Centers for Medicare & Medicaid Services
Information Security and Privacy Group

Risk Management Handbook (RMH)
Chapter 19 Privacy Procedures

Version 1.0

October 25, 2018

Record of Changes

The "Record of Changes" table below capture changes when updating the document. All columns are mandatory.

Version Number	Date	Chapter Section	Author/Owner Name	Description of Change
1.0	10/25/2018	All	CMS ISPG	Publication

Effective Date/Approval

This Procedure becomes effective on the date that CMS's Deputy Chief Information Security Officer signs it and remains in effect until it is rescinded, modified or superseded.

Signature: /S/ Date of Issuance _____

Kevin Allen Dorsey
CMS Deputy Chief Information Security Officer
(DCISO)

Table of Contents

Tables

Figures

1. Introduction

1.1 Purpose

The Centers for Medicare & Medicaid Services (CMS) Risk Management Handbook (RMH) Chapter 19 Privacy provides the procedures for implementing the requirements of the CMS Information Systems Security and Privacy Policy (IS2P2) and the CMS Acceptable Risk Safeguards (ARS). The following is a diagram that breaks down the hierarchy of the IS2P2, ARS, and RMH:

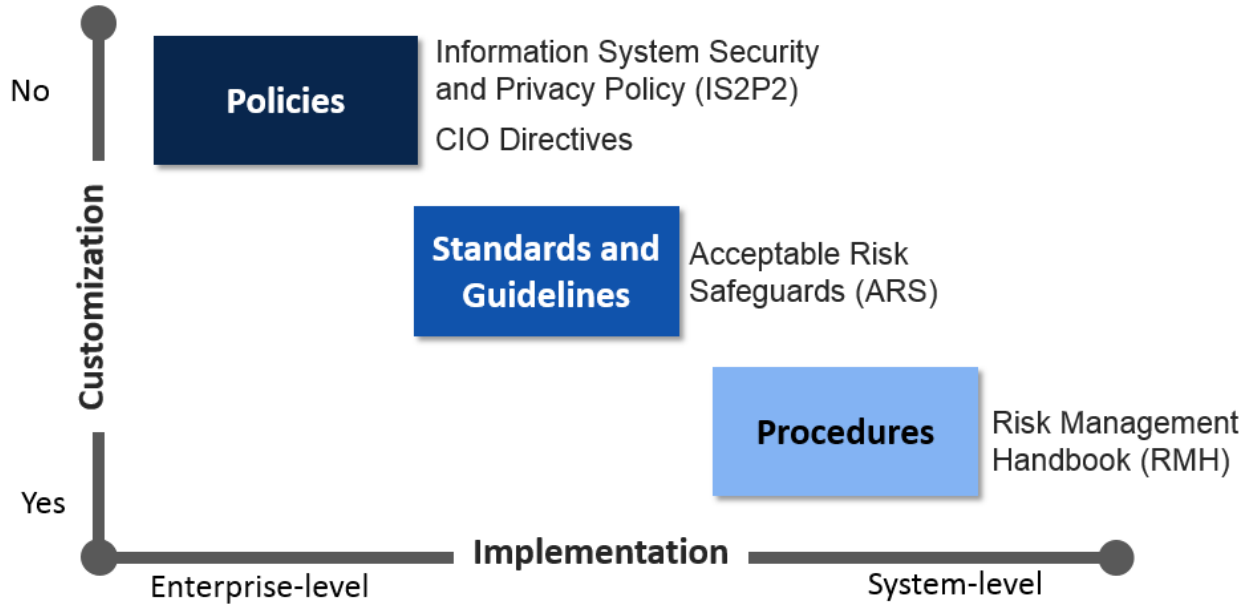


Figure 1: Three-Tiered Hierarchy

This document describes procedures that facilitate the implementation of the privacy family of controls. To promote consistency among all RMH Chapters, CMS intends for Chapter 19 to align with guidance from the National Institute of Standards and Technology (NIST). CMS incorporates the content of NIST's Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations; and NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, into its governance documents, tailoring that content to the CMS environment.

1.2 Authority

The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor. The Federal Information Security Modernization Act of 2014 designates NIST with responsibility to develop guidance to federal agencies on information security and privacy requirements for federal information systems.

As an operating division of the Department of Health and Human Services (HHS), CMS must also comply with the HHS IS2P, Privacy Act of 1974 ("Privacy Act"), the Privacy and Security Rules developed pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the E-Government Act of 2002, which relates specifically to electronic authentication requirements. The HHS Office for Civil Rights (OCR) is responsible for enforcement of the HIPAA Security and Privacy Rules. CMS seeks to comply with the requirements of these authorities, and to specify how CMS implements compliance in the CMS IS2P2.

HHS and CMS governance documents establish roles and responsibilities for addressing privacy and security requirements. In compliance with the HHS Information Systems Security and Privacy Policy (IS2P), the CMS Chief Information Officer (CIO) designates the CMS Chief Information Security Officer (CISO) as the CMS authority for implementing the CMS-wide information security program. HHS also designates the CMS Senior Official for Privacy (SOP) as the CMS authority for implementing the CMS-wide privacy program. Through their authority given by HHS, the CIO and SOP delegate authority and responsibility to specific organizations and officials within CMS to develop and administer defined aspects of the CMS Information Security and Privacy Program.

All CMS stakeholders must comply with and support the policies and the procedures referenced in this handbook to ensure compliance with federal requirements for implementation of information security and privacy controls.

1.3 Scope

This handbook documents procedures that facilitate the implementation of the privacy and security controls defined in the CMS IS2P2 and the CMS ARS. This RMH Chapter provides authoritative guidance on matters related to the Privacy family of controls for use by CMS employees and contractors that support the development, operations, maintenance, and disposal of CMS information systems. This handbook does not supersede any applicable laws, existing labor management agreements, and/or higher-level agency directives or other governance documents.

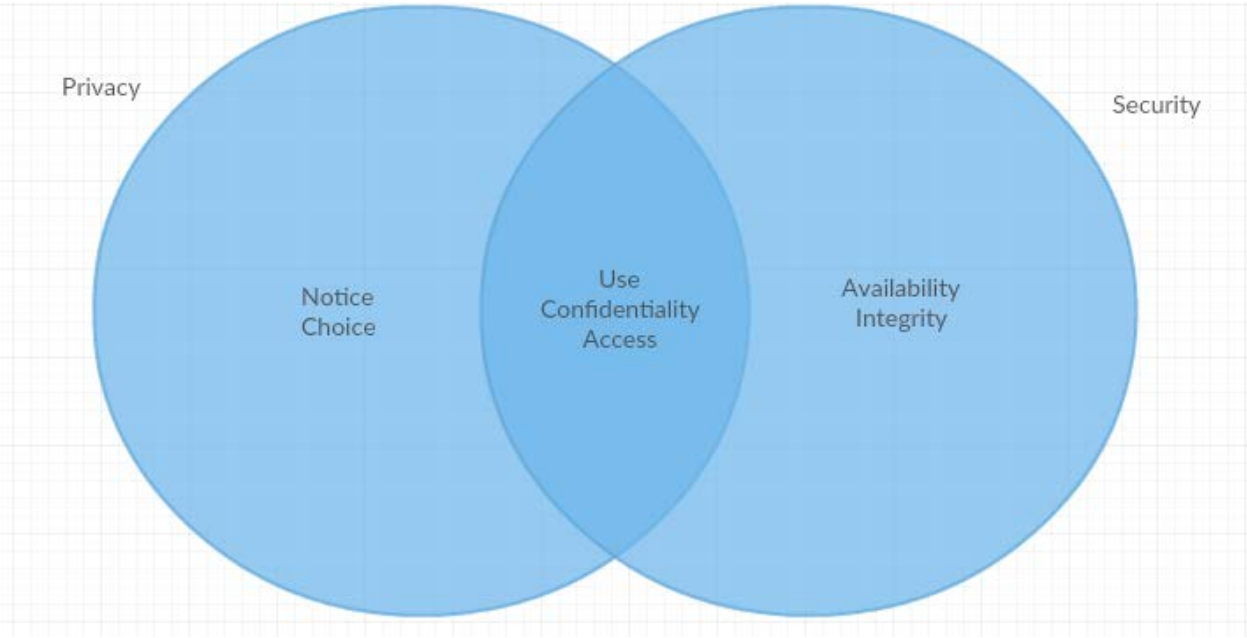


Figure 2: Overlap of Privacy and Security

1.4 Background

This handbook aligns with NIST SP 800-53 catalogue of controls, the CMS IS2P2, and the CMS ARS. Each procedure relates to a specific NIST security control family. Additional sections of this document crosswalk requirements to other control families and address specific audit requirements issued by various sources (e.g., OMB, OIG, HHS, etc.).

RMH Chapter 19 provides processes and procedures to assist with the consistent implementation of the HIPAA Privacy Rule, Privacy Act, and NIST 800-53 Privacy family of controls for any system that stores, processes, or transmits CMS information on behalf of CMS. This chapter identifies the policies, minimum standards, and procedures for the effective implementation of selected security and privacy controls and control enhancements in the RA family.

CMS's comprehensive information security and privacy policy framework includes:

- An overarching policy (CMS IS2P2) that provides the foundation for the security and privacy principles and establishes the enforcement of rules that will govern the program and form the basis of the risk management framework
- Standards and guidelines (CMS ARS) that address specific information security and privacy requirements
- Procedures (RMH series) that assist in the implementation of the required security and privacy controls based upon the CMS ARS standards.

FISMA further emphasizes the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a risk-defined frequency. NIST SP 800-53 states under the Privacy control family that an organization must define, develop, disseminate, review, and update its Privacy documentation at least once every three years. This includes a formal, documented system security package that addresses purpose,

scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented processes and procedures to facilitate the implementation of the Privacy policy and associated controls.

The Risk Assessment process exists within the Risk Management Framework (RMF) which emphasizes:

- Building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls
- Maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes
- Providing essential information to senior leaders to facilitate decisions regarding the mitigation or acceptance of information-systems-related risk to organizational operations and assets, individuals, external organizations, and the Nation.

The RMF[1] has the following characteristics:

- Promotes the concept of near-real-time risk management and ongoing-information-system authorization through the implementation of robust continuous monitoring processes;
- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;
- Integrates information security and privacy protections into the enterprise architecture and eXpedited Life Cycle (XLC);
- Provides guidance on the selection, implementation, assessment, and monitoring of controls and the authorization of information systems;
- Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function); and
- Establishes responsibility and accountability for security and privacy controls deployed within organizational information systems and inherited by those systems (i.e., common controls).

The following table lists the sections of the RMH and the corresponding compliance need that is being met. As one can see, there are a number of controls that meet the compliance requirements of multiple authorities. This table shows how this RMH is designed to be all-inclusive with every privacy requirement that CMS must demonstrate compliance with.

Risk Management Handbook (RMH), Chapter 19 Section	HIPAA Privacy Rule	Privacy Act	HITECH Act	FISMA Control (Appendix J)
3.1 Use and Disclosure	X	X	N/A	X
3.2 Other Permitted Uses and Disclosures	X	X	N/A	X
3.3 Minimum Necessary	X	X	N/A	X

[1] https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final

Risk Management Handbook (RMH), Chapter 19 Section	HIPAA Privacy Rule	Privacy Act	HITECH Act	FISMA Control (Appendix J)
3.4 Verification of Identity	X	X	N/A	X
3.5 Authorization	X	N/A	N/A	X
3.6 Personal Representatives	X	X	N/A	N/A
3.7 Notice of Privacy Practices	X	N/A	X	X
3.8 Individuals' Rights to Access, Inspect, and Obtain	X	X	X	X
3.9 Amendment and Correction of PHI	X	X	X	X
3.10 Accounting of Disclosures	X	X	X	X
3.11 Request for Restrictions	X	N/A	X	N/A
3.12 Confidential Communications	X	N/A	N/A	N/A
3.13 De-Identification of PHI	X	N/A	N/A	X
3.14 Creating a Limited Data Set	X	N/A	N/A	N/A
3.15 Business Associates	X	N/A	X	X
3.16 Breach Notification	X	X	X	X
3.17 Administrative Procedures	X	X	N/A	N/A
4.1.1 Authority to Collect	X	X	N/A	X
4.1.2 Purpose Specification	N/A	X	N/A	X
4.2.1 Governance and Privacy Program	N/A	X	N/A	X
4.2.2 Privacy Impact Assessment	N/A	N/A	N/A	X
4.2.3 Privacy Requirements for Contractors and Service Providers	X	X	X	X
4.2.4 Privacy Monitoring and Auditing	N/A	N/A	N/A	X
4.2.5 Privacy Awareness and Training	X	X	N/A	X
4.2.6 Privacy Reporting	N/A	X	N/A	X
4.2.7 Privacy-Enhanced System Design and Development	N/A	N/A	N/A	X
4.2.8 Accounting of Disclosures	X	X	X	X
4.3.1 Data Quality	N/A	X	N/A	X
4.3.2 Validate PHI	N/A	N/A	N/A	X
4.3.3 Re-Validate PHI	N/A	N/A	N/A	X
4.3.4 Data Integrity and Data Integrity Board	N/A	X	N/A	X
4.3.5 Publish Agreements on Website	X	X	X	X
4.4.1 Minimization of PII	X	X	N/A	X
4.4.2 Locate/Remove/Redact/Anonymize PII	N/A	N/A	N/A	X
4.4.3 Data Retention and Disposal	N/A	X	N/A	X
4.4.4 System Configuration	N/A	N/A	N/A	X
4.4.5 Minimization of PII Used in Testing, Training, and Research	N/A	N/A	N/A	X
4.5.1 Consent	N/A	X	N/A	X
4.5.2 Mechanisms Supporting Itemized or Tiered Consent	N/A	N/A	N/A	X

Risk Management Handbook (RMH), Chapter 19 Section	HIPAA Privacy Rule	Privacy Act	HITECH Act	FISMA Control (Appendix J)
4.5.3 Individual Access	X	X	X	X
4.5.4 Redress	X	X	X	X
4.5.5 Complaint Management	X	X	X	X
4.5.6 Response Times	X	X	N/A	X
4.6.1 Inventory of PII	N/A	N/A	N/A	X
4.6.2 Privacy Incident Response	X	X	X	X
4.7.1 Privacy Notice	X	N/A	X	X
4.7.2 Real-Time or Layered Notice	N/A	N/A	N/A	X
4.7.3 System of Records Notices and Privacy Act Statements	N/A	X	N/A	X
4.7.4 Public Website Publication	X	X	X	X
4.7.5 Dissemination of Privacy Program Information	N/A	N/A	N/A	X
4.8.1 Internal Use	X	X	N/A	X
4.8.2 information Sharing with Third Parties	X	X	X	X

Table 1: Requirements Traceability Matrix

The following graphic is an overview of the information lifecycle:

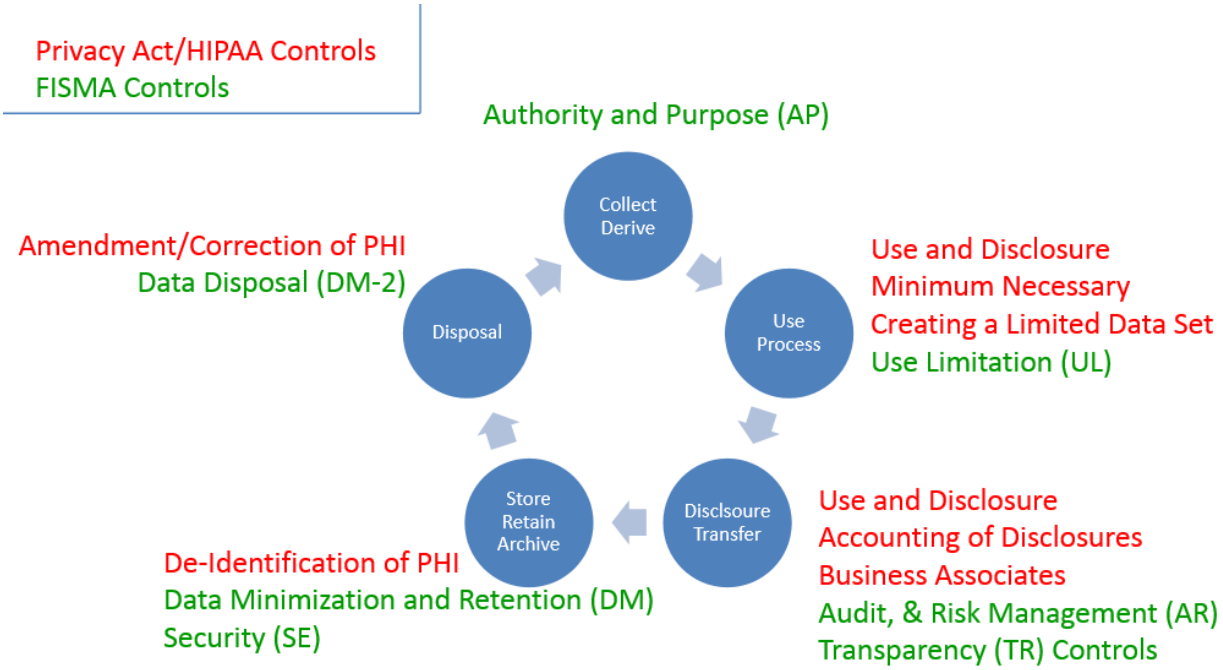


Figure 3: Privacy Controls in the Information Lifecycle

2. Policy

Policy delineates the security management structure, clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress, compliance, and direction to all CMS employees, contractors, and any individual who receives authorization to access CMS information technology (IT) systems or systems maintained on behalf of CMS to assure the confidentiality, integrity, and availability of CMS information and information systems.

2.1 Information Systems Security and Privacy Policy (IS2P2)

The CMS IS2P2[2] defines the framework and policy under which CMS protects and controls access to CMS information and information systems in compliance with HHS policy, federal law, and regulations. This Policy requires all CMS stakeholders to implement adequate information security and privacy safeguards to protect all CMS sensitive information.

[2] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Information-Systems-Security-and-Privacy-Policy-IS2P2.html?DLPage=1&DLEntries=10&DLFilter=is2&DLSort=0&DLSortDir=ascending

The policy contained within the CMS IS2P2 and the procedures contained within this document assist in satisfying the requirements for controls that require CMS to create a policy and associated procedures related to Risk Assessment for information systems.

2.2 Chief Information Officer (CIO) Directives

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 the CMS IS2P2. 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.

The dynamic nature of information security and privacy disciplines and the constant need for assessing risk across the CMS environment can cause gaps in policy, to arise outside of the policy review cycle. The CMS Policy Framework includes the option to issue a CIO Directive[3] to address identified gaps in CMS policy and instruction to provide immediate guidance to CMS stakeholders while a policy is being developed, updated, cleared, and approved.

3. Standards

Standards define both functional and assurance requirements within the CMS security and privacy environment. CMS policy is executed with the objective of enabling consistency across the CMS environment. The CMS environment includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. These components are responsible for meeting and complying with the security and privacy baseline defined in policy and further prescribed in standards. The parameters and thresholds for policy implementation are built into the CMS standards, and provide a foundation for the procedural guidance provided by the Risk Management Handbook series.

3.1 Acceptable Risk Safeguards (ARS)

The CMS Acceptable Risk Safeguards (ARS)[4] provides guidance to CMS and its contractors as to the minimum acceptable level of required security and privacy controls that must be implemented to protect CMS's information and information systems, including CMS sensitive information. The initial selection of the appropriate controls is based on control baselines. The initial control baseline is the minimum list of controls required for safeguarding an IT system based on the organizationally identified needs for confidentiality, integrity, and/or availability.

A different baseline exists for each security category (high, moderate, low) as defined by NIST Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. The ARS provides a catalog of low, moderate, and high controls, in addition to non-mandatory controls outside of the FIPS-199 baseline selection. The ARS, based upon the FIPS 200 and NIST SP 800-53, provides guidance on tailoring controls and enhancements for specific types of missions and business functions,

[3] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/Policies.html

[4] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication.html?DLPage=1&DLEntries=10&DLSort=0&DLSortDir=ascending

technologies, or environments of operation. Users of the ARS may tailor specific mandatory controls as well as most of the non-mandatory and unselected controls.

4. Roles and Responsibilities

A comprehensive list of information security and privacy roles and responsibilities for CMS stakeholders is contained in the CMS IS2P2. The following roles from the CMS IS2P2 are specific to the procedures contained within this RMH chapter.

Role	Applicable Controls
HHS Chief Information Officer (CIO)	AR-1, AR-3, SE-1
HHS Chief Information Security Officer (CISO)	AR-1, SE-1
HHS Office of General Counsel	TR-2
CMS Chief Information Officer (CIO)	AR-1, AR-3, SE-1
CMS Chief Information Security Officer (CISO)	AR-1, SE-1
CMS Information System Security Officer (ISSO)	AR-4
CMS Cyber Risk Advisor (CRA)	AR-4, AR-7
CMS Privacy Subject Matter Expert (SME)	AR-7
CMS Information Security and Privacy Group (ISPG)	DM-3, SE-1, SE-2
CMS Cybersecurity Integration Center (CCIC)	AR-5
CMS Office of Information Technology (OIT)	AR-7, DI-1, DM-3, DM-3(1)
CMS Senior Official for Privacy (SOP)	Personnel Designations, Complaints, AP-1, AP-2, AR-1, AR-2, AR-3, AR-4, AR-5, AR-6, AR-8, IP-2, IP-4, SE-1, TR-3, UL-1, UL-2
CMS Business Owner (BO)	Other Permitted Uses & Disclosures, Minimum Necessary, Notice of Privacy Practices, Accounting of Disclosures, De-Identification of PHI, Creating a Limited Data Set, AP-1, AP-2, DM-1, DM-2, IP-1, IP-1(1), TR-1, TR-1(1), UL-1, UL-2
CMS Federal Employee and Contractors	Use and Disclosure, Accounting of Disclosures, Training, Employee Sanctions, Refraining from Intimidating or Retaliatory Acts, Mitigation, AR-3
CMS System Owner/Maintainer	AP-2, AR-2 ,DI-1, DI-1(1), DM-1, DM-2, DM-2(1), UL-1
CMS Privacy Act Officer	Other Permitted Use & Disclosure, Individuals' Rights to Access, Amendment and Correction of PHI, Accounting of Disclosures, Request for Restriction of the Use and/or Disclosure of PHI, Creating a Limited Data Set, AR-4, IP-2, IP-3, TR-2, TR-2(1), TR-3
Division of Security and Privacy Compliance (DSPC)	AR-5, DM-3
Office of Enterprise Data Analytics (OEDA)	AR-8

5. HIPAA/HITECH and Privacy Act Procedures

This section contains the procedures that facilitate the implementation of the requirements within the HIPAA Privacy Rule, Privacy Act, NIST 800-53A, and/or the CMS ARS. Some of the controls listed below map to one or more related FISMA controls, but others do not.

5.1 Use and Disclosure

As authorized by statute, regulation, or Executive Order, CMS conducts activities involving the collection, use, and disclosure of Protected Health Information (PHI) and Personally Identifiable Information (PII). CMS collects, uses, and discloses PII/PHI for payment and health care operations if and only if CMS can identify a statute or Executive Order that provides CMS with the authority for that action. Regulations, internal guidance, or informal guidelines are not sufficient to provide CMS with the authority to take action with reference to PII or PHI.

CMS relies on statutes, regulations, Executive Orders, and CMS' policies and procedures establish whether a collection, use, or disclosure of PHI or PII is required or permitted. CMS's authority to collect is included in its Privacy Act Systems of Records, web site Privacy Act Notices, Privacy Impact Assessments, and in other compliance documents and notices.

For internal uses, CMS develops and implements policies and procedures that limit access and use of PII/PHI based on the specific needs and roles of its workforce members, thereby limiting access to that which is required to carry out their duties. To do so, CMS identifies 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.

This policy applies to all CMS employees and contractors using PII/PHI in conducting the work of the agency. The following steps detail the CMS-specific process for use and disclosures of PII/PHI.

- **Step 1**: CMS shall evaluate each program's collection, maintenance, use, and disclosure of PII and PHI to ensure conformance to CMS policy, procedure, and applicable laws.
- **Step 2**: CMS shall use notice and comment rulemaking to publish program regulations in the Federal Register based on the applicable statutory authority, Executive Order(s), and the desired program policies.
- **Step 3**: CMS shall publish Privacy Act Systems of Records in the Federal Register that describe the authority and purpose for the collection, maintenance, use, and disclosure of PII that will be contained in Systems of Records.
- **Step 4:** CMS provides a Notice of Privacy Practices for Original Medicare in the annual Medicare and You Handbook that describes the uses and disclosures of PII/PHI and individual's access rights.

5.2 Other Permitted Uses and Disclosures

CMS may use and disclose protected health information (PHI) and personally identifiable information (PII) as allowed by federal law and with an individual's authorization. If CMS does not have the individual's authorization, it may only use and disclose PII/PHI as permitted under

applicable law, including the HIPAA Privacy Rule and the Privacy Act. HIPAA governs PHI, and the Privacy Act governs PII. Other program specific or specialize laws may layer added requirements or conditions on the disclosure of particular categories of PHI or PII. For example, substance abuse treatment records are subject to HIPAA, the Privacy Act, and SAMHSA's part 2 regulations.

For internal uses, CMS develops and implements policies and procedures that limit access and use of PII/PHI based on the specific needs and roles of its workforce members, thereby limiting access to that which is required to carry out their duties. CMS further limits these individuals' access such that they can only access the records they need to access, and/or limits access to only the data elements within those records that are relevant to the performance of those specific roles. Finally, CMS may limit access to only the conditions under which those individuals need access to PII/PHI to do their jobs.

Under the Privacy Act, for each System or Records, a list of all disclosures permitted without the subject's notification and consent are found in the System or Records Notice's "routine uses" section.

Subject to certain limitations and requirements, which generally include the minimum necessary concept and disclosure-specific limitations and requirements, the HIPAA Privacy Rule permits covered entities to disclose PHI without the subject individuals' authorization under the following conditions:

- **Uses and disclosures required by law (45 CFR 164.103; 164.512(a))**

  CMS is permitted to use and disclose PII/PHI when it is required by law (including, but not limited to statute, regulation, or court orders). Permitted uses or disclosures are limited to those permitted by the relevant law.

- **Uses and disclosures for public health activities (45 CFR 164.103; 164.512(a))**

- **Uses and disclosures for public health activities, to:**

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

- **Disclosures about victims of abuse, neglect, or domestic violence (45 CFR 164.501; 164.512(b))**

  CMS supports the disclosure of PII/PHI for purposes of protecting victims of abuse, neglect, or domestic violence.

- **Uses and disclosures for health oversight activities (45 CFR 164.501; 164.512(d))**

  CMS 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; or
- Entities subject to civil rights laws for which health information is necessary for determining compliance.

Permitted health oversight activity disclosures do not include an investigation or other activity in which the beneficiary is the subject of the investigation or activity unless certain conditions are met.

- **Disclosures for judicial and administrative proceedings (45 CFR 164.512(e))**

  CMS regularly discloses PII/PHI in the course of judicial or administrative proceedings.

- **Disclosures for law enforcement purposes (45 CFR 164.512(f))**

  CMS discloses PII/PHI for law enforcement purposes.

- **In response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court of competent jurisdiction, CMS handles the request as a Freedom of Information Act (FOIA) request in accordance with HHS policy.**

- **Uses and disclosures about decedents (45 CFR 160.103; 164.502(g)(1); 164.508)**

  CMS may only disclose PII/PHI about decedents in the past fifty years when CMS has the proper documentation necessary to determine the legal authority of the requester or the legal relationship of the requester to the decedent (e.g. executor).

- **Uses and disclosures for research purposes (45 CFR 164.501; 164.512(i))**

  CMS discloses PII/PHI for research purposes when the PII/PHI request is approved by the CMS Privacy Board (i.e. OEDA) and an independent Privacy Board or an Institutional Review Board (IRB) has modified or waived the Privacy Rule authorization requirements. The researcher must receive a HIPAA waiver from an external Privacy Board or IRB as the CMS Privacy Board does not issue HIPAA waivers for external research requests. IRBs may also make findings regarding Human Subjects research, but those findings are distinguishable from the required Privacy Rule waivers or modifications.

- **Uses and disclosures to avert a serious threat to health or safety (45 CFR 164.512(j))**

  CMS 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.

  CMS also discloses to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.

- **Uses and disclosures for specialized government functions (45 CFR 164.512(k))**

  CMS uses or discloses PII/PHI for specialized government functions.

- **Disclosures for workers' compensation (45 CFR 164.512(l))**

  CMS 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.

The following steps detail the CMS-specific process for other permitted use and disclosures of PII/PHI.

General Procedures

When CMS receives a request for PII/PHI from an external organization, a determination is made on whether such use and disclosure is permitted by law. The request is reviewed by the CMS Business Owner in consultation with the Privacy Office, which will consult with the CMS Division of the Office of General Counsel as needed.

Procedures for Disclosures for Judicial and Administrative Proceedings (45 CFR 164.512(e))

- CMS regularly discloses PII/PHI in the course of judicial and administrative proceedings. This is done in response to an order from a court of competent jurisdiction (Federal District Court or higher), or a subpoena if CMS discloses only the PII/PHI explicitly authorized by the order and/or subpoena.
- CMS generally seeks a protective order when it receives a court order or subpoena seeking PII/PHI. The protective order restricts or limits the use of the data provided by CMS only for uses as outlined in the court order.
- Regardless of the origin of the court orders or subpoena, the CMS employee in receipt of the legal document shall forward it to the CMS Privacy Act Officer. The Privacy Act Officer sends all court orders to the Office of General Counsel (OGC) General Law Division, to confirm legal sufficiency. If a protective order is not included in or with the court order or subpoena, then OGC General Law Division returns the request to the requester with instructions on how to resubmit.
- After OGC GLD confirms legal sufficiency, the court order is sent to the Privacy Act Officer. The Privacy Act Officer acknowledges receipt of the court order or subpoena within 10 working days.
- The Privacy Act Officer determines if CMS has the responsive documents. If CMS has the documents, authorization is given for the request to be acted on by the data disclosure component (DDC).
- The disclosure component pulls the requested data. If there are any questions on whether the data is responsive to the court order, the Privacy Act Officer reviews the data, verifies that the data is responsive, and, subject to review for privilege, authorizes its disclosure. Only data that is explicitly requested is released.

- Before the data is sent to the requester, the DDC notifies the EPPE staff within OEDA and the OEDA staff enter the disclosure into the EPPE tracking system and then releases the data to the requester.
- If CMS does not have the data that is requested, the Privacy Act Officer, in conjunction with OGC, will communicate with the appropriate parties.

Procedures for Disclosures for Law Enforcement Purposes

- Law Enforcement (LE) requests may come to CMS through a FOIA request, the Office of General Counsel, a letter to the Privacy Office, or a letter to the Business Owner. All law enforcement requests must be in writing.
- These requests are forwarded to the Privacy Act Officer.
- When the request is received, the Privacy Act Officer acknowledges receipt of the request within 10 working days.
- The request is reviewed to ensure it meets the requirements of the Privacy Act, the HIPAA Privacy Rule and HSS and CMS policy and procedures for a law enforcement letter. Among other things, the request must meet the following requirements:
    a. Come from the head of the law enforcement agency (or a delegated authority);
    b. Be written on agency letterhead stationery;
    c. Be for a legitimate active case;
    d. Be specific and limited in scope to the purpose for which the information is sought;
    e. State the applicable law that authorizes the requester to obtain the information; and
    f. Contain an original signature of the head of the law enforcement agency or designee.
- If the written request does not contain the required elements, the Privacy Act Officer returns the request; along with information on what is missing and how to resubmit.
- When a completed request is received, the Privacy Act Officer determines if CMS has the responsive documents. If CMS has the documents, authorization is given for the request to be acted on by the data disclosure component.
- The disclosure component pulls the data. If there are no questions concerning the data, the data is sent to the requester. If there are any questions on whether the data is responsive to the request, the Privacy Act Officer reviews the data, verifies that the data is responsive, and authorizes its disclosure. Only data that is explicitly requested is released.

- Before the data is sent to the requester, the DDC completes the required entries into CMS's data tracking system to document and track its release and then releases the data to the requester.
- If CMS does not have the data that is requested, the Privacy Act Officer in conjunction with OGC will communicate with the appropriate parties

Procedures for Use and Disclosures about Decedents

CMS may only disclose PII/PHI about decedents in the past fifty years when CMS has the proper documentation necessary to determine the legal relationship of the requester or the legal relationship of the requestor to the decedent (e.g. executor). After receiving proper documentation, follow the general procedures for use and disclosure discussed above.

Procedures for Use and Disclosures for Research Purposes

- CMS discloses PII/PHI for research purposes when the PII/PHI request is approved by the CMS Privacy Board.
- Requests for Research Identifiable Files (RIF) data are reviewed by OEDA to ensure that the beneficiary's privacy is protected, that the request for identifiable data is legally permitted, and that all required documents are completed, reviewed, and approved.
- A list of the required documents for a request for RIF data can be found on the ResDAC website (www.resdac.org). After ResDAC reviews the packet and the packet is finalized by the researcher, they must obtain a waiver from an external IRB then the request will be forwarded to the CMS Privacy Board for review. If the request is approved by the CMS Privacy Board, the Privacy Board notifies the researcher, and the request is processed with a signed CMS data use agreement (DUA).

5.3 Minimum Necessary

CMS is required to collect, use, and disclose only the minimum amount of protected health information (PHI) and personally identifiable information (PII) necessary to conduct treatment, payment, and health care operations, and to conduct all other permitted uses and disclosures. For internal uses, CMS develops and implements procedures that limit access and use of PII/PHI based on specific needs of and roles of its workforce members, thereby limiting access to that which is required to carry out their duties. Whenever possible, CMS further limits these individuals' access such that they can only access the records they need to access, and/or limits access to only the data elements within those records that are relevant to the performance of those specific roles. Finally, CMS may limit access to only the conditions under which those individuals need access to PII/PHI to do their jobs.

CMS makes reasonable efforts to limit the use or disclosure of PII/PHI to the minimum necessary in order to accomplish the intended purpose of the use, disclosure, or request. CMS relies, if such reliance is reasonable under the circumstances, on the wording of the request for disclosure to determine the minimum necessary PII/PHI to be disclosed.

When requesting PII/PHI from other covered entities, CMS limits any such request to that which is reasonably necessary to accomplish the purpose for which it makes the request.

For requests made on a routine and recurring basis, CMS limits the PII/PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

All other requests are reviewed on an individual basis to determine that the PII/PHI sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made.

The following paragraph details the process for collecting, using, and disclosing the minimum amount of PHI and PII necessary to conduct permitted operations.

It is the responsibility of the CMS Business Owner to determine the minimum necessary PII/PHI required to conduct the activity for which the agency is authorized. A Contracting Officer's Representative, working with the Contracting Officer and the Business Owner, makes the determination. The Privacy Office and the Office of General Counsel are consulted, as necessary.

5.4 Verification of identity

Prior to any disclosure of Protected Health Information (PHI) or Personally Identifiable Information (PII), CMS:

- Authenticates the identity of a person requesting PII/PHI and, as appropriate, the authority of any such person permitted access to PII/PHI;
- If the requester represents themselves as the personal representative of a person authorized to receive access to PII/PHI, CMS will authenticate both the identity of the person and of the personal representative. CMS will then treat the 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; and
- Obtains any documentation, statements, or representations that serve to authenticate the individual and/or confirm the status and identity of their personal representative, whether oral or written, from the authorized person requesting the PII/PHI.

The following steps detail the CMS-specific process for verifying an individual's identity.

Authentication of Identity Prior to Disclosure of PII/PHI

For detailed guidance in authenticating identity prior to disclosing PII/PHI, use CMS Program Pub. 100-01 Medicare General Information, Eligibility, and Entitlement, Transmittal 7, dated June 25, 2004. Available for download at https://www.cms.gov/Regulations-and-Guidance/Guidance/Transmittals/Downloads/R7GI.pdf

Verification of Legal Authority to Act as Personal Representative

- CMS relies on documentation, statements, or representations that, on their face, legally authorize a person to act on the beneficiary's behalf or on behalf of a deceased individual or the decedent's estate. This documentation, if applicable, should be part of the beneficiary's record.

- After the personal representative's identity has been authenticated and before disclosure of PII/PHI, CMS checks the beneficiary's record for the required documentation that authorizes an individual to act as a personal representative (e.g., Guardianship and Letters Testamentary). If the documentation is in the record, then the PII/PHI can be disclosed.

- If the documentation is not in the record, then CMS refers the requester to Medicare.gov for information on submitting the required documentation available at: https://www.medicare.gov/medicareonlineforms/publicforms/cms10106.pdf, or directs the requester to call 1-800-MEDICARE.

5.5 Authorization

CMS requires the individual's written authorization for any use or disclosure of Protected Health Information (PHI) or Personally Identifiable Information (PII) that is not for treatment, payment, health operations, or otherwise permitted or required by the HIPAA Privacy Rule and/or the Privacy Act. This includes a situation where an individual wants their information shared with a third party.

CMS does not condition payment, enrollment, or benefits eligibility on an individual granting an authorization.

CMS's requires all written consent to be in plain language and contain specific information, such as the PII/PHI to be used or disclosed, the persons or entities disclosing and receiving the information, the expiration date of the consent, and information providing the right to revoke the authorization in writing if it has not been acted upon already.

The following steps detail the CMS-specific process for requesting and receiving an individual's written authorization.

CMS has a standard authorization form, "1-800-Medicare Authorization to Disclose Personal Health Information." The form includes information on how to submit a completed authorization, as well as the required elements needed for a valid authorization under the HIPAA Privacy rule.

Individuals can receive the form by:

a. Downloading it from Medicare.gov. https://www.medicare.gov/medicareonlineforms/publicforms/cms10106.pdf.

b. Completing it online at https://www.medicare.gov/MedicareOnlineForms/AuthorizationForm/OnlineFormStep.asp

c. Requesting it by mail by calling 1-800-MEDICARE.

- **Step 1:** When a written form is received, the form is reviewed for completeness. If the form is not complete with the required information, the form is returned. The individual is instructed to complete all required information and to resubmit.

- **Step 2:** If the written form is complete, the identity and authority of the individual is determined in accordance with the instructions contained in CMS Policies and Procedures, "Verification of Identity."
- **Step 3:** Once verification of identity and authority is complete, CMS documents and retains the signed authorization in the beneficiary's record.

5.6 Personal Representatives

CMS generally treats a personal representative the same as the individual, with respect to uses and disclosures of the individual's Personal Identifiable Information (PII) and Protected Health Information (PHI) relevant to that personal representation, as well as 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.

The following steps detail the CMS-specific process for treating a personal representative with respect to uses and disclosures.

- In making a determination of whether an individual has the authority to act as the personal representative for someone else, CMS relies on documentation, statements, or representations that, on their face, legally authorize a person to act on the beneficiary's behalf or on behalf of a deceased individual or the decedent's estate. This documentation must be included in the beneficiary's record. Examples of the required documentation include, but are not limited to, Guardianship, Letters Testamentary, or Executor/Executrix papers issued by a court.
- If an individual calls 1-800-MEDICARE, they are instructed to send in the legal documentation that establishes their legal authority to act as a legal representative for the beneficiary. Detailed instructions for submitting this documentation are available at Medicare.gov. The form titled, Authorization to Disclose Personal Health Information Form, can be downloaded from https://www.medicare.gov/MedicareOnlineForms/PublicForms/CMS10106.pdf.

5.7 Notice of Privacy Practices

CMS gives a notice of its privacy practices to all beneficiaries of the Medicare Fee-for-Service Program. This notice describes the ways in which Medicare uses and discloses an individual's protected health information (PHI). The notice states Medicare's duties to protect the privacy of this information. This notice also describes the individual's rights, including the right to notify if they believe their privacy rights have been violated.

CMS provides the individual with the Notice of Privacy Practices in several ways. The notice is:

- Provided at the time of enrollment in Medicare.
- Published in the *Medicare & You Handbook*, which enrollees receive annually.
- Available online at www.Medicare.gov

CMS reviews the Notice of Privacy Practices at least annually to determine if there are material changes to the uses and disclosures, the individual's rights, Medicare's legal duties, or other

privacy practices stated in the notice. In addition, CMS makes updates to the Notice of Privacy Practices whenever any material changes are made to the uses and disclosures.

All revisions are made and redistributed per the HIPAA Privacy Rule.

The following details the CMS-specific process for giving proper notice of its privacy practices.

Publishing the Notice

- CMS publishes its "Notice of Privacy Practices for Original Medicare" annually in the Medicare & You Handbook. The Handbook is posted on Medicare.gov and is also available by requesting a copy from 1-800-MEDICARE.
- The Handbook is distributed to beneficiaries every fall in the following ways:
  a. It is mailed through the U.S. Postal Service.
  b. Beneficiaries can sign up at Medicare.gov/gopaperless to get the Medicare & You handbook electronically (This is also called the eHandbook).

Modifications to the Notice

- **Step 1:** If the CMS privacy staff, in working with CMS Business Owners and the Office of General Counsel, become aware of material changes in uses and/or disclosures, they will determine if the change triggers a need to modify the current Notice. The Business Owner develops the updated language to be used in the Notice. The changes made to the Notice are cleared by the Office of General Counsel. When cleared, the privacy staff informs the Office of Communications about the updated language to insert into the Notice.
- **Step 2:** In addition, at the time of the annual Medicare & You update, the CMS privacy staff reviews the Notice of Privacy Practices.
- **Step 3:** The updated Notice is generally distributed as part of the updates to the Medicare & You handbook.

Website Privacy Policies

Each Business/Information System Owner must ensure that each of their website privacy policies:

a. is labeled consistently and clearly as the website's "Privacy Policy;"[5]
b. contains a clear introduction stating that information collected about individuals will be appropriately handled;
c. states whether the website will collect and store any type of PII; how it will be collected (automatically, via e-mail, using web forms, or some other way); what information will be collected; and how it will be used;

[5] Memorandum 03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003), Attachment A, Part III.A., "Privacy Policy Clarification."

d. states whether the website will collect any PII relevant to detecting privacy or security incidents, and whether CMS will use that information to take action once an incident is detected;

e. informs visitors whenever providing requested information is voluntary;[6]

f. informs visitors how to grant consent for CMS's specific uses of voluntarily-provided information;

g. informs visitors of (1) authorization requirements for sales of PHI, marketing and psychotherapy notes, (2) the right of an individual to restrict disclosures of PHI to a health plan for health care for which the individual has paid out of pocket, (3) the duty of CMS to provide notice of a breach of unsecured PHI, and (4) the right to opt out of fundraising communications

h. informs visitors how to grant consent for any CMS use of mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act;[7]

i. where interaction with CMS via the website is voluntary, provides useful information that the public would need to make an informed decision about whether and how to interact with CMS;

j. is updated whenever CMS makes a change to how PII is collected, stored, maintained, used, or disclosed;

k. includes a time/date stamp to inform visitors of the last time CMS made a change to the practices the privacy policy describes;

l. includes a link to the CMS Privacy Program Page;[8] and

m. is updated to be aligned with the CMS-wide Website Privacy Policy whenever a change is made to that policy.[9]

If Business/Information System Owners will create or maintain a website that will be subject to the Administrative Simplification Rules of the Health Insurance Portability and Accountability Act (HIPAA) of 1996; and in particular if that website will collect, store, disclose, use, or transfer protected health information (PHI) as that term is defined by the HIPAA Privacy and Security Rules, the website must also contain a Notice of Privacy Practices consistent with the

[6] Memorandum 03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003), Attachment A, Part III.D., "Content of Privacy Policies."

[7] Memorandum 17-06, Policies for Federal Agency Public Websites and Digital Services (November 8, 2016), Section 6.B., "Privacy Policies on Agency Websites."

[8] CMS is required to maintain a Privacy Program page, the required contents of which are set out by OMB Memorandum 17-06, Section 6.B.1. That page may currently be found at https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/index.html.

[9] The CMS-wide Website Privacy Policy may currently be found at https://www.cms.gov/About-CMS/Agency-Information/Aboutwebsite/Privacy-Policy.html.

HIPAA Privacy Rule, Section 45 CFR § 164.520, "Notice of privacy practices for protected health information."[10]

If Business/Information System Owners will create or maintain any website that uses web measurement and customization technologies,[11] whether that website is a CMS-owned or operated website or a third-party website or application, they must also ensure that the privacy policy for that website:

a. informs the public that the website will use web measurement and customization technologies, and explains how users[12] may make either an opt-out or opt-in decision;
b. provides users who decline to opt-in or decide to opt-out with access to information that is comparable to the information available to users who opt-in or decline to opt-out;
c. if applicable, cites the appropriate Privacy Impact Assessment (PIA) and/or System of Records Notice (SORN);
d. includes:
    i. the purpose of the web measurement and/or customization technology;
    ii. the usage Tier (as that term defined by OMB Memorandum 10-22), session type, and technology used;
    iii. the nature of the information collected;
    iv. the purpose and use of the information;
    v. whether and to whom the information will be disclosed;
    vi. the privacy safeguards applied to the information;
    vii. the data retention policy for the information;
    viii. whether the technology is enabled by default or not and why;
    ix. how to opt-out of the web measurement and/or customization technology;
    x. a statement that opting-out still permits users to access comparable information or services; and
    xi. the identities of all third party vendors involved in the measurement and customization process.

Note that compliance with the above item will also assist Business/Information System Owners in complying with ARS control Systems and Communication Protection (SC)-CMS-2, Website Usage.

If Business/Information System Owners will link to, use, or implement third-party websites or applications, they must take actions related to two type of notices.[13] First, they must ensure the CMS-wide Website Privacy Policy, referred to above, accurately addresses within its scope relevant facts about the third-party websites and applications the Business/Information System

[10] The HHS Office for Civil Rights provides model Notices of Privacy Practices at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html

[11] Web measurement and customization technologies are defined as "technologies that are used to remember a user's online interactions with a website or online application in order to conduct measurement and analysis of usage or to customize the user's experience." OMB Memorandum 10-22, *Guidance for Online Use of Web Measurement and Customization Technology* (June 25, 2010).

[12] Throughout this document "user" refers to any member of the public who accesses a website, whether they use any website interactive functions or not.

[13] OMB Memorandum 10-23, "Guidance for Agency Use of Third-Party Websites and Applications" (June 25, 2010).

Owners create or maintain. Second, they must create new privacy notices, specific to each use of third-party websites or applications, and if feasible post them on the websites where the public will access them. For the first category of privacy compliance activities, they must ensure that the CMS-wide Website Privacy Policy notes:

a. the specific purpose of all CMS uses of third-party websites or applications;
b. how the relevant program or office will use PII that becomes available through the use of each third-party website or application;
c. who at CMS will have access to any PII collected via the third-party website or application;
d. with whom CMS will share PII outside CMS;
e. whether and how CMS will maintain PII, and for how long;
f. how CMS will secure PII that it uses or maintains through the third-party website or application; and
g. what other privacy risks exist, if any, and how CMS will mitigate those risks

Business/Information System Owners that use or maintain third-party websites and applications must also:

a. when feasible, provide links to the relevant privacy policies of the third-party websites and applications being used;
b. when feasible, post a separate Privacy Notice on the third-party website or application itself;
c. take all practical steps to ensure the third-party website or application-specific Privacy Notice is easily visible whenever the third-party website or application is accessed, limited in content to information specific to the use of the particular third-party website or application, clearly labeled, written in plain language, and prominently displayed at all locations where the public might make PII available to CMS; and
d. ensure that the Privacy Notice will:

    i. explain that the website or application is not a government website or application, that it is controlled or operated by a third party, and that CMS's Privacy Policy does not apply to the third party;
    ii. indicate whether and how CMS will maintain, use, or share PII that becomes available through the use of the third-party website or application;
    iii. explain that by using the website or application to communicate with CMS, individuals may be providing nongovernment third parties access to PII;
    iv. direct individuals to CMS's official website;
    v. direct individuals to the CMS-wide Website Privacy Policy as described in (1)-(3), above; and

vi. be updated periodically[14] to be comprehensive and consistent with the CMS-wide Website Privacy Policy

5.8 Individuals' Rights to Access, Inspect, and Obtain a Copy of their PHI or Health Record

CMS provides individuals the right to access, inspect, and obtain copies of their Protected Health Information (PHI), Personally Identifiable Information (PII), and Electronic Health Record (EHR) in a designated record set or in a CMS Privacy Act System of Records.

The following steps detail the CMS-specific process for providing individuals access.

- **Step 1:** When an individual calls 1-800-MEDICARE requesting access to their records, the individual is instructed to send in a written request, and is provided appropriate instructions on how to submit the request.
- **Step 2:** Written requests are received by the applicable System Manager through various means.
- **Step 3:** All written requests are reviewed to ensure that they include the following authentication information: full name, date of birth, health insurance claim number, and one other piece of information such as address, phone number, and/or effective dates of Part A coverage.
- **Step 4:** If the written request is not complete with the required information, the request is returned. The individual is instructed to complete all required information and resubmit.
- **Step 5:** If the written request is complete, the identity of the individual requesting access to records is determined in accordance with the instructions contained above in "Verification of Identity."
- **Step 6:** Once verification of identity and authority is complete, the System Manager or designee reviews the request and gathers the requested materials for the individual.
- **Step 7:** For all completed requests where the individual requests a copy of the records, the records are sent to the individual's address on file.
- **Step 8:** All requests, designations, and correspondence relating to the individual's request for access are maintained by the agency in the individual's record.
- **Step 9:** When an individual makes a request to access, inspect, and obtain a copy of his or her PII/PHI, CMS acts upon the request:

  a. Within 30 days of receipt of the written request if the information is maintained or accessible onsite, or

[14] Frequency of updates may vary. Updates must be made whenever changes are made to existing laws or other authorities that would affect the content of the Privacy Notice. Business/Information System Owners must also review Privacy Notices no less often than every three years to verify Privacy Notices are complete and up-to-date.

b. Within 60 days if it is not maintained or accessible onsite.

c. If CMS is unable to respond to the request within these timeframes, it may extend its response time by up to 30 additional days.

Individuals may request to have a copy of their EHR in an electronic format. Furthermore, the individual can direct CMS to transmit a copy of their EHR to an entity or person designated by the individual if choice is clear, conspicuous, and specific.

5.9 Amendment and Correction of PHI

CMS provides individuals the right to amend and correct their Protected Health Information (PHI),Personally Identifiable Information (PII), and Electronic Health Record (EHR) maintained in a designated record set or a CMS Privacy Act System of Records.

The following steps detail the CMS-specific process for amending and correcting PHI.

When an individual requests amendment/correction to PII/PHI, CMS acts on the request no later than 60 days after receiving the request. If CMS is unable to act within this period, CMS will extend the time to complete the written request by no more than 30 additional days after the initial 60 days.

- **Step 1:** When an individual calls 1-800-MEDICARE requesting an amendment/correction of their PII/PHI, the individual is instructed to send in a written request, and is provided appropriate instructions on how to submit the request. If an individual telephones CMS to request a change to his/her demographic information (e.g., name and address), CMS refers the individual to the Social Security Administration (SSA).
- **Step 2:** Written requests are received by the applicable System Manger through various means.
- **Step 3:** All written requests are reviewed to ensure that they include the following authentication information: full name, date of birth, health insurance claim number, and one other piece of information such as address, phone number, and/or effective dates of Part A coverage.
- **Step 4:** If the written request is not complete with the required information, the request is returned. The individual is instructed to complete all required information and resubmit.
- **Step 5:** If the written request is complete, the identity of the individual requesting amendment/correction to an individual's records is determined in accordance with the instructions contained above in Section 3.4 "Verification of Identity."
- **Step 6:** Once verification of identity and authority is complete, the System Manger or designee reviews the request, determines whether amending the individual's information is appropriate, and notifies the individual. All documentation is placed in the individual's record.
- **Step 7:** If an individual writes to CMS to request a change to his/her demographic information (e.g., name, address), the CMS Customer Service Representative (CSR)

will call the beneficiary about contacting the SSA. If the CSR is unable to reach the beneficiary by phone, the CSR will follow up with a letter to the beneficiary with this information.

- **Step 8:** Other requests for amendments/changes to PII/PHI are forwarded to the beneficiary's Medicare Administrative Contractor (MAC) for resolution. If the MAC determines that the request is appropriate, then the MAC makes the correction to the record. The MAC notifies the individual in writing that the correction was made.

Denial of Correction or Amendment

- If the request for correction or amendment is denied, in whole or in part, the MAC will inform the System Manager.
- The System Manager or designee will document the denial in the beneficiary's record and a timely denial notice will be sent to the individual. The denial notice will inform the individual that the individual may submit a written statement of disagreement with the denial of all or part of a requested amendment and the basis of such disagreement.

CMS denies a request for correction or amendment of PHI for reasons, including but not limited to cases where:

- The individual's PHI is not part of the record.
- CMS did not create the record.
- The record is not available to the individual for inspection under federal law.
- The record is already accurate and complete.

Any written statement or statement of disagreement by the individual, any response by CMS, and any other document pertaining to the request will become part of the individual's record.

5.10 Accounting of Disclosures

CMS provides individuals the right to an accounting of disclosures of their Protected Health Information (PHI) and Personally Identifiable Information (PII) by CMS or its business associates.

CMS accounts for disclosures as required under the Privacy Act, HIPAA, and HITECH. The accounting of disclosures records information concerning all disclosures made to organizations external to CMS pursuant to routine uses under the Privacy Act. CMS routine uses are defined in the System of Records Notice for each system. (See https://www.cms.gov/Regulations-and-Guidance/Guidance/PrivacyActSystemofRecords/index.html)

CMS also accounts for disclosures as required under the HIPAA Privacy Rule. Under the Privacy Rule, individuals have the right to an accounting of all disclosures of PHI except for disclosures made:

- To carry out treatment, payment, or operations;

- To CMS employees who maintain the record and who have a need for the record in the performance of their duties; including but not limited to, payment or health care operations, or for disclosures to the Secretary of HHS, that are required in order to investigate or determine compliance with the HIPAA Privacy Rule requirements;
- That are required under the Freedom of Information Act (FOIA);
- To the individual; or
- Pursuant to the individual's written authorization. [15]

The following steps detail the CMS-specific process for accounting of disclosures.

- **Step 1:** An individual calls 1-800-MEDICARE or writes to CMS for an accounting of disclosures of their PHI. The individual is instructed to send in a written request, and is provided appropriate instructions on how to submit the request.
- **Step 2:** Written requests are received by the applicable System Manager through various means.
- **Step 3:** All written requests are reviewed to ensure that they include the following authentication information: full name, date of birth, health insurance claim number, and one other piece of information such as address, phone number, and/or effective dates of Part A coverage.
- **Step 4:** If the written request is not complete with the required information, the request is returned. The individual is instructed to complete all required information and resubmit.
- **Step 5:** If the written request is complete, the identity of the individual requesting an accounting of disclosure is determined in accordance with the instructions contained above in Section 3.4 "Verification of Identity."
- **Step 6:** CMS acts on the request no later than 60 days after receipt of the request and may extend this time for an additional 30 days, so long as it informs the individual in writing of the reason(s) for the delay and the date by which the individual can expect the accounting.
- **Step 7:** The System Manager works in conjunction with the individual to determine the information needed to address the request. The System Manager works in conjunction with the Business Owner of the requested records to determine whether the individual's records were disclosed.
- **Step 8:** The System Manager will respond in writing and include for each disclosure:
    a. Date of the disclosure;
    b. Name and address of the person or organization receiving the PHI;

[15] 45 CFR § 160.528, Accounting of disclosures of protected health information.

c. A brief description of the PHI disclosed (e.g., health plan beneficiary numbers, Social Security Number, and medical record numbers);

d. A brief statement of the purpose of the disclosure (or include a copy of the written request for disclosure, if appropriate).

- **Step 9:** CMS maintains the correspondence, including the explanation sent to the individual, in the individual's record.

Temporary Suspensions of an Individual's Right to Receive an Accounting of Disclosures to Health Oversight Agencies or Law Enforcement Officials

If a health oversight agency or law enforcement official provides a written request that meets the following requirements, CMS must temporarily suspend the individual's right to an accounting of disclosures for the time period specified in that written request:

- A health oversight agency or a law enforcement official may submit a written statement to request CMS to suspend an individual's right to receive an accounting of disclosures to such health oversight agency or law enforcement official. The written statement must specify:
  a. The reasons that an accounting to the individual would be likely to impede the agency's or official's activities; and
  b. The time for which such a suspension is required.
- If CMS agrees to suspend an individual's right to receive an accounting of disclosures, the following must occur:
  a. During the period of suspension, any disclosures to such health oversight agency or law enforcement official requiring an accounting must still be recorded.
  b. At the end of the suspension of access, an individual's right to receive a complete accounting is reinstated.
- A health oversight agency or a law enforcement official may orally request a temporary suspension. If an oral request is made, CMS must:
  a. Document the identity of the agency or official who made the request; and
  b. Exclude the disclosure(s) for no longer than 30 days from the date of the request, unless a written request is provided during that time.

5.11 Request for Restriction(s) of the Use and/or Disclosure of PHI

CMS provides individuals the right to request that CMS restrict uses or disclosures of Protected Health Information (PHI) or Personally Identifiable Information (PII) about the individual.

CMS is required to agree to any such restriction; if (1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (2) the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

If the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, CMS 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, CMS will request that such health care provider not further use or disclose the PHI.

The following steps detail the CMS-specific process for handling requests for restrictions.

Request

- **Step 1:** When an individual calls 1-800-MEDICARE to request restrictions of the use and/or disclosure of their PHI, the individual is instructed to send in a written request, and is provided appropriate instructions on how to submit the request.
- **Step 2:** Written requests are received by the applicable System Manager through various means.
- **Step 3:** All written requests are reviewed to ensure that they include the following authentication information: full name, date of birth, health insurance claim number, and one other piece of information such as address, phone number, and/or effective dates of Part A coverage. The individual is not required to provide a reason for the request.
- **Step 4:** If the written request is not complete with the required information, the request is returned. The individual is instructed to complete all required information and resubmit.
- **Step 5:** If the written request is complete, the identity and authority of the individual requesting the restriction is determined in accordance with the instructions contained above in Section 3.4 “Verification of Identity.”

  * Note: The individual is not required to provide a reason for the request.
- **Step 6:** Once verification of identity is complete, the System Manager or designee reviews the request, determines whether to agree to the request, and notifies the individual of their determination. All documentation is placed in the individual’s record.

Exception

If restricted information is disclosed to a health care provider for emergency treatment, CMS will request that the receiving health care provider not further use or disclose the PHI, using the following language, “This [health care record or other document] is restricted from further release. It is provided for the purpose of emergency treatment, but should not be further disclosed or used without the permission of the individual to whom the information pertains.”

Restriction

A restriction agreed to by CMS shall not prevent the use or disclosure of PHI:

- To an individual who requests access to their own PHI.
- As required by the Secretary, HHS, to investigate or determine compliance by CMS with the HIPAA Privacy Rule.

- As required by law.
- As required to conduct public health activities.
- To report information for the purposes of protecting victims of abuse, neglect, or domestic violence.
- To conduct health oversight activities.
- In support of judicial and administrative proceedings.
- For law enforcement purposes.
- About decedents.
- For research purposes.
- To avert a serious threat to health or safety.
- For specialized government functions.
- To support a claim for workers' compensation.

Termination of a Restriction

CMS terminates its agreement to a restriction if the individual:

- Agrees to or requests the termination of the restriction in writing; or
- Agrees to the termination and through an oral agreement that is then documented.

5.12 Confidential Communications

CMS provides individuals the right to request and to receive communications of Protected Health Information (PHI) by alternate means or to an alternate location if the individual makes a request in writing. CMS accommodates all reasonable requests.

The following steps detail the CMS-specific process for handling requests for confidential communications.

- **Step 1:** When an individual calls 1-800-MEDICARE or writes to CMS to make a request for confidential communication by alternate means or location, the individual is referred to the Social Security Administration.
- **Step 2:** Individuals may also log into the MyMedicare webpage, and follow the instruction to direct that their Medicare Summary Notices only be available through a secure login at the MyMedicare website.

5.13 De-Identification of PHI

CMS creates datasets that do not identify individuals and makes them publicly available when there is legal authority permitting their creation and dissemination.

The following steps detail the CMS-specific process for de-identifying PHI.

CMS creates public use files (PUF) as part of the administration of its programs. PUFs are created from data contained in the Privacy Act Systems of Records. There are no restrictions on the use and disclosure of PUFs.

The following procedures are used to de-identify Protected Health Information (PHI) or to determine when health information is not individually identifiable:

- **Step 1:** De-identification is accomplished by removing the following identifiers of the individual or of the individual's relatives, employers, or household members:
    a. Names;
    b. All elements of a street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code for areas that contain over 20,000 people;
    c. All elements of dates (except year) for dates directly related to the patient, (e.g., birth date, admission/discharge dates, and date of death);
    d. All ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
    e. Telephone numbers;
    f. Fax numbers;
    g. E-mail address(es);
    h. Social security numbers;
    i. Medical record numbers;
    j. Health plan beneficiary numbers;
    k. Account numbers;
    l. Certificate/license numbers;
    m. License plate numbers, vehicle identifiers, and serial numbers;
    n. Device identifiers and serial numbers;
    o. Uniform Resource Locator (URL) address(es);
    p. Internet Protocol (IP) addresses numbers;
    q. Biometric identifiers, including finger and voice prints;
    r. Full-face photographic images and comparable images; and
    s. Any other unique identifying number except as created by CMS to re-identify the information. This determination also requires that CMS does not have actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual.
- **Step 2:** If a person designated by CMS, with knowledge and experience of generally accepted statistical and scientific methods for rendering information not

individually identifiable, applies such methods and determines that the risk is very small that the information could be used alone, or in combination with other available information, by an anticipated recipient of such information to identify the individual, then the information is determined to be de-identified. This designated person with knowledge and experience of statistical and scientific methods must document the methods and results of the analysis that justify the determination.

a. De-identification will be performed at the origin of the data.

b. Hard copy PHI will be de-identified by obliterating (making unreadable and unrecognizable) the individual identifier(s).

c. The original(s) must not be modified.

- **Step 3:** Once a business owner has created a PUF, the business owner completes the Data Governance Board's "DGB Public Use File Briefing Document." The document is presented to and reviewed by the Data Governance Board for approval.
- **Step 4:** Once approved, the PUF is available for public use.

5.14 Creating a Limited Data Set

Safeguarding Protected Health Information (PHI) is among the highest priorities of CMS. Therefore, CMS enters into a valid data use agreement (DUA), whenever appropriate, to protect the limited data sets (LDS) that will be used and/or disclosed for purposes of research, public health, or health care operations.

The following steps detail the CMS-specific process for using an LDS.

- A LDS may be used or disclosed only for research, public health, or health care operations purposes. It is the responsibility of CMS business owners who use and disclose PHI to recognize situations involving the disclosure of a LDS to contact the DUA Mailbox to initiate the preparation of an appropriate CMS DUA. The Office of General Counsel (OGC), the Privacy Act Officer, and OEDA may also help determine whether a particular purpose constitutes research, public health, or health care operations, and whether use or disclosure of an LDS is appropriate in a given situation.
- Use or disclosure of an LDS may be appropriate in situations where completely de-identified data would not be useful to the recipient, but disclosure of health information accompanied by specific dates, geographic information, and/or unique identifying numbers (e.g., study ID numbers) would be useful. Disclosure of a LDS pursuant to a CMS DUA will be deemed appropriate if the purpose of the use or disclosure is for research, public health, or health care operations purposes, and the use or disclosure complies with CMS's policies and requirements for obtaining approvals, documenting the terms and conditions, and governing the scope of the particular research, public health, or health care operations activity.
- An LDS will still contain PHI. HIPAA generally requires that a covered entity obtain a written HIPAA Authorization from an individual prior to using or disclosing the individual's PHI. An exception exists for use or disclosure of a LDS

if the covered entity enters into a DUA with the recipient of the LDS. The DUA gives the covered entity contractual assurances that the LDS recipient will protect the PHI once it is in its possession. An LDS may not be used or disclosed without first entering into a DUA.

- CMS may approve or deny any LDS request, whether the request is for an initial use or disclosure of an LDS or for an extension of the original DUA. CMS may rely on a researcher's request that meets the minimum necessary requirements if such reliance is reasonable under the circumstances.
- CMS may deny any request for the use/disclosure of an LDS if the requirements under the permitted disclosure pursuant provisions in 45 C.F.R. §§164.502(a)) and 164.514(e) are not met. Each data request must also be reviewed to determine whether it meets HIPAA minimum necessary requirements under 45 C.F.R. §164.514(d).

Use of a DUA

- The appropriate CMS LDS DUA must be used when it is appropriate for CMS to enter into a DUA.
- An LDS should not be used or disclosed until both parties have signed a DUA.

Accounting for Disclosures

HIPAA does not require CMS to account for disclosures of a LDS; however, a LDS is considered Personally Identifiable Information (PII) under the Privacy Act of 1974. Disclosures of a LDS to the intended recipient pursuant to a DUA must be accounted for in order for CMS to comply with the Privacy Act, 5 USC §552a(c).

Compliance

Any CMS employee who becomes aware of a pattern of activity or practice by a LDS recipient that may constitute a material breach or violation of the CMS DUA between such recipient and CMS must immediately inform the Privacy Office and provide a description of the facts giving rise to such belief. CMS does not retaliate against any employee who reports known or suspected compliance issues or violations to the OGC.

5.15 Business Associates

Any person or organization that performs functions or activities that involve the use or disclosure of Protected Health Information (PHI) on behalf of CMS must have a Business Associate Agreement (BAA) in their contract. Examples of functions or activities on behalf of CMS include claims processing, data analysis, and utilization review. The CMS Business Associate Clause can be found at https://agx.cms.gov/Libraries/DocumentDownloadHandler.ashx?LibraryDocumentID=70055.

The BAA establishes the uses and disclosures of PII/PHI by the business associate. It also provides satisfactory assurance that the business associate will appropriately safeguard the information. Examples of these safeguards include administrative, physical, and technical safeguards. It also includes the reporting of breaches of PII/PHI, as well as the return or destruction of PII/PHI upon termination of the contract.

The following steps detail the CMS-specific process for involving Business Associates in the use and disclosure of PHI.

- CMS Office of Acquisition and Grants Management is responsible for ensuring that all contracts involving the collection, use, or disclosure of PII/PHI include the Business Associate Agreement.
- Contracts that do not involve the collection, use, and disclosure of PII/PHI do not include the Business Associate Agreement.
- Contracting Officers working with their Contracting Officer's Representative ensure that the provisions of the Business Associate Agreement are executed.

5.16 Breach Notification

HITECH Act imposes data breach notification requirements for unauthorized uses and disclosures of "unsecured PHI." These notification requirements are similar to many state data breach laws related to personally identifiable financial information (e.g. banking and credit card data). Under the HITECH Act "unsecured PHI" essentially means "unencrypted PHI."

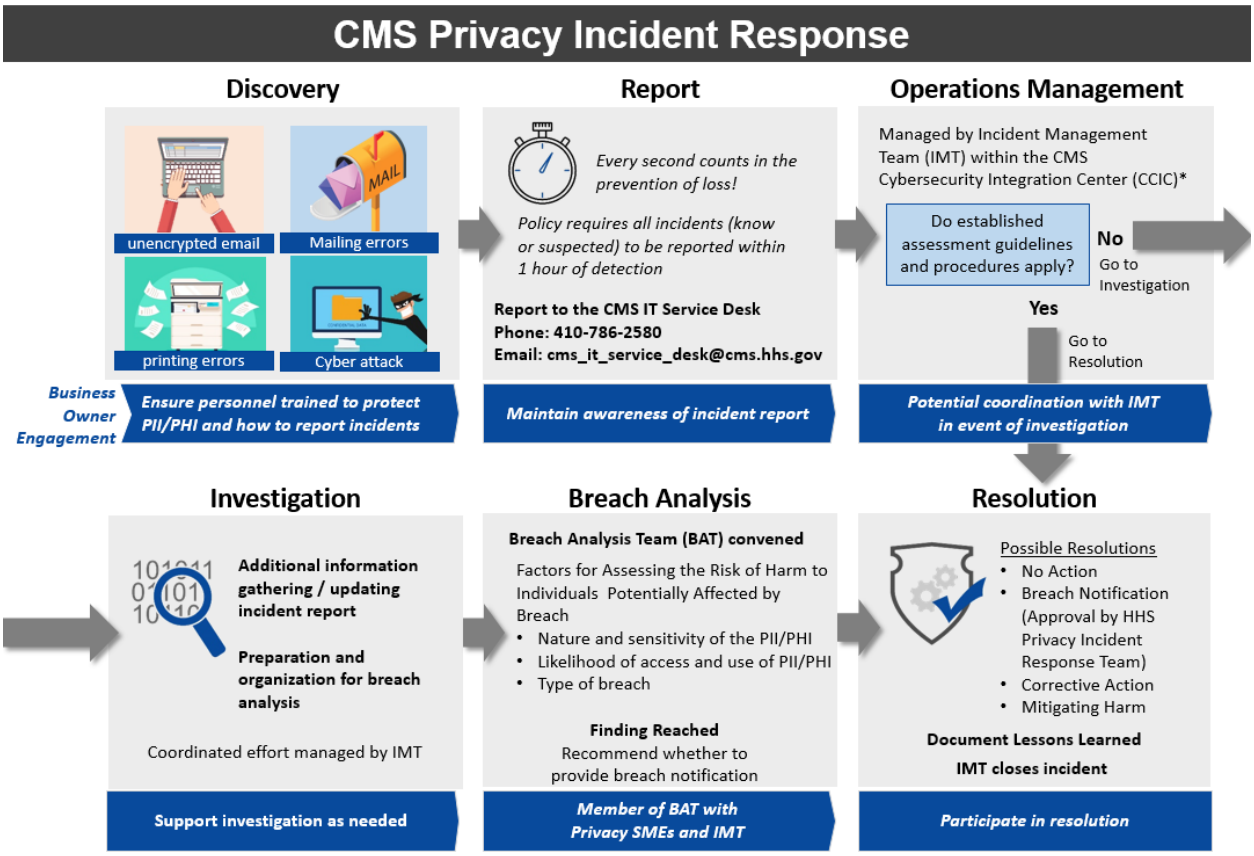
CMS is required to notify individuals of any unsecured breach. If a breach impacts 500 individuals or more then HHS must also be notified. Notification will trigger posting the breaching entity's name on HHS' website. Under certain conditions local media will also need to be notified. Furthermore, notification is triggered whether the unsecured breach occurred externally or internally.

CMS uses a risk-based analysis for privacy breaches using OMB, HITECH, and HIPAA guidance. This guidance requires organizations to determine the sensitivity of its data, based on the information and the context in which the information appears, and then to determine the level of response, based on the resultant privacy risk to the organization and to affected individuals.

CMS defines a breach as the loss of control, compromise, unauthorized disclosure unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

CMS defines an incident as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

The flowchart below gives an overview of the incident and breach response process:



*CCIC is a contractor of Information Security & Privacy Group (OIT)

Figure 4: CMS Privacy Incident Response

The following steps detail the CMS-specific process for privacy breach notification:

- **Step 1:** The Breach Analysis Team (BAT) conducts a Breach Analysis and their findings conclude whether breach notification is required.
- **Step 2:** The Business Owner, in coordination with the Director of the Division of Security, Privacy Policy, and Governance (DSPPG), gives proper notice to the required parties under HITECH (i.e. notification letter to HHS Office of Civil Rights).

5.17 Administrative Procedures

CMS develops and implements written privacy policies and procedures that are consistent with the HIPAA Privacy Rule and the Privacy Act.

The following steps detail the CMS-specific process for procedures ensuring compliance with the requirement to maintain administrative procedures under the HIPAA Privacy Rule and the Privacy Act.

Personnel Designations

CMS designates the Senior Official for Privacy (SOP) as its lead for the agency's development and implementation of privacy policies and procedures.

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.

Training

CMS trains all members of its workforce and contractors on privacy policies and procedures as necessary and appropriate to carry out their functions within and in support of CMS.

CMS provides training on its privacy policies and procedures for:

- Each new member of the workforce and each contractor, all of whom will receive training beginning on their first day of orientation. Training is required for each employee to acquire access to CMS computer systems.
- Each member of the workforce and each contractor receive training annually as part of the annual certification to maintain access to CMS computer systems; and
- Each member of CMS's workforce and each contractor, whose functions are affected by a material change in policies or procedures, receive training prior to the change becoming effective.

Safeguards

CMS maintains policies and procedures to safeguard Protected Health Information (PHI) and Personally Identifiable Information (PII) in accordance with federal requirements for both electronic and paper records to include administrative, technical, and physical safeguards. These are documented in the CMS Information Security Acceptable Risk Standards (ARS) for accrediting CMS information technology (IT) systems; the CMS IS2P2, and this Risk Management Handbook. Examples include:

- Administrative Safeguards – policies and procedures related to security management, assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plans, and periodic evaluation.
- Technical Safeguards – policies and procedures that include user access and restriction controls, audit controls, integrity controls, person or entity authentication controls, and transmission security controls.
- Physical Safeguards – policies and procedures that include facility access controls, workstation use controls, workstation security controls, and device and media controls.

Complaints

- The complaint process is explained in the CMS Notice of Privacy Practices. As described in the Notice, individuals are directed to call 1-800-MEDICARE. The customer service representative directs the individual to send in a written complaint to the Office of the Ombudsman.
- All mail communication goes to the Office of the Ombudsman. The Office of the Ombudsman triages the complaints and works in coordination with the Office of the SOP to address it. All complaints are documented in the individual's records.

- The customer service representative may also provide information on filing a complaint with the U.S. Department of Health and Human Services or Office for Civil Rights.

Employee Sanctions

Sanctions for members of the workforce who fail to comply with the privacy policies and procedures can be found in the CMS Master Labor Agreement.

Mitigation

When CMS becomes aware of the use or disclosure of PII/PHI in violation of applicable federal law and/or of its policies or procedures by one or more of its workforce, contractors, or business associates, CMS follows the procedures documented in the Risk Management Handbook Incident Response Plan (copy can be found on the ISPG Library).

Refraining from Intimidating or Retaliatory Acts

CMS does not intimidate, threaten, coerce, discriminate against, or take retaliatory action against employees or contractors for exercising their rights under the HIPAA Privacy Rule, the Privacy Act, or participating in any process for:

- 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; and
- Opposing any act or unlawful practice under the HIPAA Privacy Rule or Privacy Act and the manner of opposition is reasonable and does not involve a disclosure of PHI not permitted (HIPAA Privacy Rule §164.530 (g)(1)).

These requirements are included in the CMS Master Labor Agreement.

Waiver of Rights

Individuals shall not be required to waive their rights including, but not limited to, their right to file a complaint as a condition for the provision of payment, eligibility, or other benefits.

Standard Policies and Procedures

CMS implements standard policies and procedures in accordance with the HIPAA Privacy Rule and Privacy Act.

Changes to Policies or Procedures

CMS changes its policies and procedures as necessary and appropriate to comply with changes in HIPAA regulations and the Privacy Act.

Documentation

CMS maintains:

- Its policies and procedures in written and electronic form;

- All communication, actions, activities, or designations that are required to be documented; and
- Documentation sufficient to meet its burden of proof under HIPAA Privacy Rule §164.414(b).

6. FISMA Privacy Policy and Procedures

The following is a list of privacy controls that must be complied with per the Federal Information Security Management Act (FISMA).

6.1 Authority and Purpose (AP)

This family of controls ensures that CMS: (i) identifies the legal bases that authorize a particular personally identifiable information (PII) collection or activity that impacts privacy; and (ii) specifies in their notices the purpose(s) for which PII is collected.

6.1.1 Authority to Collect (AP-1)

Before collecting PII, CMS determines whether the contemplated collection of PII is legally authorized. Authorization must be provided by a statute or executive order: regulations, best practices, or agency-level policies do not by themselves provide adequate authority to collect. Program officials consult with the Senior Official for Privacy (SOP), and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements.

The following steps detail the CMS-specific process for obtaining authority to collect PII.

The Business Owner, with SOP support, determines and documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of specific programs and the needs of information systems.

6.1.2 Purpose Specification (AP-2)

Often, statutory language expressly authorizes specific collections of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the Senior Official for Privacy (SOP) and legal counsel, that there is a close connection between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to PIAs, SORNs, and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice.

The following steps detail the CMS-specific process for identifying and documenting, purpose specification.

- **Step 1:** The System Owner/Maintainer, in consultation with the Business Owner, describes the purpose(s) for which PII is collected, used, maintained, and shared in privacy compliance documentation and in its privacy notices (e.g., PIAs, SORNs, Privacy Act Statements, and/or Computer Matching Agreement (CMAs)).
- **Step 2:** The System Owner/Maintainer, in consultation with the Business Owner, ensures the following:
    - The system only collects and uses PII relevant to its purposes

- PII entering the system from other systems is limited to predetermined data elements.
- Generation of new PII is restricted to pre-determined data elements;
- PII output is properly labeled regarding permissible uses and restrictions on usage of the PII;
- PII is transferred to authorized entities only for predetermined, documented purposes and business needs;
- If transferring PII to other agency systems or to third parties via the user interface, the system notifies the user of the permissible uses and restrictions on usage of the PII;
- User interfaces provide a notification when saving PII outside the system or printing PII, reminding the user of the permissible uses and restrictions on usage of the PII; and
- The system limits disclosure of PII to those data elements that are necessary for the purposes of the system

6.2 Accountability, Audit, and Risk Management (AR)

This family of controls enhances public confidence. It includes controls that address governance, monitoring, risk management, and assessment, and through these controls, CMS demonstrates compliance with applicable privacy protection requirements and minimization of privacy risk.

6.2.1 Governance and Privacy Program (AR-1)

Effective implementation of privacy and security controls requires collaboration among the Senior Official for Privacy (SOP), Chief Information Officer (CIO), and Chief Information Security Officer (CISO). To maximize organizational compliance with privacy requirements and best practices, the organization should ensure its privacy professionals engage with both its security community and the Federal privacy community to remain current and to share lessons-learned or other privacy-related information.

The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of a SOP with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program.

The table below outlines the CMS parameters for control AR-1.

Table 2: CMS Defined Parameters - Control AR-1

Control	Control Requirement	CMS Parameter

AR-1	The organization: c. Allocates [*Assignment: organization-defined allocation of budget and staffing*] sufficient resources to implement and operate the organization-wide privacy program; f. Updates privacy plan, policies, and procedures [*Assignment: organization-defined frequency, at least biennially*].	The organization: c. SOP allocates an appropriate allocation of budget and staffing resources to implement and operate the organization-wide privacy program; f. SOP updates privacy plan, policies, and procedures, as required to address changing requirements, but no less often than every two years.

The following steps detail the CMS-specific process for establishing a governance and privacy program.

- **Step 1:** CMS appoints a Senior Official for Privacy (SOP) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems.
- **Step 2:** SOP monitors federal privacy laws and policy for changes that affect the privacy program.
- **Step 3:** SOP requests and advocates for an appropriate allocation of budget and staffing resources to implement and operate the organization-wide privacy program.
- **Step 4:** SOP develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures.
- **Step 5:** SOP develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.
- **Step 6:** SOP updates privacy plan, policies, and procedures, as required to address changing requirements, but no less often than every two years.

6.2.2 Privacy Impact and Risk Assessment (AR-2)

In the latest revision of NIST 800-53, this control was re-named to include risk. The reason is that organizations are moving towards a risk-based assessment of privacy and it is important that if you are doing a privacy impact assessment, to evaluate and account for the risk involved and include that in the assessment as well.

Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the mission, business processes, and information systems. Privacy Impact Assessments are structured reviews (qualitative and quantitative) of both the risk and effect of how information is handled and maintained as well as the potential impacts or harms to individuals and organizations that would result from mishandling or losing control of PII. The term “PIA” can refer either to the process of conducting the assessment, or to the document, that is the outcome of that process

Organizational privacy risk assessment processes consider the entire life cycles of all business processes that involve collecting, using, maintaining, sharing, or disposing of PII. The tools and processes for assessing risk may vary across offices and information systems.

The following steps detail the CMS-specific process for privacy impact and risk assessments.

- **Step 1:** Senior Official for Privacy documents and implements a process for assessing privacy risk to individuals that would result from incidents or events involving the collection, sharing, storing, transmitting, use, and disposal of PII.
- **Step 2:** System Owner/Maintainer conducts PIAs for information systems or electronic collections of information in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.
- **Step 3:** System Owner/Maintainer reviews the PIA no less than every three (3) years and publishes the PIA in accordance with HHS guidance.

6.2.3 Privacy Requirements for Contractors and Service Providers (AR-3)

Contracts and other acquisition-related documents permit CMS to communicate and enforce the implementation of privacy and security controls by contractors and service providers. As a general principle, contractors and service providers must protect PII in the same way and to the same extent that CMS does.

The following steps detail the CMS-specific privacy requirements for contractors and service providers.

Senior Official for Privacy (SOP), in consultation with the Chief Information Officer (CIO), establishes privacy roles, responsibilities, and access requirements for contractors and service providers. This includes privacy requirements in contracts and other acquisition-related documents. SOP shall review, every two (2) years, a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the contracts include clauses that make all requirements of the Privacy Act apply to the system and that make the criminal penalty provisions of the Privacy Act apply to the contractor or service provider and its personnel.

6.2.4 Privacy Monitoring and Auditing (AR-4)

Monitoring and auditing activities ensure privacy controls are implemented and operating effectively. To promote accountability, CMS regularly assesses the implementation of privacy controls, and identifies and addresses any gaps. These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems.

The table below outlines the CMS parameters for control AR-4.

Table 3: CMS Defined Parameters - Control AR-4

Control	Control Requirement	CMS Parameter
AR-4	The organization monitors and audits privacy controls and internal privacy policy [*Assignment: organization-defined frequency*] to ensure effective implementation	The organization monitors and audits privacy controls and internal privacy policy no less often than once every 365 days to ensure effective implementation

The following steps detail the CMS-specific process for privacy monitoring and auditing.

- **Step 1:** As part of the security assessment and authorization program, the Cyber Risk Advisor (CRA) and Information System Security Officer (ISSO) work together to ensure that the privacy controls are monitored and audited no less often than once every 365 days by an independent assessor to ensure effective implementation.
- **Step 2:** Senior Official for Privacy, Privacy Act Officer, and support privacy staff monitors for changes to applicable privacy laws, regulations, guidance, and policy affecting internal privacy policy on a regular basis, and ensure that updates are made to policies and governance documents no less often than once every 365 days to ensure internal privacy policy remains effective.
- **Step 3:** As part of the security assessment and authorization program, CRA and ISSO work together to document, track, and ensure performance of corrective actions identified through monitoring or auditing. If a third-party web application is being used, then the CRA and ISSO must ensure that a Third Party Web Application Assessment is completed.

6.2.5 Privacy Awareness and Training (AR-5)

Privacy Awareness and Training are an effective means to reduce privacy risk within an organization. Training is designed to teach a skill, while awareness is a reminder, which may include a reminder to use and apply that skill (such as spotting or reporting a privacy incident). Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs address many topics, but often include discussions of specific staff responsibilities and the consequences of failing to carry out those responsibilities.

Organizations update awareness and training material based on changing statutory, regulatory, mission, program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training in conjunction with existing information security training.

The table below outlines the CMS parameters for control AR-5:

Table 4: CMS Defined Parameters - Control AR-5

Control	Control Requirement	CMS Parameter

AR-5	The organization: b. Administers basic privacy training [*Assignment: organization-defined frequency, at least annually*] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [*Assignment: organization-defined frequency, at least annually*]; and c. Ensures the personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [*Assignment: organization-defined frequency, at least annually*].	The organization: b. Administers basic privacy training no less often than once every three hundred sixty-five (365) days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII no less often than once every three hundred sixty-five (365) days; and c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements no less often than once every three hundred sixty-five (365) days.

The following steps detail the CMS-specific process for privacy training and awareness.

- **Step 1:** Senior Official for Privacy develops, implements, and updates a comprehensive privacy training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.
- **Step 2:** Office of Information Technology (OIT) administers basic privacy training no less often than once every three hundred sixty-five (365) days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII no less often than once every three hundred sixty-five (365) days; and
- **Step 3:** OIT ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements no less often than once every three hundred sixty-five (365) days.

6.2.6 Privacy Reporting (AR-6)

Privacy reporting helps organizations remain accountable to external authorities. The process may also serve as a check on assessment of privacy risks and implementation of privacy controls.

Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models.

The following steps detail the CMS-specific process for privacy reporting.

- **Step 1:** OMB, Congress, the HHS Office of the Secretary, CMS senior executives, or other oversight bodies establish laws, regulations, policies or other mandates for CMS to gather information concerning its privacy program, either periodically or ad hoc.
- **Step 2:** Senior Official for Privacy (SOP) requires appropriate CMS staff or offices to research and document the required information, and delivers the information to

authorized requestors. Reports will most often include information concerning compliance with specific statutes, regulations, and other mandates.

- **Step 3:** SOP updates privacy reports, as necessary, within any mandated time period (e.g., specified by statute or regulation). At least some reports, such as the Privacy Appendix of the FISMA Report, are anticipated to be required no less often than once every 365 days.

6.2.7 Privacy-Enhanced System Design and Development (AR-7)

Automating and incorporating privacy controls into system design and development provides a concrete way of ensuring information systems are behaving in a way that is intended to achieve privacy objectives. Privacy by Design is a broadly accepted privacy best practice and calls for considering privacy risks in the design and management of information systems. In addition to building in security and privacy controls discussed throughout this Handbook, this control considers additional privacy-specific system characteristics and controls that must be built into the system to address privacy risks.

To the extent feasible, when designing organizational information systems, organizations employ technologies and system capabilities that automate privacy controls affecting the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents.

The following procedure details the CMS-specific process for privacy enhanced system design and development.

Office of Information Technology (OIT) designs information systems to support privacy by automating privacy controls to the extent feasible, integrating and meeting privacy requirements throughout the eXpedited Life Cycle (XLC), and incorporating privacy concerns into reviews of significant changes to HHS/CMS systems, networks, physical environments, and other agency infrastructures.

The Cyber Risk Advisor, in consultation with the Privacy SME, also conducts periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act, the organization's privacy policy, and any other legal or regulatory requirements.

6.2.8 Accounting of Disclosures (AR-8)

Both the Privacy Act and the HIPAA Privacy Rule require accounting of disclosures in certain circumstances. There are differences in the requirements to account for disclosures under the Privacy Act and under the HIPAA Privacy Rule.

The Senior Official for Privacy (SOP) periodically consults with managers of organization systems of records to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals within CMS with a need to know in order to carry out duties consistent with the purpose of the collection, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to statutory requirements.

The following steps detail the CMS-specific process for accounting of disclosures.

- **Step 1:** Office of Enterprise Data Analytics (OEDA) keeps an accurate accounting of disclosures of information held in each system of records, including:
  - (a) Date, nature, and purpose of each disclosure of a record; and
  - (b) Name and address of the person or agency to which the disclosure was made.
- **Step 2:** OEDA retains the accounting of disclosures for the life of the record or five (5) years after the disclosure is made, whichever is longer.
- **Step 3:** OEDA makes the accounting of disclosures available to the person named in the record upon request.

6.3 Data Quality and Integrity (DI)

This family of privacy controls enhances public confidence that any personally identifiable information (PII) collected and maintained by CMS is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.

6.3.1 Data Quality (DI-1)

An organization's data quality assurance process must be commensurate with the sensitivity of the PII. The level of assurance of data quality must be appropriate given the risks that a privacy incident could have on an individual's rights, benefits, privileges, health, or safety as determined by the system owner in consultation with the organization's privacy office. CMS takes reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API).

The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

The table below outlines the CMS parameters for control DI-1:

Table 5: CMS Defined Parameters - Control DI-1

Control	Control Requirement	CMS Parameter
DI-1	The organization: c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [*Assignment: organization-defined frequency*]	The organization: c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems no less often than once every 365 days or as directed by the HHS Data Integrity Board

The following steps detail the CMS-specific process for ensuring data quality.

- **Step 1:** System Owner/Maintainer confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information.
- **Step 2:** System Owner/Maintainer collects PII directly from the individual to the greatest extent practicable.
- **Step 3:** System Owner/Maintainer checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems no less often than once every 365 days or as directed by the Data Integrity Board.
- **Step 4:** The Business Owner issues acceptable business practices ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

6.3.2 Validate PII (DI-1(1))

Validating PII that is used to determine a right, benefit, or privilege for an individual ensures that the determination is based on accurate, timely, and relevant information. Procedures for validating PII should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

The following steps detail the CMS-specific process for validating PII.

Authentication of Identity

For detailed guidance in authenticating identity, use CMS Program Pub. 100-01 Medicare General Information, Eligibility, and Entitlement, Transmittal 7, dated June 25, 2004. Available for download at https://www.cms.gov/Regulations-and-Guidance/Guidance/Transmittals/Downloads/R7GI.pdf

Verification of Legal Authority to Act as Personal Representative

- CMS relies on documentation, statements, or representations that, on their face, legally authorize a person to act on the beneficiary's behalf or on behalf of a deceased individual or the decedent's estate. This documentation, if applicable, should be part of the beneficiary's record.
- After the personal representative's identity has been authenticated and before disclosure of PII/PHI, CMS checks the beneficiary's record for the required documentation that authorizes an individual to act as a personal representative (e.g., Guardianship and Letters Testamentary). If the documentation is in the record, then the PII/PHI can be disclosed.
- If the documentation is not in the record, then CMS refers the requester to Medicare.gov for information on submitting the required documentation available at: https://www.medicare.gov/medicareonlineforms/publicforms/cms10106.pdf, or directs the requester to call 1-800-MEDICARE.

6.3.3 Re-Validate PII (DI-1(2))

Re-validation of PII used to determine a right, benefit, or privilege for an individual, is necessary to ensure the determination is based on the most accurate, timely, and relevant information.

Frequency of revalidation should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the CMS' privacy office.

The following steps detail the CMS-specific process for re-validating PII.

CMS requests that the individual or individual's authorized representative revalidate that PII collected is still accurate no less often than once every 365 days or as directed by the Data Integrity Board.

Authentication of Identity

For detailed guidance in authenticating identity, use CMS Program Pub. 100-01 Medicare General Information, Eligibility, and Entitlement, Transmittal 7, dated June 25, 2004. Available for download at https://www.cms.gov/Regulations-and-Guidance/Guidance/Transmittals/Downloads/R7GI.pdf

6.3.4 Data Integrity and Data Integrity Board (DI-2)

If conducting or participating in Computer Matching Agreements (CMAs) with other federal agencies or non-federal agencies, regarding applicants for and recipients of financial assistance or payments under federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records, an agency must establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In the case of CMS, they leverage with the HHS Data Integrity Board for this purpose. The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under CMAs.

The following steps detail the CMS-specific process for data integrity and the data integrity board.

- **Step 1:** Office of Information Technology (OIT) documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls.
- **Step 2:** HHS establishes a Data Integrity Board (DIB) when appropriate to oversee CMAs and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

6.3.5 Publish Agreements on Website (DI-2(1))

In a privacy context, the principle of "access" recommends that whenever feasible, individuals should have the ability to review PII about themselves held within systems of records. Such access should be timely, simplified, and inexpensive. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors.

In support of this principle, CMS has determined that computer-matching agreements (CMAs) are appropriate for publication on its website.

The following details the CMS-specific process for publishing agreements on their website.

The Data Integrity Board (DIB) publishes CMAs on the public website.

6.4 Data Minimization and Retention (DM)

This family of privacy controls helps CMS implement the data minimization and retention requirements to collect, use, and retain personally identifiable information (PII) only if it is relevant and necessary for the purpose for which it was originally collected. CMS retains PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

6.4.1 Minimization of Personally Identifiable Information (DM-1)

Reducing PII to the minimum required to accomplish the legally authorized purpose of collection and retaining PII for the minimum necessary period of time reduces the risk of PII breaches and will reduce the risk of the organization making decisions based on inaccurate PII.

Organizations take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect.

The table below outlines the CMS parameters for control DM-1:

Table 6: CMS Defined Parameters - Control DM-1

Control	Control Requirement	CMS Parameter
DM-1	The organization: c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [*Assignment: organization-defined frequency, at least annually*] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.	The organization: c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings no less often than once every three hundred sixty five (365) days to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

The following steps detail the CMS-specific process for minimization of personally identifiable information.

- **Step 1:** Business Owner and System Owner/Maintainer identify the minimum PII elements that are relevant and necessary to accomplish the purpose of collection (and where a collection of certain PII requires legal authorization, HHS/CMS must ensure that such collection is legally authorized).
- **Step 2:** Business Owner limits the collection and retention of PII to the minimum elements identified in the notice and, when the collection of PII is made directly from the subject individual, limits its purposes to those for which the individual has provided consent to the extent permitted by law.

- **Step 3:** Business Owner and System Owner/Maintainer conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings, no less often than once every three hundred sixty-five (365) days, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

6.4.2 Locate/Remove/Redact/Anonymize PII (DM-1(1))

Anonymized information is defined as previously identifiable information that has been de-identified and for which a code or other association for re-identification no longer exists. Anonymizing information usually involves the application of statistical disclosure limitation techniques to ensure the data cannot be re-identified, such as generalizing the data, suppressing the data, introducing noise into the data, swapping the data, and replacing data with the average value. Using these techniques, the information is no longer PII, but may remain useful for some research and policy development purposes.

The following details the CMS-specific process for locating/removing/redacting/anonymizing PII.

Office of Information Technology (OIT), where feasible and within the limits of technology and the law, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit authorized use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

6.4.3 Data Retention and Disposal (DM-2)

Both the Privacy Act and the Federal Records Act require records to be maintained and disposed of in accordance with a published records schedule. Disposal and destruction of PII must be done securely so that it may not be reconstructed.

National Archives and Records Administration provides retention schedules that govern the disposition of federal records. Program officials and business owners coordinate with records officers, Cyber Risk Advisor, and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper.

The table below outlines the CMS parameters for control DM-2:

Table 7: CMS Defined Parameters - Control DM-2

Control	Control Requirement	CMS Parameter

DM-2	The organization: a. Retains each collection of personally identifiable information (PII) for [*Assignment: organization-defined time period*] to fulfill the purpose(s) identified in the notice or as required by law; c. Uses [*Assignment: organization-defined techniques or methods*] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).	The organization: a. Retains each collection of personally identifiable information (PII) for the time period specific by the NARA approved records schedule in consultation with the Records Management Officer to fulfil the purpose identified in the notice or as required by law; c. Uses Federal Information Processing Standards (FIPS) validated techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records)

The following steps detail the CMS-specific process for data retention and disposal.

- **Step 1:** System Owner/Maintainer retains each collection of PII for the time period specified by the NARA-approved records schedule in consultation with the Records Management Officer to fulfill the purpose(s) identified in the notice or as required by law
- **Step 2:** System Owner/Maintainer disposes of, destroys, erases, and/or anonymizes 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
- **Step 3:** System Owner/Maintainer uses FIPS-validated techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records)

6.4.4 System Configuration (DM-2(1))

HIPAA requires the organization to follow specific procedures for system configuration and to implement policies and procedures to address the final disposition of PHI and/or the hardware or electronic media on which it is stored.

The following procedure details the CMS-specific process for system configuration.

System Owner/Maintainer configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under a NARA-approved records schedule.

6.4.5 Minimization of PII Used in Testing, Training, and Research (DM-3)

When developing and testing information systems, PII is at a heightened risk for accidental loss, theft, or compromise. Therefore, CMS needs to take measures to reduce that risk.

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes.

The following steps detail the CMS-specific process for minimization of PII used in testing, training, and research.

- **Step 1:** The Office of Information Technology (OIT) develops policies and procedures that minimize the use of PII for testing, training, and research. The policies and procedures covering testing, training, and research are detailed in other chapters of the Risk Management Handbooks.
- **Step 2:** OIT implements controls to protect PII used for testing, training, and research.
- **Step 3:** OIT, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

6.4.6 Risk Minimization Techniques (DM-3(1))

Anonymizing PII is one technique to reduce risk and decreases the potential impact if the PII is compromised. Organizations can minimize risk to privacy of PII by using techniques such as de-identification. When PII is of a sufficiently sensitive nature, to the maximum extent possible, PII should be anonymized in accordance with one of the techniques discussed in NIST SP 800-122 prior to its use in development or testing.

The following steps detail the CMS-specific process for risk minimization.

Office of Information Technology shall use techniques to minimize the risk to privacy of using PII for research, testing, or training.

6.5 Individual Participation and Redress (IP)

This family of privacy controls addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their personally identifiable information (PII). By providing individuals with access to their PII, and with the ability to have their PII corrected or amended, when appropriate, the controls in this family enhance public confidence in any decisions CMS makes based on the PII.

6.5.1 Consent (IP-1)

Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices.

Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII/PHI.CMS ensures that opt-in consent is provided in all cases where it is required by law or other binding authorities.

The following steps detail the CMS-specific process for obtaining consent.

- **Step 1:** Business Owner provides means, whenever required, and otherwise as feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII/PHI prior to its collection.
- **Step 2:** Business Owner provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII/PHI.
- **Step 3:** Business Owner obtains consent, whenever required, and otherwise as feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII/PHI.
- **Step 4:** Business Owner ensures that individuals are aware of and, whenever required by law and in other cases when 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/PHI.

6.5.2 Mechanisms Supporting Itemized or Tiered Consent (IP-1(1))

Individual consent or authorization is required under the HIPAA Privacy Rule for uses and/or disclosures of an individual's protected health information (PHI).

Organizations can provide, for example, individuals' itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, organizations construct consent mechanisms to ensure that organizational operations comply with individual choices.

The following details the CMS-specific process for mechanisms supporting itemized or tiered consent.

Business Owner implements mechanisms to support itemized or tiered consent for specific uses of data.

6.5.3 Individual Access (IP-2)

Access affords individuals the ability to review PII about them held within organizational systems of records. Access must be timely, provided in a format that the individual is able to understand, and provided as inexpensively as possible. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The Senior Official for Privacy (SOP) working with the Privacy Act Officer is responsible for the content of Privacy Act records request processing, in consultation with legal counsel.

Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding.

The following steps detail the CMS-specific process for giving individuals access.

- **Step 1:** When an individual calls 1-800-MEDICARE requesting access to their records, the individual is instructed to send in a written request, and is provided appropriate instructions on how to submit the request.
- **Step 2:** Written requests are received by the applicable System Manager through various means.

- **Step 3:** All written requests are reviewed to ensure that they include the following authentication information: full name, date of birth, health insurance claim number, and one other piece of information such as address, phone number, and/or effective dates of Part A coverage.
- **Step 4:** If the written request is not complete with the required information, the request is returned. The individual is instructed to complete all required information and resubmit.
- **Step 5:** If the written request is complete, the identity of the individual requesting access to records is determined in accordance with the instructions contained above in Section 3.4 "Verification of Identity."
- **Step 6:** Once verification of identity and authority is complete, the System Manager or designee reviews the request, determines whether disclosure is possible and appropriate, and notifies the individual.
- **Step 7:** For all completed requests where the individual requests a copy of the records, the records are sent to the individual's address on file.
- **Step 8:** All requests, designations, and correspondence relating to the individual's request for access are maintained by the agency in the individual's record.
- **Step 9:** When an individual makes a request to access, inspect, and obtain a copy of his or her PII/PHI, CMS acts upon the request:
    a. Within 30 days of receipt of the written request if the information is maintained or accessible onsite, or
    b. Within 60 days if it is not maintained or accessible onsite.

CMS provides a 30-day extension to complete action on the written request.

- **Step 10:** System Manager publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records
- **Step 11:** System Manager publishes access procedures in SORNs
- **Step 12:** System Manager adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests

6.5.4 Redress (IP-3)

Redress supports data integrity requirements for PII by providing a process for individuals to request correction of, or amendment to, their PII maintained by an organization. Redress supports the ability of individuals to ensure the accuracy of PII held by organizations.

Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate.

The following steps detail the CMS-specific process for redress.

- **Step 1:** When an individual calls 1-800-MEDICARE requesting an amendment/correction of their PII/PHI, the individual is instructed to send in a written request, and is provided appropriate instructions on how to submit the request. If an individual telephones CMS to request a change to his/her demographic information (e.g., name and address), CMS refers the individual to the Social Security Administration (SSA).
- **Step 2:** Written requests are received by the applicable System Manager through various means.
- **Step 3:** All written requests are reviewed to ensure that they include the following authentication information: full name, date of birth, health insurance claim number, and one other piece of information such as address, phone number, and/or effective dates of Part A coverage.
- **Step 4:** If the written request is not complete with the required information, the request is returned. The individual is instructed to complete all required information and resubmit.
- **Step 5:** If the written request is complete, the identity of the individual requesting amendment/correction to an individual's records is determined in accordance with the instructions contained above in Section 3.4 "Verification of Identity.
- **Step 6:** Once verification of identity and authority is complete, the System Manager or designee reviews the request, makes a determination whether an amendment, addition or correction to the individual's record is appropriate, and notifies the individual. All documentation is placed in the individual's record, including a record of having made any addition or amendment in response to the individual's request.
- **Step 7:** If an individual writes to CMS to request a change to his/her demographic information (e.g., name, address), the CMS Customer Service Representative (CSR) will call the beneficiary about contacting the SSA. If the CSR is unable to reach the beneficiary by phone, the CSR will follow up with a letter to the beneficiary with this information.
- **Step 8:** Other requests for amendments/changes to PII/PHI are forwarded to the beneficiary's Medicare Administrative Contractor (MAC) for resolution. If the MAC determines that the request is appropriate, then the MAC makes the correction to the record. The MAC notifies CMS and the individual in writing that the correction was made.

Denial of Correction or Amendment

- If the request for correction or amendment is denied, in whole or in part, the MAC will inform the System Manager.
- The System Manager or designee will document the denial in the beneficiary's record and a timely denial notice will be sent to the individual. The denial notice will inform the individual that the individual may submit a written statement of

1750 disagreement with the denial of all or part of a requested amendment and the basis
1751 of such disagreement. This statement of disagreement will be maintained in the
1752 individual's record.

1753 CMS denies a request for correction or amendment of PII/PHI for reasons, including but not
1754 limited to:

1755 • The individual's PII/PHI is not part of the record.
1756 • CMS did not create the record.
1757 • The record is not available to the individual for inspection under federal law.
1758 • The record is already accurate and complete.

1759 Any written statement or statement of disagreement by the individual, any response by CMS, and
1760 any other document pertaining to the request will become part of the individual's permanent
1761 record.

1762 6.5.5 Complaint Management (IP-4)

1763 Complaints, concerns, and questions from individuals can serve as a valuable source of external
1764 input that ultimately improves operational models, uses of technology, data collection practices,
1765 and privacy and security safeguards. Organizations provide complaint mechanisms that are
1766 readily accessible by the public, include all information necessary for successfully filing
1767 complaints (including contact information for the Senior Official for Privacy (SOP) or other
1768 official designated to receive complaints), and are easy to use. Organizational complaint
1769 management processes include tracking mechanisms to ensure that all complaints received are
1770 reviewed and appropriately addressed in a timely manner.

1771 The following steps detail the CMS-specific process for complaint management.

1772 SOP implements a process for receiving and responding to complaints, concerns, or questions
1773 from individuals about organizational privacy practices.

1774 • The complaint process is explained in the CMS Notice of Privacy Practices (detailed in
1775 Section 3.4 of this Handbook). As described in the Notice, individuals are directed to call
1776 1-800-MEDICARE. The customer service representative directs the individual to send in
1777 a written complaint to the Office of the Ombudsman.
1778 • All mail communication goes to the Office of the Ombudsman. The Office of the
1779 Ombudsman triages the complaints and works in coordination with the Office of the SOP
1780 to address each. All complaints are documented in the individual's records.
1781 • The customer service representative may also provide information on filing a complaint
1782 with the U.S. Department of Health and Human Services or Office for Civil Rights.

1783 6.5.6 Response Times (IP-4(1))

1784 Timely communication and resolution of complaints from individuals demonstrates
1785 responsiveness by the organization and reduces the organization's risk of reputational damage
1786 and potential violations of HIPAA and the Privacy Act.

1787 The following steps detail the CMS-specific process for response times.

- **Step 1:** CMS acknowledges complaints, concerns, or questions from individuals within ten (10) working days.
- **Step 2:** CMS completes review of requests within thirty (30) working days of receipt, unless unusual or exceptional circumstances preclude completing action by that time.
- **Step 3:** CMS responds to any appeal as soon as possible, but no later than thirty (30) working days after receipt of the appeal unless the appeal authority can show good cause to extend the response period.

6.6 Security (SE)

This family of privacy controls supplements the security controls to ensure that technical, physical, and administrative safeguards are in place to protect personally identifiable information (PII) collected or maintained by organizations against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework. These security controls include only those that are not addressed under any other governance document (including the IS2P2, ARS, or other RMH Chapters).

6.6.1 Inventory of Personally Identifiable Information (SE-1)

The PII inventory identifies the organization's information assets and identifies those assets collecting, using, maintaining, or sharing PII. The PII inventory identifies those assets most likely to impact privacy; provides a starting point for organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII; and to mitigate risks of PII exposure.

The table below outlines the CMS parameters for control SE-1:

Table 8: CMS Defined Parameters - Control SE-1

Control	Control Requirement	CMS Parameter
SE-1	The organization: a. Establishes, maintains, and updates [*Assignment: organization-defined frequency*] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and b. Provides each update of the PII inventory to the CIO or information security official [*Assignment: organization-defined frequency*] to support the establishment of information security requirements for all new or modified information systems containing PII.	The organization: a. Establishes, maintains, and updates no less often than once every three hundred and sixty five (365) days an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and b. Provides each update of the PII inventory to the CIO or information security official no less often than once every three hundred and sixty five (365) days to support the establishment of information security requirements for all

		new or modified information systems containing PII.

The following steps detail the CMS-specific process for inventorying personally identifiable information.

- **Step 1:** Office of Information Technology (OIT) establishes, maintains, and updates, no less often than once every three hundred sixty-five (365) days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII.
- **Step 2:** OIT provides each update of the PII inventory to the CMS Senior Official for Privacy (SOP) and the CMS CISO no less often than once every three hundred sixty-five 365 days to support the establishment of information security requirements for all new or modified information systems containing PII.

6.6.2 Privacy Incident Response (SE-2)

CMS uses a risk-based analysis for privacy breaches using OMB, HITECH, and HIPAA guidance. This guidance requires organizations to determine the sensitivity of its data, based on the information and the context in which the information appears, and then to determine the level of response, based on the resultant privacy risk to the organization and to affected individuals.

CMS defines a breach as the loss of control, compromise, unauthorized disclosure unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

CMS defines an incident as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Please see the Figure 4. Privacy Incident Response for an overview of the incident and breach response process.

The following is the CMS-specific process for privacy incident response.

- **Step 1:** A suspected or confirmed incident/breach is discovered and reported to CMS IT Service Desk. If the incident is reported by the Medicare Administrative Contractors (MAC) they report incidents to the CMS IT Service Desk and Center for Medicare (CM) mailbox simultaneously.
- **Step 2:** The CMS IT Service Desk reports the issue to Incident Management Team (IMT) or Center for Medicare (CM) depending upon the nature of the reported issue
- **Step 3:** If the incident is sent to CM, they conduct a risk assessment and provide the assessment to IMT for concurrence and then apply any necessary remediation.
- **Step 4:** If the incident is sent to IMT, they contact the applicable Business Owner(s) to collaborate on incident management. Including, conducting an investigation and gathering any additional information required to determine if the issue is an incident or a

breach. If the issue is determined to be an incident they follow the applicable procedures detailed in the IMT Handbook and IMT Playbook

- **Step 5:** If the IMT/CM determines there is a breach, they will request that a breach analysis is conducted, as appropriate. The Breach Analysis Team (BAT) will conduct an analysis to determine the impact/harm by following the BAT Standard Operating Procedure (found on the ISPG Library). The BAT consists of the applicable Business Owner, ISSO, and select members of IMT and DSPPG. The BAT will reach a finding on whether breach notification is necessary.
- **Step 6:** Should breach notification be determined necessary by the BAT. The BAT will coordinate the drafting of a breach notification and obtaining approval from the HHS Privacy Incident Response Team.
- **Step 7:** Proper remediation occurs to the satisfaction of CMS, which can include, but is not limited to: corrective action, mitigating harm, re-training, or individual sanctions.

6.7 Transparency (TR)

This family of privacy controls ensures that CMS provide public notice of their information practices and the privacy impact of their programs and activities.

6.7.1 Privacy Notice (TR-1)

Providing the appropriate notification of privacy practices to the individual enables the individual to make an informed decision when they provide their consent.

Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide general public notice through a variety of means, as required by law or policy, including system of records notices (SORN), privacy impact assessments (PIA), or in a website privacy policy. As required by the Privacy Act, the organization also provides 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.

The following steps detail the CMS-specific process for providing adequate privacy notice.

- **Step 1:** Business Owner provides effective notice to the public and to individuals regarding:
  - Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;
  - Authority for collecting PII;
  - The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and
  - The ability to access and have PII amended or corrected if necessary.
- **Step 2:** Business Owner describes:
  - The PII the organization collects and the purpose(s) for which it collects that information;

- How the organization uses PII internally;
- Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing;
- Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent;
- How individuals may obtain access to PII; and
- How the PII will be protected.

- **Step 3:** Business Owner revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.
- **Step 4:** Read the "Notice of Privacy Practice" procedures listed above under the Privacy Act & HIPAA section and ensure that all requirements detailed therein have been met.

6.7.2 Real-Time or Layered Notice (TR-1(1))

Real-time notice facilitates informed consent and promotes trust from the individual when collecting sensitive PII. Real-time notice used in conjunction with a Privacy Act Statement or Privacy Advisory, based on the sensitivity of the PII provided or collected, ensures the individual provides informed consent.

Real-time notice is defined as notice at the point of collection. A layered notice approach involves providing individuals with a summary of key points in the organization's privacy policy. A second notice provides more detailed/specific information.

The following details the CMS-specific process for real-time or layered notice.

Business Owner provides real-time notice (i.e. notice at all points of collections) and where appropriate, layered notice, whenever any system or business process it collects PII.

6.7.3 System of Records Notices and Privacy Act Statements (TR-2)

SORNs and Privacy Act Statements, i.e., (e)(3) notices, provide 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 Privacy Act defines "maintain" as "maintain, collect, use or disseminate." These requirements impact decisions made during planning, design, development, and operation of programs and systems.

Organizations issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as "a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier." SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons.

The following steps detail the CMS-specific process for system of records notices and privacy act statements.

CMS, through the HHS Privacy Act Officer, OpDiv Privacy Subject Matter Experts, and the HHS Office of General Counsel:

- **Step 1:** Publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII;
- **Step 2:** Keeps SORNs current; and
- **Step 3:** Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

6.7.4 Public Website Publication (TR-2(1))

Publications on the organization websites improves transparency by providing individuals easier access to information about how their PII will be collected, used, maintained, or shared; and centralizing the information regarding to whom an individual should submit a request for access or amendment to their information covered by the SORN.

The following steps detail the CMS-specific process for public website publication.

Privacy Act Officer shall publish all SORNs on a designated page of CMS' public website.

6.7.5 Dissemination of Privacy Program Information (TR-3)

Making information about an organization's privacy program readily available to the public reduces the burden on individuals wanting to better understand an organization's privacy practices. It also reduces the burden on privacy offices and program officials by providing answers to common privacy questions through an easily accessible forum.

Organizations employ different mechanisms for informing the public about their privacy practices. Mechanisms include, but are not limited to, privacy impact assessments (PIA), system of records notices (SORN), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters).

The following steps detail the CMS-specific process for dissemination of privacy program information.

- **Step 1:** Privacy Act Officer ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Official for Privacy (SOP).
- **Step 2:** Senior Official for Privacy ensures that its privacy practices are publicly available through organizational websites or otherwise.

6.8 Use Limitation (UL)

This family of privacy controls ensures that CMS only use personally identifiable information (PII) either as specified in their 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 that the scope of PII use is limited accordingly.

6.8.1 Internal Use (UL-1)

Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the Senior Official for Privacy (SOP) and

where appropriate, legal counsel, organizations document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new use(s) of PII.

The following steps detail the CMS-specific process for internal use.

- **Step 1:** Business Owner ensures that use of PII is consistent with the privacy notices related to the system, including SORN, Privacy Impact Assessment, and notices provided at points of collection.
- **Step 2:** Business Owner ensures that disclosures of PII are consistent with the privacy notices related to the system, including SORN, Privacy Impact Assessment, and notices provided at points of collection.
- **Step 3:** System Owner/Maintainer ensures the authorization schema for the system aligns with the business logic within the system.
- **Step 4:** System Owner/Maintainer ensures the system responds to authorization changes within a defined timeframe.
- **Step 5:** System Owner/Maintainer ensures the system connects to source systems to ensure process changes in authorizations are based on relevant organizational events (e.g., separations, job changes, etc.).
- **Step 6:** System Owner/Maintainer ensures the system requests appropriate credentials at the time of request for initial access to sufficiently identify the user/system making the request.

6.8.2 Information Sharing with Third Parties (UL-2)

Sharing PII with third parties introduces new risks to the individual that, as applicable, requires organizations to establish formal agreements with the third party and ensure the sharing is compatible with the purposes described in notice to, and consent from, the individual. Consideration of privacy risks for sharing PII apply regardless of the method used or whether the information remains stored in the system of records. Data removed from an information system covered by a system of records notice (e.g., a Human Resources database) and shared in another format (e.g., an Excel spreadsheet) must still meet purpose and use requirements of the associated notice. PII not in a system of records that is shared with a third party still must meet the Purpose Specification and, relatedly, Use Limitation FIPPs (i.e. data extracts of PII shared via an Excel spreadsheet or database archive).

A third party is an individual or organization besides CMS and the individual about whom CMS collects and uses information.

The organization Senior Official of Privacy and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s).

The following steps detail the CMS-specific process for information sharing with third parties.

- **Step 1:** Business Owner shares 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

- **Step 2:** Where appropriate, Business Owner enters into Memoranda of Understanding (MOU), Memoranda of Agreement (MOA), Letters of Intent, Computer Matching Agreements (CMAs), Data Use Agreements (DUAs), or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used
- **Step 3:** Business Owner monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and
- **Step 4:** Business Owner evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required

Appendix A. Acronyms

Selected acronyms used in this document are defined below.

Acronyms	Terms
AO	Authorization Official
ARS	Acceptable Risk Safeguards
BAT	Breach Analysis Team
CBT	Computer-based Training
CCIC	CMS Cybersecurity Integration Center
CDM	Continuous Diagnostics and Mitigation
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare and Medicaid Services
CMS CO	CMS Contracting Officers
CMS IS	CMS Information Security
CMS IS2P2	CMS Information Systems Security and Privacy Policy
CONOPS	Concept of Operations
CRA	Cyber Risk Advisor
CSIRC	Computer Security Incident Response Center
CSIRTs	Computer Security Incident Response Teams
DDoS	Distributed Denial of Service
DoS	Denial of Service
ERS	Enterprise Remedy System
EUA	Enterprise User Administration
FAQ	Frequently Asked Questions
FISMA 2014	Federal Information Security Modernization Act of 2014

Acronyms	Terms
FMAT	Forensics and Malware Analysis Team
FTI	Federal Tax Information
HHS	Health and Human Services
HHS CSIRC	HHS Computer Security Incident Response Center
HIPAA	Health Insurance Portability and Accountability Act of 1996
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IIR	Initial Incident Reporting
IMT	Incident Management Team
IOC	Indicators of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
IRA	Incident Response Authority
IRC	Internal Revenue Code
IRL	Incident Response Lead
IRC	Internal Revenue Code
IRP	Incident Response Plan
IRS	Internal Revenue Service
IRT	Incident Response Team
ISO	Information Systems Owners
ISP	Information Security Personnel
ISPG	Information Security and Privacy Group
ISSO	Information Systems Security Officer
IT	Information Technology
LAN	Local Area Network

Acronyms	Terms
LEOs	Law Enforcement Organizations
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NVD	National Vulnerability Database
OCISO	Office of the Chief Information Security Officer
O&M	Operations and Maintenance
OMB	Office of Management and Budget
ODP	Organizational Defined Parameters
OPDIV	Operating Divisions
OS	Operating System
OSSM	OCISO Systems Security Management
OSSO	Office of Security and Support Operation
PCII	Protected Critical Infrastructure Information
PHI	Protected Health Information
PI	Program Integrity
PII	Personally Identifiable Information
PIRT	Privacy Incident Response Team
PIV	Personal Identity Verification
POA&Ms	Plan of Action and Milestones
POC	Point of Contact
Pre-BAT	Pre-Breach Analysis Team
RMH	Risk Management Handbook
RV	Risk Vision
SCA	Security Controls Assessment
SCAP	Security Content Automation Protocol

Acronyms	Terms
SIEMs	Security Information Event Management
SOC	Security Operations Center
SOP	Senior Official for Privacy
SP	Special Publication
SQL	Structured Query Language
SSN	Social Security Number
SSP	System Security Plan
SU	System User
SUID	Set User ID
TCP	Transmission Control Protocol
TIGTA	Treasury Inspector General for Tax Administration
TTL	Time to Live
UID	User ID
URL	Universal Resource Locator
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USGCB	U.S. Government Configuration Baselines
VPN	Virtual Private Network

2021

Appendix B. Glossary of Terms

Selected terms and definitions in this document are defined below (e.g. Breach and a brief definition of its meaning).

Terms	Definitions
Acceptable Risk Safeguards	CMS Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR),” http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity
Accounting of Disclosures	Information that describes a covered entity’s disclosures of PHI other than for treatment, payment, health care operations, and disclosures made with Authorization, and certain other limited disclosures.
Administrative Vulnerability	An administrative vulnerability is a security weakness caused by incorrect or inadequate implementation of a system’s existing security features by the system administrator, security officer, or users. An administrative vulnerability is not the result of a design deficiency. It is characterized by the fact that the full correction of the vulnerability is possible through a change in the implementation of the system or the establishment of a special administrative or security procedure for the system administrators and users. Poor passwords and inadequately maintained systems are the leading causes of this type of vulnerability.
After Action Report	A document containing findings and recommendations from an exercise or a test.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Authorization	An individual's written permission to allow a covered entity to use or disclose specified protected health information (PHI) for a particular purpose. Except as otherwise permitted by the Rule, a covered entity may not use or disclose PHI for research purposes without a valid Authorization. https://privacyruleandresearch.nih.gov/dictionary.asp
Breach	A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.
Breach Analysis Team	An information security and privacy incident and breach response team with the capability that includes preparation, identification, containment, eradication, recovery, and follow-up capabilities to ensure effective recovery from information security and privacy incidents and breaches.

Terms	Definitions
Business Associate	A person or entity that performs certain functions or activities that involve the use or disclosure of PII/PHI on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. Business associate functions and activities include claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; practice management; and re-pricing. Business associate services are legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial. 45 CFR §160.103 provides the full definition of "business associate."
Centers for Medicare & Medicaid Services	CMS covers 100 million people through Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplace.
Chief Information Officer	1. Agency official responsible for: • Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; • Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and • Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency
Chief Information Security Officer	The incumbent in the position entitled Chief Information Security Officer. The CISO 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.
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.
CMS FISMA Controls Tracking System	CMS database that maintains current FISMA information (e.g., POCs, artifacts) to support organizational requirements and

Terms	Definitions
	processes (e.g., communication, contingency planning, training, data calls).
CMS Minimum Security Requirements	Description of the minimum requirements necessary for an information system to maintain an acceptable level of security.
CMS IT Service Desk	For the purposes of incident response coordination, the CMS IT Service Desk is a sub-component of the CMS Information Security and Privacy Group and IMT, whose responsibilities include but are not limited to the following: • Act as the first point of contact for security incidents or anomalies, and record information provided by the system user, CMS Business Owner/Information Systems Owner (ISOs) or On-site Incident Response Authority (IRA) , depending on alert source • Generate a CMS incident ticket to document the incident for CMS records • Determine if the incident relates to PII • Immediately refer information security incidents to the IMT
CMS Marketplace	The Affordable Care Act helps create a competitive private health insurance market through the creation of Health Insurance Marketplaces. These State-based, competitive marketplaces, which launch in 2014, will provide millions of Americans and small businesses with "one-stop shopping" for affordable coverage.
Correctional Institution	Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. (45 CFR 164.501)
Covered Entity	A health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard. CMS's Medicare fee-for-service program, also known as original Medicare, is a covered entity. https://privacyruleandresearch.nih.gov/dictionary.asp
Cyber Risk Advisor	Act as Subject Matter Expert in all areas of the CMS Risk Management Framework (RMF).
Department of Health and Human Services	The United States Department of Health and Human Services (HHS), also known as the Health Department, is a cabinet-level department of the U.S. federal government with the goal of protecting the health of all Americans and providing essential human services. Its motto is "Improving the health, safety, and well-being of America". Before the separate federal Department of Education was created in 1979, it was called the Department of Health, Education, and Welfare (HEW).

Terms	Definitions
Data Aggregation	The combining of PHI to permit data analyses that relate to the health care operations of the respective covered entities. (45 CFR 164.501)
Data Compromise and Data Spills	Data compromise is the exposure of information to a person not authorized to access that information either through clearance level or formal authorization. This could happen when a person accesses a system he is not authorized to access or through a data spill. Data spill is the release of information to another system or person not authorized to access that information, even though the person is authorized to access the system on which the data was released. This can occur through the loss of control, improper storage, improper classification, or improper escorting of media, computer equipment (with memory), and computer generated output.
Data Destruction or Corruption	The loss of data integrity can take many forms including changing permissions on files so that files are writable by non-privileged users, deleting data files and or programs, changing audit files to cover-up an intrusion, changing configuration files that determine how and what data is stored and ingesting information from other sources that may be corrupt.

Data Use Agreement (DUA)	An agreement between the covered entity and the LDS recipient that:
	• Establishes the permitted use(s) and/or disclosure(s) of the LDS by the LDS recipient;
	• Establishes who is permitted to use or receive the LDS;
	• Provides that the LDS recipient will:
	  • Not use or further disclose the information other than as permitted by the DUA or as otherwise required by law;
	  • Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the DUA;
	  • Report to CMS any use or disclosure of the information not provided for by the DUA of which the LDS recipient becomes aware;
	  • Ensure that any agents, including a subcontractor, to whom it provides the LDS agrees to the same restrictions and conditions that apply to the LDS recipient with respect to use(s) and/or disclosure(s) of the LDS; and
	  • Not attempt to re-identify the information or contact the individuals.

De-Identification and De-Identified Data	De-identification is the general term for any process of removing the association between a set of identifying data and the data subject. Records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual is de-identified data. (NISTIR 8053)

Terms	Definitions
Denial of Service (DoS)	An action (or series of actions) that prevents any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, delay, or interruption of service. An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Designated Record Set	A designated record set is a group of records maintained by or for a covered entity that includes: • Medical and billing records about individuals maintained by or for a covered health care provider; • Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or • Used, in whole or in part, by or for the covered entity to make decisions about individuals. A record is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity. For the purposes of CMS's procedures, the individual's Medicare Summary Notice and the individual's entitlement and enrollment date are the designated record set.
Disclosure	The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. (https://privacyruleandresearch.nih.gov/dictionary.asp
Enterprise User Administration	Manages the CMS user identifications. For more detail see https://portal.cms.gov/wps/portal/unauthportal/faq
Event	An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
Exercise	A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.
Exercise Briefing	Material that is presented to participants during an exercise to outline the exercise's agenda, objectives, scenario, and other relevant information.
eXpedited Life Cycle	CMS-XLC-1 The CISO must integrate information security and privacy into the CMS life cycle processes. The XLC provides the processes and practices of the CMS system development life cycle in accordance with the CMS Policy for Information Technology (IT)

Terms	Definitions
	Investment Management & Governance. The CMS CISO maintains the RMH Volume 1 Chapter 1, Risk Management, in the XLC to document the CMS information system life cycle, in accordance with the RMF.
Federal Tax Information (FTI)	Federal Tax Returns and return information are confidential, as required by Internal Revenue Code (IRC) Section 6103. The information is used by the Internal Revenue Service (IRS) is considered FTI and ensure that agencies, bodies, and commissions are maintaining appropriate safeguards to protect the information confidentiality. [IRS 1075] Tax return information that is not provided by the IRS falls under PII.
Full Live Test	Exercise plan incorporates real scenarios and injects into the exercise.
Health Care	Care, services, or supplies related to the health of an individual, including: • Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual that affects the structure or function of the body; and • Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. https://privacyruleandresearch.nih.gov/dictionary.asp
Health Care Clearinghouse	A public or private entity, including a billing service, re-pricing company, community health management information system or community health information system, and "value-added" networks and switches that either process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or receive a standard transaction from another entity and process or facilitate the processing of health information into a nonstandard format or nonstandard data content for the receiving entity. (https://privacyruleandresearch.nih.gov/dictionary.asp
Health Care Operations	Health care operations includes any of the following functions performed by a covered entity: • Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

Terms	Definitions
	• Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; • Underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable; • Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; • Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and • Business management and general administrative activities of the entity, including, but not limited to: – Management activities relating to implementation of and compliance with the requirements of this subchapter; – Customer service, including the provision of data analyses for policyholders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policyholder, plan sponsor, or customer. – Resolution of internal grievances; – The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and – Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. (45 CFR 164.501)
Health Care Provider	A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. (https://privacyruleandresearch.nih.gov/dictionary.asp
Health Insurance Portability and Accountability Act of 1996	An act that amended the Internal Revenue Code of 1986, to improve portability and continuity of health insurance coverage in the group and individual markets; to combat waste, fraud, and abuse in health insurance and health care delivery; to promote the use of medical

Terms	Definitions
	savings accounts; to improve access to long-term care services and coverage; to simplify the administration of health insurance; and for other purposes.
Health Information	Any information, whether oral or recorded in any form or medium, that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. (https://privacyruleandresearch.nih.gov/dictionary.asp
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information. http://www.hhs.gov/hipaa
Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule	The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. The Privacy Rule is located at 45 CFR Part 160, Subparts A, and E of Part 164. http://www.hhs.gov/hipaa
Health Oversight Agency	An agency or authority of the United States that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. (45 CFR 164.501)
Health Plan	For the purposes of Title II of HIPAA, an individual or group plan that provides or pays the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)) and including entities and government programs listed in the Rule. Health plan excludes: (1) any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in

Terms	Definitions
	section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and (2) a government-funded program (unless otherwise included at section 160.103 of HIPAA) whose principal purpose is other than providing, or paying for the cost of, health care or whose principal activity is the direct provision of health care to persons or the making of grants to fund the direct provision of health care to persons. This applies to CMS's Medicare fee-for-service program, also known as original Medicare. (https://privacyruleandresearch.nih.gov/dictionary.asp
HHS Computer Security Incident Response Center	A capability set up for assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).
HHS Privacy Incident Response Team	The FISMA system 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 IRT reports to the CMS CCIC IMT, which is responsible for CMS-wide incident management.
Hotwash	A debrief conducted immediately after an exercise or test with the staff and participants.
Hybrid Entity	A single legal entity that is a covered entity, performs business activities that include both covered and non-covered functions, and designates its health care components as provided in the Privacy Rule. If a covered entity is a hybrid entity, the Privacy Rule generally applies only to its designated health care components. However, non-health care components of a hybrid entity may be business associates of one or more of its health care components, depending on the nature of their relationship. An example of a hybrid entity is a university. A university may be a single legal entity that includes an academic medical center's hospital that conducts electronic transactions for which HHS has adopted standards. Because the hospital is part of the legal entity, the whole university, including the hospital, will be a covered entity. However, the university may elect to be a hybrid entity. To do so, it must designate the hospital as a health care component. (https://privacyruleandresearch.nih.gov/dictionary.asp
Hybrid Test	An exercise with some live scenarios facilitated by a response team for realism (probes, scans, email spoofing, etc.);
Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
Incident Management Team	CMS IMT provides 24X7 incident management support for the enterprise. It is a single communication point for CMS leadership for security incidents and updates.

Terms	Definitions
Incident Response	Incident response outlines steps for reporting incidents and lists actions to resolve information systems security and privacy related incidents. Handling an incident entails forming a team with the necessary technical capabilities to resolve an incident, engaging the appropriate personnel to aid in the resolution and reporting of such incidents to the proper authorities as required, and report closeout after an incident has been resolved.
Individual Health Information	Individually Identifiable Health Information is a subset of health information including demographic data collected concerning an individual that: • Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse • Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual or the past, present, or future payment for the provision of healthcare to an individual, and meets either of the following: • Identifies the individual • There is a reasonable basis to believe the information can be used to identify the individual
Information System Security Officer	Person responsible for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with System Security Officer (SSO). Individual assigned responsibility by the Senior Agency Information Security Officer, authorizing official, management official, or Information System Owner for maintaining the appropriate operational security posture for an information system or program.
Information Systems Security and Privacy Policy	This Policy provides direction to all CMS employees, contractors, and any individual who receives authorization to access CMS information technology (IT) systems or systems maintained on behalf of CMS 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 subject to federal law, regulation, and guidance.
Information Technology	The term information technology with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by the executive agency directly or is used by a contractor, under a contract with the executive agency; or use of that equipment, to a significant extent, in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance). This includes peripheral equipment

Terms	Definitions
	designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. In the preceding sentence, equipment is used by an executive agency if, the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Injects	Injects are scenario based exercises created by a functional exercise team during one of several phases (e.g., Development Phase, Conduct Phase for testing, training and exercise programs for IT plans and capabilities). An example inject is, A Controller would play the role of the Chief Information Officer and would call the Team Chief to provide information and request follow-on action. Expected actions by the Team chief or other exercise participants are documented, to aid controllers, simulators, or data collectors in anticipating what actions will result from the inject. For more information on injects see: NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (page B-8 at: http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf
Inmate	A person incarcerated or confined to a correctional institution. (45 CFR 164.501)
Insider Attack	Insider attacks can provide the greatest risk. In an insider attack, a trusted user or operator attempts to damage the system or compromise the information it contains
Insider Threat	An insider threat generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network (system or data). Intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems.1 Insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices. Insiders do not always act alone and may not be aware as Insiders, facilitate aiding a threat actor (i.e., the unintentional insider threat). It

Terms	Definitions
	is vital that organizations understand normal employee baseline behaviors and ensure employees understand how being used as conduit information can be obtained.
Intrusions or Break-Ins	An intrusion or break-in is entry into and use of a system by an unauthorized individual.
Institutional Review Board (IRB)	An IRB can be used to review and approve a researcher's request to waive or alter the Privacy Rule's requirements for an Authorization. The Privacy Rule does not alter the membership, functions and operations, and review and approval procedures of an IRB regarding the protection of human subjects established by other Federal requirements. (https://privacyruleandresearch.nih.gov/dictionary.asp
Law Enforcement Official	Means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian Tribe, who is empowered by law to: (a) Investigate or conduct an official inquiry of a potential violation of law; or (b) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
Limited Data Sets	A limited amount of PHI to be used or disclosed for research, public health, or health care operations that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: • Names; • Postal address information, other than town or city, state, and ZIP code; • Telephone numbers; • Fax numbers; • Email address; • Social Security numbers; • Medical Record Numbers; • Health plan beneficiary numbers; • Account numbers; • Certificate/license numbers • Vehicle identifiers and serial numbers, including license plate numbers; • Device identifiers and serial numbers; • Universal Resource Locators (URL);

Terms	Definitions
	• Internet Protocol (IP) addresses; • Biometrics identifiers, including finger and voice prints; and • Full face photographic images and any comparable images
Malicious Code	Malicious code is software or firmware intentionally inserted into an information system for an unauthorized purpose.
Malicious Software (Malware)	Malicious code is software based attacks used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome because to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can replicate rapidly, thereby making containment an especially difficult problem. The following is a brief listing of various software attacks: 1. **Virus:** It is propagated via a triggering mechanism (e.g., event time) with a mission (e.g., delete files, corrupt data, send data). 2. **Worm:** An unwanted, self-replicating autonomous process (or set of processes) that penetrates computers using automated hacking techniques. 3. **Trojan horse:** A useful and innocent program containing additional hidden code that allows unauthorized computer network exploitation (CNE), falsification, or destruction of data. 4. **Spyware:** Surreptitiously installed malicious software intended to track and report the usage of a target system or collect other data the author wishes to obtain. 5. **Rootkit Software:** Software intended to take full or partial control of a system at the lowest levels. Contamination defined as inappropriate introduction of data into a system. 6. **Privileged User Misuse:** Privileged user misuse occurs when a trusted user or operator attempts to damage the system or compromise the information it contains. 7. **Security Support Structure Configuration Modification:** Software, hardware and system configurations contributing to the Security Support Structure (SSS) are controlled, being an essential to maintaining the security policies of the system Unauthorized modifications to these configurations can increase the risk to the system.
Marketing	Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. (45 CFR 164.501)
Master Scenario Events List (MSEL)	A chronologically sequence outline of the simulated events and key event descriptions that participants will be asked to respond to during an exercise.

Terms	Definitions
Message Inject	A pre-scripted message will be given to participants during the course of an exercise.
Minimum Necessary	The least information reasonably necessary to accomplish the intended purpose of the use, disclosure, or request. Unless an exception applies, this standard applies to a covered entity when using or disclosing PHI or when requesting PHI from another covered entity. A covered entity that is using or disclosing PHI for research without Authorization must make reasonable efforts to limit PHI to the minimum necessary. A covered entity may rely, if reasonable under the circumstances, on documentation of IRB or Privacy Board approval or other appropriate representations and documentation under section 164.512(i) as establishing that the request for protected health information for the research meets the minimum necessary requirements. (https://privacyruleandresearch.nih.gov/dictionary.asp
Office of Management and Budget	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”). The Privacy Act addresses CMS applicable information security and privacy requirements, arising from federal legislation, mandates, directives, executive orders. The Department of Health and Human Services (HHS) policy by integrating NIST SP-800-53v4, 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.
Paper Inject/Event	A specific activity executed as part of a Master Scenarios Event List (MSEL), MSEL is a collection of pre-scripted events intended to guide an exercise towards specific outcomes. Paper injects drive exercise play. The exercise planning process determines the participants, exercise scenario, injects and the execution order of the course of the exercise. Planners must tailor injects for each exercise to meet the desired outcomes. For example, if the exercise centers on assessing the ability to detect and properly react to hostile activity, the exercise planners would need to structure one or more scenarios that involve hostile activities against the target IT assets. The exercise planner would design these scenarios to stimulate the training audience and elicit responses that that match the desired outcomes of the specific exercise and the overarching objectives.
Participant Guide	An exercise document that typically contains the exercise’s purpose, scope, objectives, and scenario, and a copy of the IT plan being exercised.

Terms	Definitions
Payment	Payment means the activities undertaken by: • A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or • A health care provider or health plan to obtain or provide reimbursement for the provision of health care, • Payment relates to the individual to whom health care is provided and include, but are not limited to: – Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; – Risk adjusting amounts due based on enrollee health status and demographic characteristics; – Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing; – Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; – Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and – Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: □ Name and address; □ Date of birth; □ Social security number; □ Payment history; □ Account number; and □ Name and address of the health care provider and/or health plan. (45 CFR 164.501)
Planner(s)	The group responsible for planning and executing the exercise in a realistic manager.
Privacy Board	A board that is established to review and approve requests for waivers or alterations of Authorization in connection with a use or disclosure of PHI as an alternative to obtaining such waivers or alterations from an IRB. A Privacy Board consists of members with varying backgrounds and appropriate professional competencies as necessary to review the effect of the research protocol on an individual's privacy rights and related interests. The board must include at least one member who is not affiliated with the covered

Terms	Definitions
	entity, is not affiliated with any entity conducting or sponsoring the research, and is not related to any person who is affiliated with any such entities. A Privacy Board cannot have any member participating in a review of any project in which the member has a conflict of interest. (https://privacyruleandresearch.nih.gov/dictionary.asp
Privacy Incident	A Privacy Incident is a Security Incident that involves Personally Identifiable Information (PII) or Protected Health Information (PHI), or Federal Tax Information (FTI) where there is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users or any other than authorized purposes. Users must have access or potential access to PII, PHI, and/or FTI in usable form whether physical or electronic. Privacy incident scenarios include, but are not limited to: • Loss of federal, contractor, or personal electronic devices that store PII, PHI and/or FTI affiliated with CMS activities (i.e., laptops, cell phones that can store data, disks, thumb-drives, flash drives, compact disks, etc.) • Loss of hard copy documents containing PII, PHI and/or FTI • Sharing paper or electronic documents containing PII, PHI and/or FTI with individuals who are not authorized to access it • Accessing paper or electronic documents containing PII, PHI and/or FTI without authorization or for reasons not related to job performance • Emailing or faxing documents containing PII, PHI and/or FTI to inappropriate recipients, whether intentionally or unintentionally • Posting PII, PHI and/or FTI, whether intentionally or unintentionally, to a public website • Mailing hard copy documents containing PII, PHI and/or FTI to the incorrect address • Leaving documents containing PII, PHI and/or FTI exposed in an area where individuals without approved access could read, copy, or move for future use
Protected Health Information	Individually identifiable health information that is: • Transmitted by electronic media, • Maintained in electronic media, or • Transmitted or maintained in any other form or medium. Note: PHI excludes individually identifiable health information in employment records held by a covered HIPAA entity in its role as employer.
Personal Identifiable Information	Any information about an individual including, but not limited to: education, financial transactions, medical history, and criminal or employment history; and information which can be used to distinguish or trace an individual's identity, such as the name, social security

Terms	Definitions
	number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual. Information which can be used to distinguish or trace an individual's identity, such as the name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
Pre-Breach Analysis Team	The CMS Pre-BAT, managed by the CMS Information Security and Privacy Group, with the assistance from the CMS Business Owner/Information Systems Owner (ISOs) and SOP staff as necessary, reviews, triages privacy incidents, and refers to the CMS BAT for a formal risk assessment when needed.
Privileged User Misuse	Privileged user misuse occurs when a trusted user or operator attempts to damage the system or compromise the information it contains.
Public Health Authority	Means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian Tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.
Public Health Oversight Agency	Means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian Tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.
Research	A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. This includes the development of research repositories and databases for research (45 CFR 164.501).
Red Team	A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

Terms	Definitions
Re-Identification	De-identification is the general term for any process that re-establishes the relationship between identifying data and a data subject. (NISTIR 8053)
Required By Law	Includes, but is not limited to, court orders and court-ordered warrants; subpoenas, or summons issued by a court, grand jury, a governmental or Tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require information if payment is sought under a government program providing public benefits.
Risk	The likelihood that a threat will exploit a vulnerability. For system may not have a backup power source; hence, it is vulnerable to a threat, such as thunderstorm, which creates a risk.
Risk Management Handbook	The Risk Management Handbook (RMH) compiles CMS standards, requirements, directives, practices, and procedures for protecting CMS information and information systems.
RiskVision	Incident report and tracking system used by HHS and CMS.
Rootkit Software	A type of malicious software (Malware) - Software intended to take full or partial control of a system at the lowest levels. Contamination defined as inappropriate introduction of data into a system.
Routine Use	Means with respect to the disclosure of a record, the use of such record for a purpose that is compatible with the purpose for which it was collected. With respect to Privacy Act System of Records, the agency's policy is to account for all routine use disclosures.
RSA Archer	RSA Archer is a modulated platform that assists in building an efficient, collaborative governance, risk and compliance (GRC) program. For more details see: http://www.ndm.net/rsa/Archer-GRC/archer-grc-modules
Rules of Behavior	Guidelines describing permitted actions by users and the responsibilities when utilizing a computer system. The rules that have been established and implemented concerning use of, security in and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment, and limitation of system privileges, and individual accountability.
Scenario	A sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce

Terms	Definitions
	situations that will inspire responses and thus allow demonstration of the exercise objectives.
Security Incident	In accordance with *NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide*, a security incident is defined as an event that meets one or more of the following criteria: • The successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in any information system processing information on behalf of CMS. It also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put CMS data at risk of unauthorized access, use, disclosure, modification, or destruction • An occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits • A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
Security Support Structure Configuration Modification	A type of malicious software (Malware) - Software, hardware and system configurations contributing to the Security Support Structure (SSS) are controlled. SSS is essential to maintaining the security policies of the system, unauthorized modifications to these configurations can increase the risk to the system.
Senior Official for Privacy	The SOP must be an agency official (federal government employee) and must fulfill all of 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.
Spillage	Instances where sensitive information (e.g. classified information, export-controlled information) is inadvertently place on information systems not authorized to process such information.
Spyware	A type of malicious software (Malware) that has surreptitiously installed and intended to track and report the usage of a target system, or collect other data the author wishes to obtain.
System of Records	Any records under the control of CMS from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
Tabletop Exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing the roles during an emergency and the responses to particular emergency. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

Terms	Definitions
Tabletop Test	An exercise with injects scripted by exercise planners and delivered via paper (cards/discussion).
Technical Vulnerability	A technical vulnerability is a hardware, firmware, or software weakness or design deficiency that leaves a system open to potential exploitation, either externally or internally, thus increasing the risk of compromise, alteration of information, or denial of service.
Test	An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environmental specified in an IT plan.
Test Plan	A document that outlines the specific steps performed for a particular test, including the required logistical items and expected outcome or response for each step.
Test, Training, and Exercise (TT&E) Event	An event used to support the maintenance of an IT plan by allowing organizations to identify problems related to an IT plan and implement solutions before an adverse situation occurs.
Test, Training, and Exercise (TT&E) Plan	A plan that outlines the steps taken to ensure that personnel are trained in IT plan roles and responsibilities. TT&E plans exercised to validate the viability of how IT components or systems are tested and to validate the operability in the context of an IT plan.
Test, Training, and Exercise (TT&E) Policy	A policy that outlines an organization's internal and external requirements associated with training personnel, exercising IT plans, and testing IT components.
Test, Training, and Exercise (TT&E) Program	A means for ensuring that personnel are trained in IT plan roles and responsibilities; TT&E plans are exercised to validate the viability; and how IT components or systems are tested to validate operability.
Test, Training, and Exercise (TT&E) Program Coordinator	A person who is responsible for developing a TT&E plan and coordinating TT&E events.
Threat(s)	The potential to cause unauthorized disclosure, changes, or destruction to an asset. • **Impact:** potential breach in confidentiality, integrity, failure and unavailability of information • **Types:** natural, environmental, and man-made
Training	Informing personnel of roles and responsibilities within a particular IT plan and teaching personnel skills related to those roles and responsibilities.
Transaction	The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: • Health care claims or equivalent encounter information.

Terms	Definitions
	• Health care payment and remittance advice. • Coordination of benefits. • Health care claim status. • Enrollment and disenrollment in a health plan. • Eligibility for a health plan. • Health-plan premium payments. • Referral certification and authorization. (https://privacyruleandresearch.nih.gov/dictionary.asp
Trojan Horse	A type of malicious software (Malware) – a useful and innocent program containing additional hidden code that allows unauthorized computer network exploitation (CNE), falsification, or destruction of data.
Use	The sharing, employment, application, utilization, examination, or analysis of personally identifiable information (PII) and PHI within the covered entity that maintains such information. (https://privacyruleandresearch.nih.gov/dictionary.asp
Virus	A type of malicious software (Malware) that is propagated via a triggering mechanism (e.g., event time) with a mission (e.g., delete files, corrupt data, send data).
Vulnerabilities	Any flaw or weakness that can be exploited and may result in a breach or a violation of a system's security policy.
Waiver or Alteration of Authorization	The documentation that the covered entity obtains from a researcher or an IRB or a Privacy Board that states that the IRB or Privacy Board has waived or altered the Privacy Rule's requirement that an individual must authorize a covered entity to use or disclose the individual's PHI for research purposes. (https://privacyruleandresearch.nih.gov/dictionary.asp
Workforce	Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of the covered entity, whether or not they are paid by the covered entity. (https://privacyruleandresearch.nih.gov/dictionary.asp
Worm	A type of malicious software (Malware) that is an unwanted, self-replicating autonomous process (or set of processes that penetrates computers using automated hacking techniques.

2025

Appendix C. Applicable Laws and Guidance

Appendix C provides references to both authoritative and guidance documentation supporting the "document." Subsections are organize to "level of authority" (e.g., Statutes take precedence over Federal Directives and Policies). The number on each reference represents a mapping that uniquely identifies the reference within the main body of the document. The brackets [#] in the Roles and Responsibilities section are the actual brackets in the "Policy." In this document, the brackets serve as an example of how the brackets will appear in both sections of the document.

C.1 Statutes

1 Federal Information Security Modernization Act (FISMA) of 2014
https://www.congress.gov/bill/113th-congress/senate-bill/2521

2 Health Insurance Portability and Accountability Act of 1996 (HIPAA)
http://www.hhs.gov/hipaa/

3 The Privacy Act of 1974, as amended (5 U.S.C. 552a)
http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/PrivacyActof1974.html

4 Code: 5 U.S.C. §552a(e)(10)
http://www.gpo.gov/fdsys/granule/USCODE-2010-title5/USCODE-2010-title5-partI-chap5-subchapII-sec552a/content-detail.html

5 E-Government Act of 2002 (Pub. L. No. 107-347) § 208
https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html

C.2 OMB Policy and Memoranda

1 OMB Circular A-130 Management of Federal Information Resources
http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

2 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (OMB Memorandum M-03-22)
http://www.whitehouse.gov/omb/memoranda_m03-22/

3 OMB M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*

https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf

C.3 NIST Guidance and Federal Information Processing Standards

1 NIST SP 800-53-r4, *Security and Privacy Controls for Federal Information Systems and Organizations*

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

2 NIST SP 800 53Ar4 *Guide for Assessing the Security Controls in Federal Information Systems*

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

3 US-CERT Federal Incident Notification Guidelines

https://www.us-cert.gov/incident-notification-guidelines

4 NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*

http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

C.4 HHS Policy

1 *HHS-OCIO-2014-0001 HHS Information System Security and Privacy Policy (HHS IS2P)*

To obtain a copy of this document, please email fisma@hhs.gov

2 *HHS-OCIO-2008-0001.003 HHS Policy for Responding to Breaches of Personally Identifiable Information*

http://www.hhs.gov/ocio/policy/20080001.003.html

3 *HHS-CSIRT Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response*

http://www.hhs.gov/ocio/policy/hhs_ocio_policy_2010_0004.html

C.5 CMS Policy and Directives

1 *CMS Information Systems Security and Privacy Policy (IS2P2)*

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS2P2.pdf

Appendix D. Feedback and Questions

Information security is a dynamic field and as such policies, standards, and procedures must be continually refined and updated. Feedback from the user community is invaluable and ensures that high quality documents are produced and that those documents add value to the CMS community. Should you have any recommendations for improvements to this document, please email the ISPG Policy mailbox at ISPG_Policy_Mailbox@cms.hhs.gov. Your feedback will be evaluated for incorporation into future releases of the document. Questions about any of the material include within this document may also be sent to the ISPG Policy mailbox.