Office of the Administrator
Centers for Medicare & Medicaid Services

CMS Policy for Information Security and Privacy

FINAL
Version 2.0
April 11, 2013

Document Number: CMS-OA-POL-SEC01-02.0

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *CMS POLICY FOR INFORMATION SECURITY AND PRIVACY* VERSION 2.0, APRIL 11, 2013

1) This revision replaces the April 12, 2006 issuance of the *CMS Policy for the Information Security* in response to changes in National Institute of Standards and Technology (NIST) Special Publication (SP) mandated by Federal Information Processing Standard (FIPS) 200, and changes to the *HHS-OCIO Policy for Information Systems Security and Privacy* and *HHS-OCIO Policy for Information Systems Security and Privacy Handbook*.

SUMMARY OF CHANGES IN *CMS POLICY FOR INFORMATION SECURITY*, VERSION 1.0, APRIL 12, 2006

1) Baseline Version

(This Page Intentionally Blank)

TABLE OF CONTENTS

(This Page Intentionally Blank)

1 PURPOSE

The Centers for Medicare & Medicaid Service's (CMS') information and information systems are fundamental to our daily operations and future success. We shall implement procedures and controls at all levels to protect the confidentiality and integrity of information stored and processed on our systems, and to ensure that the systems and information are available to authorized persons when required.

2 BACKGROUND

As the agency charged with administering the Medicare, Medicaid, and State Children's Health Insurance Programs; CMS collects, generates and stores financial, health care, and other sensitive information. Most of this information relates to the health care provided to the nation's Medicare and Medicaid beneficiaries, and as such, has access restrictions as required under legislative and regulatory directives. CMS must protect and ensure the security of its information and information systems.

The objective of our information security and privacy policy is to safeguard the confidentiality, integrity, and availability of our information and systems. These terms are defined[1] as follows:

- *Confidentiality* means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

- *Integrity* means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

- *Availability* means ensuring timely and reliable access to and use of information. Loss of availability is the disruption of access to or use of information or an information system.

To accomplish the objectives of the *CMS Policy for Information Security and Privacy*, CMS has established an Enterprise-wide Information Security and Privacy Program based on four pillars:

- *Security and Privacy Policies and Procedures* – to assure that security and privacy policies, standards, guidelines and procedures are developed and remain current and consistent with CMS's business, information, and information system environments.

- *Training and Awareness* – to increase staff awareness of the importance of security, to empower appropriate staff with the skills needed to conduct CMS information security and privacy management activities and to correct unsafe computing practices found in audits.

[1] Defined in 44 U.S.C. 3542 - *Definitions*, available at http://www.gpo.gov/fdsys/search/pagedetails.action;jsessionid=ypcLTxbSt71s1swvjRx24pz3Fy2p7BWMbJXG36vrcq8yp1lpjTgr!151971526!-458388207?browsePath=Title+44%2FChapter+35%2FSubchapter+III%2FSec.+3542&granuleId=USCODE-2009-title44-chap35-subchapIII-sec3542&packageId=USCODE-2009-title44&collapse=true&fromBrowse=true.

- *Security Architecture* – to assure that the information security environment continues to meet business needs and to address new and emerging threats by identifying risks and providing adequate security protection through testing, implementation, and improvement of new and existing security technologies and processes.
- *Security Assessment and Authorization* – to assure that security and privacy risks are identified, appropriate protections are in-place, and security and privacy responsibilities are assigned prior to authorizing system(s) for operation, as well as continuous monitoring thereafter.

3 SCOPE

This *CMS Policy for Information Security and Privacy* applies to all management, users, System Owners/managers, Information Owners/Stewards, system maintainers, system developers, operators, and administrators, including contractors and third parties, of CMS information systems, facilities, communications networks, and information. This policy applies to all information collected or maintained by, or on behalf of, CMS and all information systems used or operated by CMS, by a CMS contractor, or any organization on behalf of CMS.

4 POLICY

All CMS information shall be protected from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction—whether accidental or intentional—in order to maintain confidentiality, integrity, and availability. The security and privacy controls that provide this protection shall meet minimum federal requirements with additional risk-based and business-driven control implementation achieved through a defense-in-depth security structure. Access to all CMS information shall be limited based on a *least-privilege* approach and a *need-to-know* basis. Authorized user access shall be limited to only information necessary for the performance of required tasks.

Information security and privacy is a responsibility shared by senior agency officials, all CMS managers and staff, Business, Information, and System Owners, information technology (IT) professionals, and all other users of CMS information and information systems. CMS shall implement an Information Security Program that provides policies, standards, procedures, and guidance to ensure the protection of our information and information systems. CMS shall develop and maintain the *CMS Policy for the Information Security and Privacy Program* to communicate overall CMS information security and privacy policy and supporting practices, and to assist senior agency officials and Business/Information/System Owners on specific information security and privacy issues, such as management, operational, and technical safeguards.

5 ROLES AND RESPONSIBILITIES

The following entities have responsibilities related to the implementation of this policy:

5.A. CMS Administrator

The CMS Administrator has the overall responsibility for the implementation of an agency-wide information security and privacy program as required by the laws and regulation as directed by the Department of Health and Human Services (HHS) for ensuring compliance with all government-wide legal and policy requirements.

The CMS Administrator shall be responsible for the following duties, in accordance with provisions of the *Federal Information Security Management Act of 2002* (FISMA), Title III of the *E-Government Act of 2002*:

- Providing information security and privacy protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the following:
    - Information collected or maintained by or on behalf of CMS; and
    - Information systems used or operated by CMS, a contractor of CMS, or another organization on behalf of CMS.
- Complying with the requirements of FISMA and HHS-related policies, procedures, standards, and guidelines, including:
    - IT security and privacy requirements promulgated under Office of Management and Budget (OMB) Circular A-130, Appendix III; and
    - IT security and privacy standards and guidelines issued by OMB in accordance with NIST guidance, including Presidential Directives such as Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*.
- Ensuring that information security and privacy management processes are integrated with CMS strategic and operational planning processes;
- Ensuring that senior CMS officials provide information security and privacy for the information and information systems that support the operations and assets under their control;
- Designating a senior CMS official as the CMS Chief Information Officer (CIO), and delegating to the CMS CIO the authority to ensure compliance with the information security requirements imposed on CMS under FISMA;
- Designating a senior CMS official as the CMS Senior Official for Privacy (SOP), and delegating to the CMS SOP the authority to ensure a coordinated, consolidated, and consistent development and implementation of privacy policy across the agency;

- Delegating responsibility and authority for management of CMS information security programs to the CMS CIO;[2]
- Ensuring that CMS has trained personnel sufficiently to assist CMS in complying with the information security and privacy requirements under FISMA and HHS policies; and
- Ensuring that the CMS CIO, in coordination with the SOP and other senior CMS officials, reports annually to the CMS Administrator on the effectiveness of the CMS information security and privacy program, including the progress of any remedial actions.

Policy/Requirements Traceability: FISMA (Title III of the *E-Government Act*); OMB Circular A-130; Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standards for Federal Employees and Contractors*; and *Federal Continuity Directive 1 (FCD 1)*, dated February 2008; HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy* (as amended), Section 5.2.

5.B. CMS Office of Financial Management (OFM)/Chief Financial Officer (CFO)

The responsibilities of the OFM/CFO include, but are not limited to:

- Coordinating CMS's internal controls program to ensure comprehensiveness and to establish responsibility for uniform security level designations for the financial management system according to the guidelines of OMB Circular A-127, *Financial Management Systems*; and
- Targeting/selecting entities to be reviewed per OMB Circular A-123, *Management's Responsibility for Internal Control*, applying risk-based, business-driven logic to maximize the effectiveness of the evaluations.

Policy/Requirements Traceability: HHS-OCIO-2011-0003, Section 5.3; OMB Circular A-127, *Financial Management Systems*; OMB Circular A-123, *Management's Responsibility for Internal Control*; OMB Memorandum M-96-20, *Implementation of the Information Technology Management Reform Act of 1996*; and (Office of Assistant Secretary for Administration and Management (ASAM) and Office of the Assistant Secretary for Resources and Technology (ASRT); *Statement of Organization, Functions, and Delegations of Authority*, 2009).

5.C. CMS Office of Acquisition and Grants Management

The responsibilities of the Office of Acquisition and Grant Management (OAGM) include, but are not limited to:

- Partnering with the CMS CIO, the CMS SOP, and the CMS Chief Information Security Officer (CISO) to develop and implement information security and privacy-related contract clauses for incorporation in all current and future contracts; and

[2] HHS Secretary Memorandum: *Security of Information Technology Systems*, dated November 10, 2009.

[3] As defined by Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization, and Protection*, dated December 17, 2003.

- Ensuring that contracting officers (COs) enforce the requirements of information security and privacy clauses.

Policy/Requirements Traceability: HHS-OCIO-2011-0003, Section 5.4; Federal Acquisition Regulation (FAR); *Health and Human Services (HHS) Acquisition Regulation (HHSAR)*; and Assistant Secretary for Administration and Management [ASAM] and Assistant Secretary for Resources and Technology [ASRT], *Statement of Organization, Functions, and Delegations of Authority*, 2009.

5.D. CMS Office of Operations Management (OOM)

The responsibilities of OOM include, but are not limited to:

- Providing overall leadership for the development, coordination, application, and evaluation of all policies and activities within CMS that relate to physical and personnel security, the security of classified information, and the exchange and coordination of national security-related strategic information with other Federal agencies and the national security community, including national security-related relationships with law enforcement organizations and public safety agencies;
- Ensuring communications security, including secure telecommunications equipment and classified information systems, for the discussion and handling of classified information in support of the detection, defense, and response, in coordination with the CMS CISO and the Computer Security Incident Response Team (CSIRT), to security and privacy vulnerabilities, threats, and incidents;
- Protecting employees and visitors and CMS-owned and -occupied *critical infrastructure*[3];
- Assuring the integration of strategic medical, public health, biomedical and national security information;
- Managing and administering the flow of classified information;
- Coordinating national security information services to all components within the Office of the Administrator (OA); and
- Approving visits by a foreign national to any CMS facility designated as *critical infrastructure*.
- Coordinating with appropriate CMS CIO Points of Contact (POCs) and HHS Office of Security and Strategic Information (OSSI) POCs to ensure background checks are conducted for individuals with significant security responsibilities;
- Notifying the appropriate CMS CIO POC within one business day when CMS personnel are separated from CMS;

[3] As defined by Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization, and Protection*, dated December 17, 2003.

- Ensuring 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;
- Participating at the request of the HHS Computer Security Incident Response Center (CSIRC) and/or the CMS CSIRT in the investigation of Federal employees with regard to security incidents;
- Participating at the request of the HHS Privacy Incident Response Team (PIRT) and/or the CMS Breach Analysis Team (BAT) in the investigation of Federal employees relative to Personally Identifiable Information (PII) and Protected Health Information (PHI) incidents and violations; and
- Notifying the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches, using procedures specified in the CMS *Risk Management Handbook (RMH).*

Policy/Requirements Traceability: *Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Sections 5.6 and 5.30; HHS RoB; (Office for Civil Rights; Delegation of Authority, 2007); HHS Personnel Security/Suitability Handbook, dated February 1, 2005; and HHS OCIO *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response*, dated April 5, 2010.

5.E. Program Executives/Component Heads

The responsibilities of the Program Executives[4] include, but are not limited to:

- Ensuring that at least one Information Systems Security Officer (ISSO) is appointed to represent and manage Program Executives/Component Head interests and perform ISSO responsibilities on behalf of the Program Executives/Component Head;
- Ensuring that systems and data that are critical to the HHS Information Security and Privacy Program's mission receive adequate protection;
- Determining, in coordination with the Information Owner/Business Owner and System Owner, appropriate security controls and identifying resources to implement those controls;
- Coordinating system and data security requirements with information security personnel by adequately delegating system-level security requirements;
- Ensuring that security for each information system is planned, documented, and integrated into the CMS Expedited Life Cycle (XLC) from the information system's initiation phase to the system's disposal phase;
- Ensuring adequate funding is provided to implement security requirements in the CMS XLC for systems that fall within the management authority of the Program Executive;

[4] In some cases, the Program Executive may be the System Owner and/or the Data Owner/Business Owner.

- Accepting reasonable risks, based on recommendations by the HHS CISO, CMS CISO, or ISSO, and approval by the CMS Authorizing Official (AO);
- Notifying the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches, using procedures specified in the RMH; and
- Ensuring that sensitive information and proprietary software is removed from IT equipment including printers, hard drives, and other memory devices prior to those items being offered for disposal or when a transfer of custody occurs.

Policy/Requirements Traceability: *Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Section 5.21; FISMA, FIPS 199.

5.F. Director, CMS Office of Information Services (OIS), and CMS Chief Information Officer (CIO)

The CMS CIO is responsible for the implementation and administration of the CMS Information Security Program. The CIO, with input from CMS component heads, and Business and System Owners, develops and implements additional policies, standards, guidelines and procedures that fully comply with this policy and FISMA, as well as HHS and government-wide security directives. The CIO shall publish and maintain these policies, standards, and guidelines in the *CMS Policy for the Information Security and Privacy Program*[5]. The CIO is the CMS designated AO for all CMS information systems.

The CMS CIO is responsible for the following:

- Reporting quarterly to the HHS CIO on the effectiveness of CMS's information security and privacy program, including the progress of any remedial actions;
- Delegating responsibility and authority for management oversight of CMS information security programs to the CMS CISO;
- Managing internal security reviews of the program business cases, alternatives analyses, and other specific investment documents;
- Managing and certifying an inventory of all current and proposed investments containing an IT component in accordance with the HHS Capital Planning and Investment Control (CPIC) process;
- Ensuring that policies, procedures, and practices are consistent with HHS requirements in order to ensure that systems, programs, and data are secure and protected from unauthorized access that might lead to the alteration, damage, or destruction of automated resources, unintended release of HHS data, and denial of service (DoS);

[5] The *CMS Policy for the Information Security and Privacy Program* is available on the CMS Information Security Web site at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

- Coordinating as the lead, in collaboration with the CMS Senior Official for Privacy (SOP), for ensuring that all employees and contractors comply with HHS and CMS information security and privacy policies;
- Ensuring the establishment of a CSIRT to participate in the investigation, forensics, and resolution of incidents in CMS;
- Establishing, implementing, and enforcing a CMS-wide framework to facilitate an incident response program (including PII and PHI breaches) that ensures proper and timely reporting to HHS;
- Managing an inventory of all major information systems, devices and other items per FISMA requirements and as required by OMB;
- Ensuring mandatory security education and awareness is undertaken by all personnel using, operating, supervising, or managing computer systems;
- Exercising primary responsibility and authority for management of CMS's information security program;[6]
- Serving as one of six primary operational IT infrastructure managers[7] (applies to the CIO for CDC, FDA, IHS, CMS, NIH, and OS). When an HHS Operating Division (OPDIV) CIO performs as a primary operational IT infrastructure manager, he/she is responsible for performing IT risk-management duties. Where an information system relies (or partially relies) on one of the six primary operational IT infrastructures, the associated primary operational IT infrastructure manager(s)[8] must concur with the risk acceptance by also signing the security authorization package as the AO;
- Resolving any disputes from Office of the Inspector General (OIG) reviews and audits at the CMS level, where possible. If disputes cannot be resolved, they shall be escalated to the HHS CIO;[9]
- Performing the *Risk Executive* function for CMS;[10]
- Developing a strategy for the continuous monitoring[11] of security control effectiveness and any proposed or actual changes to the information system and its environment of operation; [12] and

[6] HHS Secretary Memorandum: *Security of Information Technology Systems*, dated November 10, 2009.

[7] Reference HHS Secretary Memorandum: *Security of Information Technology Systems*, dated November 10, 2009 and HHS OCIO Memorandum, *Process Guidance for Security Risk-Based Decisions Involving the Primary Operational. Information Technology Infrastructure Managers*, dated May 13, 2010.

[8] The HHS role of *Primary Operational IT Infrastructure Managers* also maps to the NIST SP 800-37 role of *Common Control Providers* for the applicable IT infrastructure.

[9] HHS OCIO Memorandum: *Resolving Security Audit Disputes* dated May 13, 2010.

[10] Per HHS-OCIO-2011-0003 Section 5.11.11, the OPDIV CIOs perform the OPDIV Risk Executive (function) on behalf of the OPDIV Heads.

[11] The monitoring strategy can be included in the security plan to support the concept of near real-time risk management and ongoing authorization. The approval of the monitoring strategy can be obtained in conjunction with the security plan approval. The monitoring of security controls continues throughout the CMS XLC.

[12] This is the responsibility of the System/Business Owner and/or the CIO as applicable.

- Executing the Risk Management Framework (RMF) tasks as listed in NIST SP 800-37 (as amended) and the *RMH*.

Policy/Requirements Traceability: *Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Section 5.11; OMB Circular A-130; NIST SP 800-37 (as amended) and the CMS RMH; and NIST SP 800-53 (as amended), *Recommended Security Controls for Federal Information Systems*.

As the designated AO for CMS systems and networks, the CIO responsibilities include but are not limited to, the following:

- Determining, through the security authorization process, in collaboration with the CMS CISO, whether to accept residual risks or to implement appropriate risk mitigation countermeasures, based on the analysis provided by the Security Control Assessor (or designee);
- Making the final security authorization decision and signing the authorization decision document;
- Ensuring that sensitive information is protected from unauthorized access in all forms at rest or in transit;
- Maintaining accountability, through the security authorization process, for the security risks associated with information system operations;
- Providing written authorization accepting responsibility and risk for a *specific* operating system or application not in compliance with HHS or CMS minimum standards; [13]
- Determining, based on organizational priorities, the appropriate allocation of resources dedicated to the protection of the information systems supporting the organization's missions and business functions; and
- Approving the continuous monitoring strategy including the set of security controls that are to be monitored on an ongoing basis and the frequency of the monitoring activities.

Policy/Requirements Traceability: *Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Section 5.18; FISMA; OMB Circular A-130; *Clinger-Cohen Act of 1996*; NIST SP 800-37 (as amended) and the CMS RMH; HHS Memorandum: *Security of Information Technology Systems*, dated November 10, 2009 and HHS Memorandum, Pr*ocess Guidance for Security Risk-Based Decisions Involving the Primary Operational, Information Technology Infrastructure Managers*, dated May 13, 2010.

[13] *Specific* risk acceptance is defined as risk and/or weaknesses that have been identified, but not remediated through the formal POA&M process. Each specific risk must be either mitigated through a formal POA&M, or accept through a formal *risk acceptance* process, and approved by the AO or their designate.

As the CMS Risk Executive, with the support of the CMS CISO, the CMS CIO also executes the following responsibilities:

- Ensuring information security and privacy considerations are integrated into programming/ planning/budgeting cycles, enterprise architectures, and acquisition/system development life cycles;
- Ensuring information systems are covered by approved security plans and are authorized to operate;
- Ensuring information security-related activities required across the organization are accomplished in an efficient, cost-effective, and timely manner; and
- Ensuring a centralized reporting process is in place of appropriate information security-related activities.

Policy/Requirements Traceability: *Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Section 5.8; FISMA; OMB Circular A-130; *Clinger-Cohen Act of 1996*; and NIST SP 800-37 (as amended) and the CMS RMH; and HHS Memorandum: *Resolving Security Audit Disputes*, dated May 13, 2010.

5.G. Chief Information Security Officer (CISO)

The CMS CISO[14] shall carry out the CIO's responsibilities under FISMA, have information security duties as his/her primary duty, shall possess professional qualifications to administer CMS information security functions, and shall head an office with the mission and resources to assist in achieving and maintaining organizational compliance with the CMS information security policies, standards and procedures.

The CMS CISO is responsible for the following activities:

- Leading CMS information security programs and promoting proper information security and privacy practices;
- Supporting the CMS SOP as the lead, to integrate Department privacy program initiatives into CMS information security practices, where applicable;
- Supporting the CMS SOP as the lead, in documenting and managing privacy implementation in CMS IT systems;
- Supporting the CMS CIO, CMS SOP, and the HHS CISO in the implementation of the HHS Information Security and Privacy Program;
- Fostering communication and collaboration among CMS's information security and privacy stakeholders to share knowledge and to better understand threats to CMS information;

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

- Providing information about the CMS information security and privacy policies to management and throughout CMS;
- Providing advice and assistance to other organizational personnel concerning the security of sensitive information and of critical data processing capabilities;
- Advising the CMS CIO about information security breaches in accordance with the information security breach reporting procedures developed and implemented by HHS and/or CMS;
- Disseminating information on potential security threats and recommended safeguards;
- Ensuring that roles with significant security responsibilities are identified and documented per HHS Memorandum *Role-Based Training of Personnel with Significant Security Responsibilities*, dated May 16, 2011;
- Conducting information security education and awareness training needs assessments to determine appropriate training resources and to coordinate training activities for target populations;
- Promulgating information security Policy, Standards, and Practices/Procedures through the issuance of the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS)*, and the *CMS Risk Management Handbook (RMH)*;
- Assisting Business Owners in establishing and implementing the required security safeguards to protect computer hardware, software, and data from improper use or abuse;
- Promoting requirements for personnel clearances, position sensitivity, and access to information systems with OOM;
- Ensuring CMS-wide implementation of HHS and CMS policies and procedures that relate to information security and privacy incident response;
- Appointing the CMS Lead for the CMS CSIRT and direct the investigation and resolution of information security and privacy incidents within CMS;
- Coordinating as the lead, and collaborating with the CMS SOP, to ensure privacy implications are addressed when PII and PHI incident response activities occur within CMS;
- Collaborating with the HHS PIRT Coordinator when the PIRT Coordinator is engaging the CMS POC for information collection and clarification, and sitting on the HHS PIRT while CMS breaches are under investigation;
- Supporting general information security and privacy awareness and Role-Based Training (RBT) activities for all personnel using, operating, supervising, or managing information systems;

- Establishing, documenting, and enforcing requirements and processes for granting and terminating all administrative privileges including, but not limited to, servers, security domains, and local workstations. Audit these processes for effectiveness; [15]
- Executing the RMF tasks as listed in NIST SP 800-37 (as amended) and the CMS RMH; and
- Acting as the lead for completion of, in coordination with the CMS Privacy Officer and CMS SOP, the CMS *FISMA and Privacy Management Report* for submission to HHS.

Policy/Requirements Traceability: *Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Section 5.12; FISMA; HHS Memorandum *Role-Based Training of Personnel with Significant Security Responsibilities*, dated May 16, 2011; and HHS Memorandum: *Office of Inspector General Management Implication Report – Need for Departmental Security Enhancements for Information Technology Assets*, dated October 13, 2009.

5.H. CMS Senior Official for Privacy (SOP)

The SOP title was extended by HHS to CMS to meet the reporting requirements outlined in M-08-21, FY 2008 *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. The agency requirement for the title is outlined in M-05-08, *Designation of Senior Agency Officials for Privacy*.

The responsibilities of the CMS SOP include, but are not limited to:

- Supporting the Department CIO/Senior Agency Official for Privacy (SAOP) in ad hoc privacy reporting activities as necessary, including the maintenance of and compliance with presidential mandates and quarterly and annual FISMA reporting activities;
- Reviewing and approving the CMS FISMA and Privacy Management Report for submission to the Department;
- Coordinating as the lead, in collaboration with the CMS CISO, in developing and supporting integration of Department privacy program initiatives into CMS information security practices, where applicable;
- Coordinating as the lead, in collaboration with the CMS CISO, in documenting and managing privacy implementation in CMS IT systems;
- Coordinating as the lead, in collaboration with the CMS CISO, in establishing and implementing privacy policies, procedures, and practices consistent with Department privacy requirements;
- Coordinating CMS policy, guidance, and system-level documentation to ensure that CMS and Department management, technical, and operational privacy requirements are addressed;

[15] From HHS CISO Memorandum to OPDIV CISOs: *Office of Inspector General Management Implication Report – Need for Departmental Security Enhancements for Information Technology Assets*, dated October 13, 2009.

- Approving written requests to process, access, or store PII and PHI from personally owned or non-Department equipment in accordance with *HHS-OCIO Policy for Information Systems Security and Privacy Handbook* Section 2.10 *Personally-Owned Equipment and Software, S-POES.4*, and the CMS ARS;
- Coordinating as the lead, in collaboration with the CMS CISO, to confirm CMS obtains contractual assurances from third parties to ensure that the third party will protect PII and PHI in a manner consistent with the privacy practices of the Department and CMS;
- Reporting, in coordination with the CMS CISO, to the HHS CIO/SAOP the effectiveness of the CMS privacy program, including weaknesses and the progress of remedial actions, as identified;
- Establishing a CMS policy framework to facilitate the development and maintenance of Privacy Impact Assessments (PIAs) for all systems based on department and Federal legislative requirements;
- Tracking and maintaining all CMS PIA activities in the Department's PIA reporting tool;
- Reviewing completed CMS PIAs and attesting that they are adequately and accurately completed;
- Promoting (i.e., escalating) CMS PIAs to the Department, and submitting completed CMS PIAs to the SAOP, or seeking revisions from the PIA author if errors are found;
- Coordinating activities to regularly review PII holdings, assessing the PII confidentiality impact level of the PII holdings, recommending controls to protect the confidentiality of the PII, and eliminating the unnecessary use or collection of PII (including Social Security numbers);
- Coordinating and ensuring that privacy education and awareness activities, specific to the CMS privacy culture, are established for all personnel using, operating, supervising, or managing computer systems;
- Coordinating with CMS budgetary offices to ensure PIA and System of Records Notice (SORN) activities are included as part of Exhibit 300 development;
- Coordinating with the CMS Privacy Act Officer to ensure that all required SORNs are completed and published in the Federal Register, and also on the HHS.gov Website;
- Coordinating with the CMS Privacy Act Officer to:
  - Keep track of the location of Privacy Act records;
  - Approve/deny/track access to and amendments of records;
  - Ensure records are complete, accurate, timely and relevant;
  - Ensure that system users are made aware of their privacy responsibilities when accessing systems that contain personal information; and

  - Ensure data collection forms include a Privacy Act Statement;

- Coordinating with CMS Privacy Act Officer to complete biannual SORN updates in accordance with OMB Circular A-130;
- Coordinating completion of Privacy Act reviews, as defined by OMB Circular A-130, with CMS Privacy Act Officer;
- Coordinating reviews of data sharing activities to ensure they occur according to applicable privacy laws and with appropriate safeguards;
- Making recommendations to the HHS CIO/SAOP and senior level officials with budgetary authority in order to allocate proper resources to identify and mitigate privacy weaknesses found in system PIAs;
- Coordinating with CMS website owners/administrators to ensure that Web-based privacy compliance requirements are met across CMS; and
- Coordinating with CMS' CSIRT and/or HHS PIRT concerning reports of the loss of control of PII and PHI.

Policy/Requirements Traceability: *Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Section 5.16; M-08-21, FY 2008 *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*; M-05-08 and *HHS Policy for Responding to Breaches of Personally Identifiable Information (PII)*, dated November 17, 2008; OMB Circular A-130; *Privacy Act*; FISMA; M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; M-11-02, *Sharing Data While Protecting Privacy*; and NIST SP 800-122, *Guide to Protecting Confidentiality of PII*.

5.I CMS Privacy Act Officer

The CMS Privacy Act Officer responsibilities include:

- Serving as a POC for issues related to the Privacy Act within CMS;
- Coordinating with CMS SOP on development, publishing, and maintenance of CMS SORNs;
- Maintaining a CMS SORN website to post current SORNs per the guidance of the HHS Privacy Act Officer;
- Supporting the CMS SOP and CMS CISO in completing required Privacy Act reviews, as defined by OMB Circular A-130; and
- Supporting completion of the CMS FISMA and Privacy Management Report for submission to the Department.

Policy/Requirements Traceability: *Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Sections 5.17 and 5.34; OMB Circular A-130; *Privacy Act*; and FISMA.

5.J. CMS Data Governance Board (DGB)

The CMS Data Governance Board (DGB) provides executive leadership for developing data management principles and policies that support and improve the operation of CMS' programs. The DGB operates under the auspices of the CMS Office of the Administrator (OA).

The DGB is led by the CMS SOP (or their designate), and is comprised of the executive leadership (director or deputy) of the CMS components that have a direct and substantial programmatic stake in the use of CMS data, including privacy (PII and PHI) and confidentiality. The responsibilities of the DGB include, but are not limited to:

- Provides a forum for executive oversight of the enterprise's data management practices, including data quality, integration, administration, architecture, and warehousing;
- Ensures CMS' business needs and data management practices are aligned with the agency's mission and in compliance with privacy and security protections;
- Clarifies and resolves common data governance challenges, exploring solutions as they relate to privacy, security, trust, and agency compliance issues, including precedent-setting data requests;
- Identifies and oversees priorities that drive the use and disclosure of data in support of agency initiatives;
- Promotes partnership between program stakeholders and the agency's data managers to ensure compatibility with the agency's target enterprise data architecture;
- Oversees the development and implementation of privacy principles that seek a consistent, consolidated, and coordinated approach for the use and disclosure of CMS data;
- Develops criteria to ensure Business Owners and custodians of data are identified and accountable for administering data use and disclosure policies, procedures, and agreements; and
- Ensures CMS data and privacy policies and procedures, including the process for how the agency responds to data requests, are documented, and made available to agency employees and outside requestors.

5.K. CMS Privacy Board

The CMS Privacy Board safeguards PII and PHI, assures that there is minimal privacy risk to an individual when PII and PHI is released to a researcher, and ensures compliance with the *Privacy Act of 1974* and the HIPAA Privacy Rule[16]. The core responsibilities of the CMS Privacy Board include but are not limited to the following:

[16] Including those portions addressed in *The Health Information Technology for Economic and Clinical Health Act (HITECH),* enacted as part of the *American Recovery and Reinvestment Act of 2009.*

- Determining whether the requestor meets the data disclosure provisions contained in the *Privacy Act of 1974* and the provisions of the HIPAA Privacy Rule;
- Determining whether the research needs identifiable data and whether the scope of the study could potentially benefit Medicare beneficiaries or help administer CMS programs;
- Examining the soundness of the research design, the expertise and experience of the investigators, and the adequacy of measures to safeguard the data;
- Applying the existing criteria for data release procedures that are posted on CMS' website;
- Certifying that the researcher's use of PII involves no more than a minimal risk to the privacy of the research subjects, that the research cannot practically be conducted without waiving individual beneficiary authorization, and that the research cannot practicably be conducted without access and use of PII;
- Recommending to the DGB improvements to CMS' data release policies, criteria for releasing PII, and the development of new research databases; and
- Developing procedures that will permit an expedited review process (i.e., review by sub-committee).

5.L. System/Business Owner and Information Owner/Steward

The responsibilities of the System/Business Owners[17] include, but are not limited to:

- Coordinating with the COs and Contracting Officer's Representatives (CORs), Program and Project Officer/Manager, and CISO to ensure that the appropriate security contracting language from the HHS Assistant Secretary for Financial Resources, the HHS Office of Grants and Acquisition Policy and Accountability (ASFR/OGAPA), CMS OAGM, and other relevant sources, are incorporated in each IT contract;
- Signing off that system security designations are appropriately determined prior to system acquisition/procurement in accordance with FIPS 199 security categorization;
- Accepting accountability for the operation of a system(s) in support of the overall HHS Information Security and Privacy Program mission;
- Processing systems at facilities and IT utilities (ITUs) that are certified at a level of security equal to or higher than the security level designated for their system;
- Ensuring that information and system categorization has been established for their system(s) and data in accordance with FIPS 199;
- Determining, in coordination with the Program Executive and Information Owner/Business Owner, appropriate security controls and identifying resources to implement those controls;

[17] The HHS role of *System Owner* maps to the NIST SP 800-37 (as amended) role of *Information System Owner*.

- Consulting with AO, CMS CIO[18], CMS CISO, System Developers and Maintainers, and the Risk Executive (function)[19] when establishing or changing system boundaries;
- Consulting with the CMS CIO or CMS CISO to establish consistent methodologies for determining information security costs for systems;
- Ensuring that security for each information system is planned, documented, and integrated into the CMS XLC from the information system's initiation phase to the system's disposal phase;
- Ensuring provision of adequate funding to implement the security requirements in the CMS XLC for systems that fall within the management authority of the Program Executive;
- Ensuring that security-related documentation at each phase of the CMS XLC meets all identified security needs;
- Ensuring that all IT systems are configured in accordance with most recent Federal system security configuration guidance[20];
- Conducting PIAs on their system(s), in coordination with the CMS SOP, if the system(s) is used to collect information on individuals, or when the Department develops, acquires, or buys new systems to handle collecting PII;
- Conducting assessments of the risk and magnitude of the harm that would result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the Department's critical operations, at no less than every three years or when significant changes occur to the system/network;
- Supporting the annual FISMA program reviews including the annual testing of security controls;[21]
- Ensuring that system weaknesses are captured in the Plan of Action and Milestones (POA&M) and are updated according to the CMS POA&M procedures;
- Ensuring that sensitivity and criticality levels have been established for their systems and data in accordance with NIST standards and guidelines;

[18] The CIOs for CDC, FDA, IHS, CMS, NIH, and OS serve as primary operational IT infrastructure managers.

[19] A *Risk Executive (Function)* is an individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success. [NIST 800-37]

[20] Departmental guidance is posted to the HHS Cyber security Program website located at http://intranet.hhs.gov/infosec/policies_type.html. While the Department has unique security configurations in place for some IT assets, the Department will rely on security configuration guidance from other Federal agencies such as NIST, DISA, and NSA for any HHS assets for which HHS does not have its own Department specific security configuration standard.

[21] Per the previous FISMA OMB reporting guidance, the Department expects annual testing of at least one-third of all security controls for each information system so that all controls are tested every three years in accordance with OMB M-10-15.

- Ensuring proper physical, administrative, and technical controls are in place to protect PII if found in the system;
- Developing security plans for their system(s) and network(s) and documenting the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs);
- Obtaining appropriate interconnection security agreements (ISAs) or memoranda of understanding (MOUs) prior to connecting with other systems and/or sharing sensitive data/ information[22];
- Ensuring that system users and support personnel receive the requisite security training (e.g., instruction in Rules of Behavior [RoB]) and developing system-specific RoBs for systems under their responsibility;
- Participating in Department and CMS-required information security RBT;
- Determining who should be granted access to the system and with what rights and privileges, and granting users the fewest possible privileges necessary for job performance in order to ensure privileges are based on a legitimate need;
- Conducting annual reviews and validations of system users' accounts to ensure the continued need for access to a system;
- Enforcing the concept of separation of duties by ensuring that no single individual has control of the entirety of any critical process;
- Ensuring that special physical security or environmental security requirements are implemented for facilities and equipment used for processing, transmitting, or storing sensitive information based on the level of risk;
- Ensuring the development, execution, and activation of a system-to-system interconnection implementation plan for each instance of a system-to-system interconnection;
- Serving as a POC for the system to whom privacy issues may be addressed;
- Collecting, modifying, using, and/or disclosing the minimum PII necessary to accomplish mission objectives;
- Notifying the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches, using procedures specified in the RMH;

[22] HHS definition of sensitive information is defined in the HHS memorandum *Updated Departmental Standard for the Definition of Sensitive Information* dated May 18, 2009, available at http://intranet.hhs.gov/infosec/policies_type.html. At HHS, sensitive information is information that has a degree of confidentiality such that its loss, misuse, unauthorized access, or modification could compromise the element of confidentiality and thereby adversely affect national health interests, the conduct of HHS programs, or the privacy of individuals entitled under the Privacy Act or the Health Insurance Portability and Accountability Act (HIPAA). IT security personnel and System Owners can equate this definition of sensitive information with data that has a FIPS 199 security impact level of Moderate or High for the confidentiality security objective. This definition of sensitive information is media neutral, applying to information as it appears in either electronic or hardcopy format.

- Ensuring that sensitive information and proprietary software is removed from IT equipment (including printers), hard drives, and other memory devices prior to those items being offered for disposal or when a transfer of custody occurs;
- Accepting accountability for having an active security authorization for all deployed systems to include pilot systems and retiring systems, to include assembling the authorization package and submitting it to the AO or AO's Designated Representative;
- Developing a strategy for the continuous monitoring[23] of security control effectiveness and any proposed or actual changes to the information system and its environment of operation; and
- Executing the RMF tasks as listed in NIST SP 800-37 (as amended) and the RMH.

Policy/Requirements Traceability: *HHS-OCIO Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Section 5.22; FISMA; NIST SP 800-37 (as amended); NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*; Assistant Secretary for Administration and Management [ASAM] and Assistant Secretary for Resources and Technology [ASRT]; *Statement of Organization, Statement of Organization, Functions, and Delegations of Authority, 2009)*.

As the Information Owner/Steward[24], the responsibilities of CMS Business Owners include, but are not limited to:

- Gathering, processing, storing, or transmitting Department data in support of the HHS Information Security and Privacy Program's mission;
- Ensuring that all CMS entities are aware of the sensitivity of data to be handled, and ensuring that data is not processed on a system with security controls that are not commensurate with the sensitivity of the data;
- Notifying the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches, using procedures specified in the RMH; and
- Executing the RMF tasks as listed in NIST SP 800-37 (as amended) and the RMH.

Policy/Requirements Traceability: *HHS-OCIO Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Section 5.23; FISMA, NIST SP 800-16 (as amended).

[23] The monitoring strategy can be included in the security plan to support the concept of near real-time risk management and ongoing authorization. The approval of the monitoring strategy can be obtained in conjunction with the security plan approval. The monitoring of security controls continues throughout the CMS XLC.

[24] The NIST SP 800-37 (as amended) role of Information Owner/Steward may be fulfilled by CMS Data Owner/Business Owner.

5.M. System Developers and Maintainers

The responsibilities of System Developers and Maintainers[25] include, but are not limited to:

- Understanding the need to plan security into information systems, especially from the beginning, and the benefits to be derived from doing so;
- Ensuring that information security-related documentation at each phase of the CMS XLC meets all identified security needs;
- Identifying laws and regulations relevant to the system's design and operation;
- Interpreting applicable laws and regulations into information security functional requirements;
- Evaluating conflicting functional requirements to select for implementing those requirements that provide the highest level of security at the minimum cost consistent with applicable laws and regulations;
- Understanding the relationship between planned information security safeguards and the features being installed on the system under development;
- Evaluating development efforts to ensure that baseline security safeguards are appropriately installed for systems being developed or modified;
- Participating in the construction of the information system in accordance with the formal design specifications, developing manual procedures, using commercial off-the-shelf (COTS) hardware/software components, writing program code, customizing hardware components, and/or using other IT capabilities;
- Designing and developing tests for security safeguard performance under a variety of normal and abnormal operating circumstances and workload levels;
- Analyzing system performance for potential security problems, and providing direction to correct any security problems identified during testing;
- Identifying information security impacts associated with system implementation procedures;
- Leading the design, development, and modification of safeguards to correct vulnerabilities identified during system implementation;
- Supporting assessments, reviews, evaluations, tests and audits of the system by both internal and external entities;
- Following the CMS XLC when developing and maintaining CMS systems;
- Notifying the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches, using procedures specified in the RMH; and

[25] The NIST SP 800-37 (as amended) role of *Information Security Architect* is assigned to CMS *System Developers and Maintainers*.

- Executing the RMF tasks as listed in NIST SP 800-37 (as amended) and the RMH.

Policy/Requirements Traceability: *HHS-OCIO Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Section 5.26; FISMA and NIST SP 800-16 (as amended).

5.N. Information System Security Officer (ISSO)

The responsibilities of each ISSO include, but are not limited to:

- Notifying the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches, using procedures specified in the RMH;
- Serving as a focal point for information security and privacy incident reporting and subsequent resolution;
- Ensuring that information security notices and advisories are distributed to appropriate CMS and contractor personnel and that vendor-issued security patches are expeditiously installed;
- Assisting the CMS CISO in reviewing CMS contracts for systems to ensure that information security is appropriately addressed in contract language;
- Ensuring that information security-related documentation at each phase of the CMS XLC meets all identified security needs;
- Maintaining the security documentation for systems under their purview, according to the NIST SP 800-37 (as amended) and the security requirements of the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS) - CMS Minimum Security Requirements (CMSR)* and the procedures and standards of the CMS *Risk Management Handbook*;
- Ensuring NIST SP 800-53 (as amended) controls are appropriate to the system based on the FIPS 199 security categorization;
- Assisting their applicable System Owner, Information Owner/Business Owner, and CMS CISO in capturing all system weaknesses in the POA&M;
- Reinforcing the concept of separation of duties by ensuring that no single individual has control of any critical process in its entirety per NIST SP 800-53 (as amended);
- Participating in Department and CMS-required information security RBT;
- Tracking all information security education and awareness training conducted for personnel and contractors, as appropriate;
- Assisting the System Owner, Information Owner/Business Owner, and CMS CISO in ensuring that all requirements specified by the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS) - CMS Minimum Security Requirements (CMSR)* and the procedures and standards of the CMS *Risk Management Handbook*, are implemented and enforced for applicable information and information systems;

- Ensuring that the appropriate operational information security posture is maintained for an information system and as such, works in close collaboration with the System Owner;
- Serving as a principal advisor on matters involving the security of an information system; and
- Executing the RMF tasks as listed in NIST SP 800-37 (as amended) and the RMH.

Policy/Requirements Traceability: *HHS-OCIO Policy for Information Systems Security and Privacy* (as amended), HHS-OCIO-2011-0003, Section 5.20; FISMA and NIST SP 800-37 (as amended); NIST SP 800-53 (as amended); FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.

5.O. Federal Employees and Contractors

The responsibilities of the CMS's users and contractors operating on behalf of CMS include, but are not limited to:

- Complying with HHS and CMS policies, standards, and procedures;[26]
- Possessing awareness that they are not acting in an official capacity when using CMS IT resources for non-governmental purposes;
- Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act data, copyright data, and procurement-sensitive information;
- Seeking guidance from supervisors when in doubt about implementing this Policy;
- Ensuring that all media containing CMS data is appropriately marked and labeled to indicate the sensitivity of the data;
- Abstaining from loading unapproved software from unauthorized sources[27] on CMS systems or networks;
- Ensuring that sensitive information is not stored on laptop computers or other portable devices unless the data is secured using encryption standards commensurate with the sensitivity level of the data;
- Reading, acknowledging, signing, and complying with the HHS and CMS RoB, as well as any system-specific RoB, before gaining access to CMS systems and networks;

[26] There are many governing information security documents, directives, procedures, and instructions currently under transition to consolidate into the ARS and RMH. These documents, in addition to the ARS and RMH are all available on the CMS information Security web site at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html. Until these documents are fully integrated into the RMH, this legacy "Virtual Handbook" web site will continue to support other relevant and binding information security procedures and processes.

[27] An unauthorized source is any location (e.g., file store or server to which a device could connect, Internet site, intranet site) or process that is not permitted by HHS or OPDIV/STAFFDIV IT security personnel for the distribution of software.

- Completing required privacy and information security awareness training;
- Implementing specified information security and privacy safeguards to prevent fraud, waste, or abuse of the systems, networks, and data they are authorized to use;
- Conforming to information security policies and procedures that minimize the risk to CMS systems, networks, and data from malicious software and intrusions;
- Agreeing not to disable, remove, install with intent to bypass, or otherwise alter information security or administrative settings designed to protect CMS IT resources;
- Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person, and logging out, locking, or enabling a password-protected screen saver before leaving their workstation; and
- Notifying the CMS CISO of actual or suspected computer-security incidents, including PII and PHI breaches, using procedures specified in the RMH.

Policy/Requirements Traceability: Policy for Information Systems Security and Privacy (as amended), HHS-OCIO 2011 0003, Section 5.32; HHS RoB; NIST SP 800 37 (as amended).

CMS organizational users (CMS employees and contractors) have the responsibility to ensure the protection of CMS' information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction by complying with the information security requirements maintained in this policy, the ARS, and in the *RMH*.

6 APPLICABLE LAWS/GUIDANCE

The following laws and guidance and any officially designated successors are applicable to this policy:

Federal Directives and Policies

- Federal Continuity Directive 1 (FCD 1): *Federal Executive Branch National Continuity Program and Requirements*, February 2008
- HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004
- HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, dated December 17, 2003
- Office of Assistant Secretary for Administration and Management and Office of the Assistant Secretary for Resources and Technology: *Statement of Organization, Functions, and Delegations of Authority*, 74 Fed. Reg. 57679-57682 (2009)
- Office for Civil Rights: *Delegation of Authority*, 74 Fed. Reg. 38630 (2009)

- Office of Resources and Technology: *Statement of Organization, Functions and Delegations of Authority, 73 Fed. Reg. 31486-31487 (2008)*
- Office of the Secretary: *Statement of Organization, Functions, and Delegations of Authority, 72 Fed. Reg. 19000-19001 (2007)*
- Office of Personnel Management (OPM) Regulation 5 *Code of Federal Regulations (CFR) 930.301*
- National Security Presidential Directive (NSPD)-1, February 13, 2001;

Statutes

- *The Health Information Technology for Economic and Clinical Health Act* (HITECH), enacted as part of the *American Recovery and Reinvestment Act of 2009*
- Public Welfare, Title 45 Code of Federal Regulations, Pt. 160. 2009 ed.
- Federal Acquisition Regulation (as amended)
- *Medicare Modernization Act of 2003*, P.L. 108-173;
- *E-Government Act of 2002*
- *Federal Information Security Management Act of 2002* (FISMA) (Pub. L. No. 107-347, Title III)
- *Clinger-Cohen Act of 1996*
- *The Health Insurance Portability and Accountability Act of 1996*
- *Paperwork Reduction Act of 1995*
- *Children's Online Privacy Protection Act of 1998*
- *The Computer Matching and Privacy Protection Act* of 1988
- *The Privacy Act of 1974*, as amended (5 U.S.C. 552a)
- *Office of Federal Procurement Policy Act* of 1974
- *Freedom of Information Act of 1966* (Public Law 89-554, 80 Stat. 383; Amended 1996, 2002, 2007)
- *Federal Records Act of 1950*

HHS Policy

- HHS-OCIO-2011-0003, *Policy for Information Systems Security and Privacy*, dated July 7, 2011.
- HHS-OCIO-2011-0003H, *Policy for Information Systems Security and Privacy Handbook*, dated July 7, 2011.

- HHS-OCIO-2010-0002.001S, *HHS Rules of Behavior For Use of HHS Information Technology Resources*, dated August 26, 2010
- HHS-OCIO-2010-0001.001S, *HHS-OCIO Standard for Security Content Automation Protocol (SCAP)-Compliant Tools*, dated June 8, 2010
- HHS-OCIO-2010-0004, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response*, dated April 5, 2010
- HHS-OCIO-2010-0003.1, *HHS-OCIO Policy for Social Media Technologies*, dated March 7, 2012
- HHS-OCIO-2010-0002, *HHS-OCIO Policy for Information Technology Capital Planning and Investment Control*, dated February 26, 2010
- HHS-OCIO-2010-0001, *HHS-OCIO Policy for Machine-Readable Privacy Policies*, dated January 28, 2010
- HHS-OCIO-2009-0003.001S, *HHS Standard for IEEE 802.11 WLAN*, dated July 27, 2009
- HHS-OCIO-2009-0001.001S, *HHS Standard for Security Configurations Language in HHS Contracts*, dated January 30, 2009
- HHS-OCIO-2009-0002.001S, *HHS Standard for Encryption Language in HHS Contracts*, dated January 30, 2009
- HHS-OCIO-2008-0004.001, *HHS OCIO Policy for Information Technology (IT) Enterprise Performance Life Cycle (EPLC)*, dated October 6, 2008
- HHS-OCIO-2008-0002.002S, *HHS Standard for Managing Outbound Web Traffic*, dated June 6, 2008
- HHS-OCIO-2011-0010.001S, *Standard for Plan of Action and Milestones (POA&M) Management and Reporting*, dated March 30, 2011
- HHS-OCIO-2008-0006.001S, *HHS Standard for FISMA Inventory Management*, dated December 23, 2008
- HHS-OCIO-2008-0007.001S, *HHS Standard for Encryption*, dated December 23, 2008
- HHS-OCIO-2008-0001.003, *HHS Policy for Responding to Breaches of Personally Identifiable Information*, dated November 17, 2008
- HHS-OCIO-2007.0004.001, *Policy for Records Management*, dated January 30, 2008
- HHS-OCIO-2006-0001, *Policy for Personal Use of Information Technology Resources,* dated February 17, 2006
- *HHS CSIRC Concept of Operations*, dated June 9, 2010
- *HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications*, dated May 2, 2012

- *HHS Federal Desktop Core Configuration (FDCC) Deviations*, dated November 5, 2008
- *HHS Federal Desktop Core Configuration (FDCC) Standard for Windows Vista*, dated November 5, 2008
- *HHS Federal Desktop Core Configuration (FDCC) Standard for Windows XP*, dated November 5, 2008
- HHS Memorandum, *Process Guidance for Security Risk-Based Decisions Involving the Primary Operational Information Technology Infrastructure Managers*, dated May 13, 2010
- HHS Memorandum, *Resolving Security Audit Finding Disputes*, dated May 13, 2010
- HHS Memorandum, *Security of Information Technology Systems*, dated November 10, 2009
- HHS Memorandum, *Office of Inspector General Management Implication Report – Need for Departmental Security Enhancements for Information Technology Assets*, dated October 13, 2009
- HHS Memorandum, *Updated Departmental Standard for the Definition of Sensitive Information*, dated May 18, 2009
- HHS Memorandum, *Role-Based Training (RBT) of Personnel with Significant Security Responsibilities*, dated May 16, 2011
- HHS Memorandum, *Security Related to Hosting Foreign Visitors and Foreign Travel by HHS Personnel*, dated April 23, 2004
- 48 CFR Chapter 3 Health and Human Services Acquisition Regulation (HHSAR), dated November 27, 2009
- 48 CFR Chapter 3 Health and Human Services Acquisition Regulation (HHSAR); Corrections, Published and effective on April 26, 2010
- FAC-2005-46, Federal Acquisition Regulation (FAR), amendments dated October 29, 2010
- *Department Information Security Policy/Standard Waiver*, dated July 16, 2010
- *HHS Logistics Management Manual*, dated February 23, 2007
- *HHS Information Security Program Privacy in the System Development Life Cycle*, dated January 16, 2007
- *HHS Memorandum, Federal Information Processing Standards (FIPS) 200 Implementation*, dated January 9, 2007
- *HHS National Security Information Manual*, dated February 1, 2005
- *HHS Personnel Security/Suitability Handbook*, dated February 1, 2005

OMB Policy and Memoranda

- OMB Circular A-127, *Financial Management Systems,* dated January 9, 2009
- OMB Circular A-130, *Management of Federal Information Resources*, dated November 28, 2000
- OMB Circular A-123, *Management Accountability and Control*, dated June 21, 1995
- OMB M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 27, 2012
- OMB FedRAMP Memorandum for Chief Information Officers, *Security Authorization of Information Systems in Cloud Computing Environments*, dated December 8, 2012.
- OMB M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 20, 2011
- OMB M-11-29, *Chief Information Officer Authorities*, dated August 8, 2011
- OMB M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, dated February 3, 2011
- OMB M-11-02, *Sharing Data While Protecting Privacy*, dated November 3, 2010
- OMB M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, dated June 25, 2010
- OMB M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, dated June 25, 2010
- OMB M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated April 21, 2010
- OMB M-10-06, *Open Government Directive*, dated December 8, 2009
- OMB M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated August 20, 2009
- OMB M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated July 14, 2009
- OMB M-08-09, *New FISMA Privacy Reporting Requirements for FY 2008*, dated January 18, 2008
- OMB M-08-10, *Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA)*, dated February 4, 2008
- OMB M-07-20, *FY 2007 E-Government Act Reporting Instructions*, dated August 14, 2007

- OMB M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated July 25, 2007
- OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007
- OMB M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated July 16, 2006
- OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006
- OMB M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006
- OMB M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006
- OMB M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 5, 2005
- OMB M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated June 13, 2005
- OMB M-05-08, *Designation of Senior Agency Officials for Privacy*, dated February 11, 2005
- OMB M-05-04, *Policies for Federal Agency Public Websites*, dated December 17, 2005
- OMB M-04-26, *Personal Use Policies and 'File Sharing' Technology*, dated September 8, 2004
- OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, August 23, 2004;
- OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (as amended)*, dated September 26, 2003
- OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, dated December 16, 2003
- OMB M-01-24, *Reporting Instructions for the Government Information Security Reform Act*, dated June 22, 2001
- OMB M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*, dated December 20, 2000
- OMB Memorandum M-00-07, *Incorporating and Funding Security in Information Systems Investments*, February 28, 2000;
- OMB M-99-20, *Security of Federal Automated Information Resources*, dated June 23, 1999
- OMB M-99-05, *Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records,"* dated January 7, 1999

- OMB M-96-20, *Implementation of the Information Technology Management Reform Act of 1996*, dated April 4, 1996

NIST Guidance

- NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*, dated May 2012
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, dated April 2010
- NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, dated January 2005
- NIST SP 800-64 Revision 2, *Security Considerations in the System Development Lifecycle*, dated October 2008
- NIST SP 800-63 Version 1.0.2, *Electronic Authentication Guideline*, dated April 2006
- NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, dated August 2012
- NIST SP 800-60 Revision 2, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*, dated August 2008
- NIST SP 800-58, *Security Considerations for Voice Over IP Systems*, dated January 2005
- NIST SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans,* dated June 2010
- NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, dated August 2009
- NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, dated February 2010
- NIST SP 800-34 Revision 1, *Contingency Planning Guide for Information Technology Systems*, dated May 2010
- NIST SP 800-30, *Guide for Conducting Risk Assessments*, dated September 2012
- NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, dated February 2006
- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, dated April 1998
- FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* Change Notice 1, dated June 23, 2006

- FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* (Draft update July 2012)
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004
- Federal Information Processing Standards (FIPS), Publication 140-2, *Security Requirements for Cryptographic Modules*, Change Notice 2, December 3, 2002;
- Federal Preparedness Circulars (FPC) 65, June 15, 2004;
- Federal Preparedness Circulars (FPC) 67, April 30, 2001;

CMS Policy and Directives

- *CMS Policy for Investment Management and Governance*, May 17, 2007.

7 EFFECTIVE DATES

This policy supersedes the *CMS Policy for Information Security* dated April 12, 2006, and becomes effective on the date that CMS' Administrator signs it and remains in effect until officially superseded or cancelled by the Administrator.

8 INFORMATION AND ASSISTANCE

Please contact the Chief Information Security Officer, at mailto:CISO@cms.hhs.gov for further information on this policy.

9 APPROVED

\ s \

Marilyn Tavenner
Acting Administrator, CMS

April 11, 2013

Date of Issuance

10 GLOSSARY

The glossary for this document is provided in the below listed document:

- RMH Volume I, Chapter 10, *CMS Risk Management Terms, Definitions, and Acronyms*, and is available on the CMS Information Security Library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

11 ATTACHMENTS

There are no attachments to this policy.

(This Page Intentionally Blank)