure use of a website, web measurement and web customization technologies, and third-party websites and applications are implemented as governed by the appropriate federal laws, regulations, and guidance [57, 58, 59, 60].

CMS-TR-3 The Program must develop and document a Dissemination of Privacy Program Information control policy that ensures information about the Privacy Program is readily available to the public to reduce the burden on individuals who want to better understand CMS's privacy practices. The Program's Dissemination of Privacy Program control procedures are documented in the ARS and RMH. The Program must:

CMS-TR-3.1 Provide answers to common privacy questions through an easily accessible forum.

CMS-TR-3.2 Provide publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices, as required in the complaints and feedback process.

CMS-TR-4 The Program must develop and document a Notice of Privacy Practices, as required by the HIPAA Privacy Rule, for all Medicare Fee-for-Service beneficiaries, which defines the uses and disclosures of PII/PHI. The notice must state Medicare's duties to protect privacy and describe the individual's rights, including the right to complain if they believe their privacy rights have been violated [17].

CMS-TR-4.1 The Program provides the individual with the Notice of Privacy Practices in several ways: directly to the individual at the time of enrollment in Medicare; as part of the *Medicare & You Handbook*, which individuals receive annually; and online at Medicare.gov.

CMS-TR-4.2 The Program reviews the Notice of Privacy Practices annually to determine if there are material changes to its uses and disclosures of PII/PHI, the individual's rights, Medicare's legal duties, or other privacy practices stated in the notice. The Program makes all revisions and redistributes the Notice per the HIPAA Privacy Rule.

[42] A system of records is defined under 5 USC § 552a(a)(5). Privacy documentation includes PIAs, SORNs, and CMAs. All SORNs must be published in the *Federal Register* and receive a review and comment within 40 days.

4.3.8 Use Limitation (UL)

The Use Limitation privacy control family ensures that CMS only uses PII either as specified in its public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure the scope of PII use is limited accordingly [48].

CMS-UL-1 The Program must develop and document a Use Limitation control family policy providing the guidelines under which CMS may use PII. The Program's Use Limitation policy is documented in Section 4.1.6 of this Policy. The Program's Use Limitation details and procedures are documented in the ARS and RMH.

CMS-UL-2 The Use Limitation control family policy limits access and use of PII/PHI based on the specific roles of its workforce to carry out their duties, the categories of PII/PHI to which access is needed, and any conditions under which the workforce needs the PII/PHI to do their jobs [17].

CMS-UL-3 The Program uses and discloses PII/PHI without an individual's authorization only as permitted under the HIPAA Privacy Rule and the Privacy Act [17].

CMS-UL-4 For internal uses, the Program develops and implements procedures that limit access and use of PII/PHI based on specific roles of its workforce to carry out their duties, the categories of PII/PHI to which access is needed, and any conditions under which the workforce needs the PII/PHI to do their jobs [17].

CMS-UL-5 The Program may disclose PHI, consistently with the HIPAA Privacy Rule, for the following purposes [17]:

CMS-UL-5.1 Uses and disclosures required by law. The Program is permitted to use and disclose PII/PHI when it is required by law (including statute, regulation, or court orders). The use or disclosure is limited to the requirements of the law.

CMS-UL-5.2 Uses and disclosures for public health activities. The Program may use or disclose PHI for public health activities, including:

- To a public health authority authorized by law to collect or receive PII/PHI for the purposes of preventing or controlling disease, injury, or disability
- To a public health authority or other appropriate government authority, authorized by law to receive reports of child abuse or neglect

CMS-UL-5.3 Disclosures about victims of abuse, neglect, or domestic violence. The Program supports the disclosure of PII/PHI for purposes of victims of abuse, neglect, or domestic violence.

CMS-UL-5.4 Uses and disclosures for health oversight activities. The Program discloses PII/PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

- The health care system

- Government benefit programs for which health information is relevant to beneficiary eligibility
- Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards
- Entities subject to civil rights laws for which health information is necessary for determining compliance

A health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity.

CMS-UL-5.5 The Program discloses PII/PHI in the course of any judicial or administrative proceeding.

CMS-UL-5.6 The Program discloses PII/PHI for law enforcement purposes.

CMS-UL-5.7 In response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court of competent jurisdiction, the Program handles the request as a FOIA request in accordance with HHS policy.

CMS-UL-5.8 The Program discloses PII/PHI about decedents when the Program has the proper documentation necessary to determine the legal relationship of the requester to the decedent, as required by law.

CMS-UL-5.9 The Program discloses PII/PHI for research purposes when the PII/PHI request is approved by the Privacy Board.

CMS-UL-5.10 The Program uses or discloses PII/PHI if the agency believes it is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone the agency believes can prevent or lessen the threat. The Program also discloses to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.

CMS-UL-5.11 The Program uses or discloses PII/PHI for specialized government functions, as appropriate.

CMS-UL-5.12 The Program discloses PII/PHI as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

CMS-UL-6 Under the Privacy Act, the Program may disclose PII if the disclosure is documented as a "routine use" in the relevant SORN [17].

Appendix A. Acronyms

A complete list of this Program's standard acronym definitions can be found in the CMS Risk Management Handbook Volume I Chapter 10, *CMS Risk Management Terms, Definitions, and Acronyms.*

AC	Access Control
ANSI	American National Standards Institute
AO	Authorizing Official
AP	Authority and Purpose
AR	Accountability, Audit, and Risk Management
ARS	Acceptable Risk Safeguards
ASFR	Assistant Secretary for Financial Resources
ATO	Authority to Operate
AT	Awareness and Training
AU	Audit and Accountability
AV	Anti-Virus
BAA	Business Associate Agreement
BAT	Breach Analysis Team
BOD	Binding Operational Directive
CA	Security Assessment and Authorization
CAO	Chief Acquisition Officer
CCB	Change Control Board
CCIC	CMS Cybersecurity Integration Center
CDM	Continuous Diagnostics and Mitigation
CDO	Chief Data Officer
CFACTS	CMS FISMA Controls Tracking System
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CHIP	Children's Health Insurance Program
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CLD	Cloud Computing

CMS IS2P2	CMS Information Systems Security and Privacy Policy
CM	Configuration Management
CMA	Computer Matching Agreements
CMS	Centers for Medicare & Medicaid Services
CMS-CLD	CMS Cloud Computing
CO	Contracting Officer
COO	Chief Operating Officer
COOP	Continuity of Operations
COR	Contracting Officer's Representative
CP	Contingency Planning
CPC	Contingency Planning Coordinator
CPIC	Capital Planning and Investment Control
CRA	Cyber Risk Advisor
CRO	Chief Risk Officer
CTO	Chief Technology Officer
CSIRC	Computer Security Incident Response Center
CSP	Cloud Service Provider
CTI	Cyber Threat Intelligence
DGB	Data Governance Board
DHS	Department of Homeland Security
DI	Data Quality and Integrity
DIB	Data Integrity Board
DM	Data Minimization and Retention
DoD	Department of Defense
DPSSI	Physical Security and Strategic Information
DUA	Data Use Agreement
EPLC	Enterprise Performance Life Cycle
E.O.	Executive Order
EOD	Entry on Duty
FEA	Federal Enterprise Architecture
FedRAMP	Federal Risk and Authorization Management Program

FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standard
FISCAM	Federal Information Systems Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
FOIA	Freedom of Information Act
FTI	Federal Tax Information
GAO	Government Accountability Office
HHS	Department of Health and Human Services
HHSAR	Health and Human Services Acquisition Regulation
HIDS	Host-Based Intrusion Detection System
HIM	Health Insurance Marketplace
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transport Protocol
HVA	High Value Asset
IA	Identification and Authentication
IEC	International Electro Technical Commission
IOC	Indicators of Compromise
IP	Individual Participation and Redress
IR	Incident Response
IRS	Internal Revenue Service
IRT	Incident Response Team
IS2P	HHS Information Systems Security and Privacy Policy
IS2P2	CMS Information Systems Security and Privacy Policy
ISA	Information Sharing Agreement
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner, Information Security Officer, International Standards Organization
ISRA	Information Security Risk Assessment
ISSO	Information System Security Officer
IT	Information Technology

ITIRB	IT Investment Review Board
LDS	Limited Data Set
MA	Maintenance
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
MTD	Maximum Tolerable Downtime
NARA	National Archives and Records Administration
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSL	National Security Letter
O&M	Operations and Maintenance
OA	Office of the Administrator
OAGM	Office of Accounts and Grants Management
OE	Operations Executive
OEDA	Office of Enterprise Data and Analytics
OGAPA	Office of Grants and Acquisition Policy and Accountability
OGC	Office of General Counsel
OIG	Office of the Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OPDIV	Operating Division
OSSI	Office of Security and Strategic Information
PE	Physical and Environmental Protection
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIRT	Privacy Incident Response Team
PIV	Personal Identity Verification
PL	Planning

PM	Program Management
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPSO	Personnel and Physical Security Officer
PS	Personnel Security
RA	Risk Assessment
RBT	Role-Based Training
RMF	Risk Management Framework
RMH	Risk Management Handbook
RoB	Rules of Behavior
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SA	System and Services Acquisition
SA&A	Security Assessment and Authorization
SA&E	Security Architecture and Engineering
SC	System and Communications Protection
SDLC	System Development Life Cycle
SE	Security
SES	Senior Executive Service
SI	System and Information Integrity
SIA	Security Impact Analysis
SOC	Security Operations Center
SOP	Senior Official for Privacy OR, Standard Operating Procedure
SOR	System of Records
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publication
SPMC	Strategic Planning Management Council
SSP	System Security Plan
SSR	Significant Security Responsibilities

TLS	Transport Layer Security
TR	Transparency
TRB	Technical Review Board
TRA	Technical Reference Architecture
UL	Use Limitation
USC	United States Code

Appendix B. Authoritative References, Statutes, Orders, Directives, Policies, and Guidance

Appendix B provides authoritative references and guidance for requirements defined in this document. Subsections are organized according to "level of authority" (e.g., statutes take precedence over federal directives and policies). Each numbered item provides the citation authority for application to the text within the main body of the IS2P2 Policy.

B.1 List of References

This subsection lists the cited authoritative and guidance documentation in the actual order of appearance within the main body of this document.

[1] HHS, *HHS Security and Privacy Language for Information and Information Technology Procurements, Version 2.0,* June 26, 2017.

[2] OMB, *Policy to Require Secure Connections across Federal Websites and Web Services, OMB Memorandum M-15-13,* June 9, 2015.

[3] HHS, *Memorandum, Requirements for Role-Based Training (RBT) of Personnel with Significant Security Responsibilities,* April 19, 2017.

[4] 5 CFR Part 930.301, *Information Systems Security Awareness Training Program,* January 1, 2011.

[5] Pub. L. 104-191, *Health Insurance Portability and Accountability Act of 1996 (HIPAA 1996),* August 21, 1966.

[6] Pub. L. 93-579, *Privacy Act of 1974 (PA 1974),* December 31, 1974.

[7] HHS, *Information Systems Security and Privacy Policy (IS2P), HHS-OCIO-2014-0001,* July 30, 2014.

[8] HHS, *HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII),* June 29, 2017.

[9] CMS, "CMS Risk Management Handbook (RMH), Chapter 08, Incident Response," 16 August 2017. [Online]. Available: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf.

[10] NIST, *Computer Security Incident Handling Guide, NIST SP 800 -61 Revision 2,* August 6, 2012.

[11] HHS, *HHS Continuity of Operations Program Policy,* April 2018.

[12] HHS, *HHS Personnel Security & Suitability Policy,* November 8, 2011.

[13] The White House, *Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization and Protection,* December 17, 2003.

[14] HHS, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response. HHS-OCIO-2010-0004,* April 5, 2010.

[15] HHS, *HHS Rules of Behavior For Use of HHS Information and IT Resources Policy. HHS-OCIO-2018-0004,* July 25, 2018.

[16] FIPS Publication 140-2, *Security Requirements for Cryptographic Modules,* May 25, 2001.

[17] 45 CFR Part 164, *Privacy of Individually Identifiable Health Information.*

[18] OMB, *Management of Federal Information Resources, OMB Circular A-130,* July 27, 2016.

[19] NIST, *A Role-Based Model for Federal Information Technology/Cybersecurity Training, NIST SP 800-16 Revision 1,* March 14, 2014.

[20] CMS, "CMS Risk Management Handbooks (RMH) and Chapters," [Online]. Available: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

[21] HHS, *HHS High Value Asset (HVA) Program Policy, HHS-OCIO-2018,* February 2018.

[22] Pub. L. 113-282, *National Cybersecurity Protection Act of 2014 (NCPA 2014),* December 18, 1974.

[23] CMS, "CMS Information Security Acceptable Risk Safeguards, CMS ARS Version 3.1," November 21, 2017. [Online]. Available: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ARS-31-Publication.zip.

[24] NIST, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST SP 800-137,* September 30, 2011.

[25] OMB, *Enhancing the Security of Federal Information and Information Systems, OMB Memorandum 14-03,* November 18, 2013.

[26] NIST, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy, NIST SP 800-37 Revision 2*, December, 2018.

[27] Pub. L. 113-283, *Federal Information Security Modernization Act of 2014 (FISMA 2014)*, December 18, 2014.

[28] FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information System*, February 2004.

[29] CMS, "CMS Records Retention Policy," [Online]. Available: http://intranet.cms.gov/Component/OSORA/IRMG/RM/Records-Management-Content.html.

[30] OMB, *Preparing for and Responding to a Breach of Personally Identifiable Information, OMB Memorandum 17-12*, January 3, 2017.

[31] IRS, *Internal Revenue Service Publication 1075, Tax Information Security Guidelines*, September 30, 2016.

[32] Pub. L. 93-400, *Office of Federal Procurement Policy Act of 1974 (OFPP '74)*, August 9, 1974.

[33] CMS, *CMS Policy for Information Technology (IT) Investment Management & Governance*, 2007.

[34] 48 CFR, *Federal Acquisition Regulations (FAR)*.

[35] 48 CFR Chapter 3, *Health and Human Services Acquisition Regulation (HHSAR 2010)*, April 26, 2010.

[36] NIST, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, NIST SP 800-53A Revision 4*, December 18, 2014.

[37] NIST, *Contingency Planning Guide for Information Technology Systems, NIST SP 800-34 Revision*, November 11, 2010.

[38] CMS, "CMS Strategy," [Online]. Available: https://www.cms.gov/About-CMS/Agency-Information/CMS-Strategy/Downloads/CMS-Strategy.pdf.

[39] HHS, *Policy for Monitoring Employee Use of HHS IT Resources*, June 26, 2013.

[40] HHS, *OS Policy for Special Monitoring of Employee Use of Information Technology Resources,* November 7, 2013.

[41] FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 9, 2006.

[42] CMS, "CMS Risk Management Handbook (RMH), Chapter 12, Security and Privacy Planning,," 31 January 2017. [Online]. Available: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-12-Security-and-Privacy-Planning.pdf.

[43] CMS, "CMS Risk Management Handbook (RMH), Chapter 04, Security Assessment and Authorization," 19 January 2019. [Online]. Available: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-04-Security-Assessment-and-Authorization.pdf.

[44] HHS, *HHS OCIO Policy for Information Technology (IT) Enterprise Performance Life Cycle (EPLC), HHS-OCIO-2008-0004.001,* October 6, 2008.

[45] OMB, *Federal Cloud Computing Strategy 2011 (Cloud-First 2011),* 2011.

[46] Department of Homeland Security, "DHS Binding Operational Directive (BOD) 18-02, Securing High Value Assets," 7 May 2018. [Online]. Available: https://cyber.dhs.gov/bod/18-02/.

[47] OMB, "M-19-03 Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program, OMB Memorandum M-19-03," 18 December 2018. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf.

[48] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, NIST SP 800-53, Revision 4,* January 22, 2015.

[49] NIST, *An Introduction to Computer Security, NIST SP 800-12 Revision 1,* June 22, 2017.

[50] NIST, *Information Security Handbook: A Guide for Managers, NIST SP 800-100,* March 7, 2007.

[51] Government Accountability Office, *Federal Information Systems Controls Audit Manual (FISCAM),* 2009.

[52] NIST, *Guide for Mapping Types of Information and Information Systems to Security Categories, NIST SP 800-60 Revision 2.*

[53] NIST, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, NIST SP 800-46 Revision 2*, July 29, 2016.

[54] NIST, *Guide to Information Technology Security Services, NIST SP 800-35*, October 9, 2003.

[55] NIST, *Guidelines on Firewalls and Firewall Policy, NIST SP 800-41 Revision 1*, September 9, 2009.

[56] 45 CFR Part 160, *Public Welfare*, 2009.

[57] Pub. L. 105-277, *Children's Online Privacy Protection Act of 1998 (COPPA 1998)*, April 21, 2000.

[58] OMB, *Guidance for Online Use of Web Measurement and Customization Technologies, OMB Memorandum 10-22*, June 25, 2010.

[59] OMB, *Open Government Directive, OMB Memorandum 10-06*, December 8, 2009.

[60] OMB, *Guidance for Agency Use of Third-Party Websites and Applications, OMB Memorandum 10-23*, June 25, 2010.

B.2 Statutes, Orders, Directives, Policies, and Guidance

The following references are organized according to "level of authority" (e.g., statutes have authoritative precedence over federal directives and policies). The number of each item maps uniquely to the cited statute, order, directive, policy, and guidance within the main body of the IS2P2 Policy.

B.2.1 Statutes

Pub. L. 93-579, *Privacy Act of 1974 (PA 1974)*, December 31, 1974.

Pub. L. 93-400, *Office of Federal Procurement Policy Act of 1974 (OFPP '74)*, August 9, 1974.

Pub. L. 104-191, *Health Insurance Portability and Accountability Act of 1996* (HIPAA 1996), August 21, 1966.

Pub. L. 105-277, *Children's Online Privacy Protection Act of 1998 (COPPA 1998)*, April 21, 2000.

Pub. L. 113-282, *National Cybersecurity Protection Act of 2014 (NCPA 2014)*, December 18, 1974.

Pub. L. 113-283, *Federal Information Security Modernization Act of 2014 (FISMA 2014)*, December 18, 2014.

5 CFR Part 930.301, *Information Systems Security Awareness Training Program*, January 1, 2011.

45 CFR Part 160, *Public Welfare*, 2009.

45 CFR Part 164, *Privacy of Individually Identifiable Health Information*.

48 CFR, *Federal Acquisition Regulations (FAR)*.

48 CFR Chapter 3, *Health and Human Services Acquisition Regulation (HHSAR 2010)*, April 26, 2010.

B.2.2 Federal Directives and Policies

The White House, *Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization and Protection*, December 17, 2003.

IRS, *Internal Revenue Service Publication 1075, Tax Information Security Guidelines*, September 30, 2016.

Department of Homeland Security, *DHS Binding Operational Directive (BOD) 18-02, Securing High Value Assets*, May 7, 2018.

Government Accountability Office, *Federal Information Systems Controls Audit Manual (FISCAM)*, 2009.

B.2.3 OMB Policy and Memoranda

Ordered by publication number.

OMB, *Management of Federal Information Resources, OMB Circular A-130*, July 27, 2016.

OMB, *Federal Cloud Computing Strategy 2011 (Cloud-First 2011)*, 2011.

OMB, *Open Government Directive, OMB Memorandum 10-06*, December 8, 2009.

OMB, *Guidance for Online Use of Web Measurement and Customization Technologies, OMB Memorandum 10-22*, June 25, 2010.

OMB, *Guidance for Agency Use of Third-Party Websites and Applications, OMB Memorandum 10-23*, June 25, 2010.

OMB, *Enhancing the Security of Federal Information and Information Systems, OMB Memorandum 14-03*, November 18, 2013.

OMB, *Policy to Require Secure Connections across Federal Websites and Web Services, OMB Memorandum M-15-13*, June 9, 2015.

OMB, *Preparing for and Responding to a Breach of Personally Identifiable Information, OMB Memorandum 17-12*, January 3, 2017.

OMB, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program, OMB Memorandum M-19-03*, December 10, 2018.

B.2.4 Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST) Special Publications (SP)

Ordered by publication number.

FIPS Publication 140-2, *Security Requirements for Cryptographic Modules,* May 25, 2001.

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information System,* February 2004.

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 9, 2006.

NIST, *An Introduction to Computer Security, NIST SP 800-12 Revision 1,* June 22, 2017.

NIST, *A Role-Based Model for Federal Information Technology/Cybersecurity Training, NIST SP 800-16 Revision 1,* March 14, 2014.

NIST, *Contingency Planning Guide for Information Technology Systems, NIST SP 800-34 Revision,* November 11, 2010.

NIST, *Guide to Information Technology Security Services, NIST SP 800 -35,* October 9, 2003.

NIST, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy, NIST SP 800-37 Revision 2,* December, 2018.

NIST, *Guidelines on Firewalls and Firewall Policy, NIST SP 800-41 Revision 1,* September 9, 2009.

NIST, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, NIST SP 800-46 Revision 2,* July 29, 2016.

NIST, *Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, NIST SP 800-53, Revision 4,* January 22, 2015.

NIST, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, NIST SP 800 -53A Revision 4,* December 18, 2014.

NIST, *Guide for Mapping Types of Information and Information Systems to Security Categories, NIST SP 800-60 Revision 2.*

Volume 1: Guide. NIST SP 800-60 Revision 1 (August 1, 2008).
Volume 2: Appendices. NIST SP 800-60 Revision 1 (August 1, 2008).

NIST, *Computer Security Incident Handling Guide, NIST SP 800-61 Revision 2,* August 6, 2012.

NIST, *Information Security Handbook: A Guide for Managers, NIST SP 800 -100,* March 7, 2007.

NIST, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST SP 800-137,* September 30, 2011.

B.2.5 HHS Policy

Ordered by date of release.

HHS, *HHS OCIO Policy for Information Technology (IT) Enterprise Performance Life Cycle (EPLC), HHS-OCIO-2008-0004.001,* October 6, 2008.

HHS, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response. HHS-OCIO-2010-0004,* April 5, 2010.

HHS, *HHS Personnel Security & Suitability Policy,* November 8, 2011.

HHS, *Policy for Monitoring Employee Use of HHS IT Resources,* June 26, 2013.

HHS, *OS Policy for Special Monitoring of Employee Use of Information Technology Resources,* November 7, 2013.

HHS, *Information Systems Security and Privacy Policy (IS2P), HHS-OCIO-2014-0001,* July 30, 2014.

HHS, "*Memorandum, Requirements for Role-Based Training (RBT) of Personnel with Significant Security Responsibilities*," April 19, 2017.

HHS, "*HHS Security and Privacy Language for Information and Information Technology Procurements, Version 2.0*," June 26, 2017.

HHS, "*HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*," June 29, 2017.

HHS, "*HHS High Value Asset (HVA) Program Policy, HHS-OCIO-2018*," February 2018.

HHS, *HHS Continuity of Operations Program Policy,* April 2018.

HHS, *HHS Rules of Behavior For Use of HHS Information and IT Resources Policy. HHS-OCIO-2018-0004,* July 25, 2018.

B.2.6 CMS Policy and Directives

B.2.6.1 Directives, Memorandums, and Policies:

Ordered by date of release.

CMS, *CMS Policy for Information Technology (IT) Investment Management & Governance,* 2007.

B.2.6.2 Directives, Memorandums, and Policies (Available Online):

CMS, "CMS Information Security Acceptable Risk Safeguards, CMS ARS Version 3.1," November 21, 2017. [Online]. Available: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ARS-31-Publication.zip.

CMS, "CMS Records Retention Policy," [Online]. Available: http://intranet.cms.gov/Component/OSORA/IRMG/RM/Records-Management-Content.html .

CMS, "CMS Strategy," [Online]. Available: https://www.cms.gov/About-CMS/Agency-Information/CMS-Strategy/Downloads/CMS-Strategy.pdf .

B.2.6.3 RMH Chapters (Available Online):

CMS, "CMS Risk Management Handbooks (RMH) and Chapters," [Online]. Available: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

CMS, "CMS Risk Management Handbook (RMH), Chapter 04, Security Assessment and Authorization," 19 January 2019. [Online]. Available: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-04-Security-Assessment-and-Authorization.pdf

CMS, "CMS Risk Management Handbook (RMH), Chapter 08, Incident Response," 16 August 2017. [Online]. Available: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf

CMS, "CMS Risk Management Handbook (RMH) Chapter 12, Security and Privacy Planning,," 31 January 2017. [Online]. Available: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-12-Security-and-Privacy-Planning.pdf

B.2.7 Associated CMS Resources

The CMS ISPG Library is available at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/Policies.html. It contains up-to-date policies, procedures, and directives, including those approved after release of this Policy.