CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF STRATEGIC OPERATIONS
& REGULATORY AFFAIRS

CMS Policy for Records and Information Management

Records & Information Management
PROGRAM

May 10, 2022
Version 2

Table of Contents

Table of Contents 2
Executive Summary 5
1. Program Scope and Objectives 6
Purpose 6
Scope 6
Background 6
RIM Authorities for CMS 7
1.1 Roles and Responsibilities 8
2. Identifying Records 11
2.1. What is a Record? 11
2.2. Information as Records 11
2.3. Types of Records 12
2.4. Metadata for Records and Records Management 15
2.5. Judicial Use of Electronic Records 16
2.6. Non-records 16
2.7. Personal Papers 17
2.8. Working Files 17
3. Scheduling Records 18
3.1. Records Inventory 18
3.2. File Plans 18
3.3. Records Schedules 19
3.4. CMS Bucket Schedule 19
3.5. Reviewing Records Schedules 19
3.6. Approval of Records Schedules 19
4. Active Records 20
4.1. Creating and Receiving Records 20
4.2. Recordkeeping Systems 20
4.3. Maintenance 24
5. Inactive Records 25
5.1. Closing Records 25
5.2. Retiring Inactive Records 26
5.3. Transferring Records 26
5.4. Destroying Records 27
5.6. Capital Planning and Investment Controls 29

6. Training and Evaluations 30
6.1. Annual Records and Information Management Training 30
Appendix A: References 31
Appendix B: Centers for Medicare & Medicaid Services Materials Removal Certification and Non-Disclosure Agreement 33
Appendix C: Centers for Medicare & Medicaid Services Certification and Non-Disclosure Agreement 34

Table of Changes

Version	Date	Edits	Author
1.0	January 3, 2022	Initial Publication	OSORA/IRISG/DRIS
2.0	May 10, 2022	Updates to Section 4	OSORA/IRISG

Executive Summary

This policy establishes the Records and Information Management (RIM) principles and practices for managing the Centers for Medicare & Medicaid Services (CMS) important records and information assets. Proper RIM practices support CMS' mission and goals while ensuring compliance with the strict records and information Laws, Regulations, and Government-Wide Policies (LRGWP). One such LRGWP is the Office of Management and Budget (OMB) Memorandum M-19-21 "Transition to Electronic Records," which directs all Federal agencies to:

1. Ensure that all Federal records are created, retained, and managed in electronic formats, with appropriate metadata;
2. Consistent with records management laws and regulations, develop plans to close agency-operated storage facilities for paper and other, analog records, and transfer those records to Federal Records Centers operated by NARA or commercial storage facilities; and
3. Maintain robust records management programs that comply with the Federal Records Act and its regulations.

M-19-21 also establishes specific deadlines that CMS must meet to remain compliant:

- By 2019, Federal agencies will manage all permanent electronic records in an electronic format.
- By 2022, Federal agencies will manage all permanent records in an electronic format and with appropriate metadata.
- By 2022, Federal agencies will manage all temporary records in an electronic format or store them in commercial records storage facilities.

The RIM Program Policy outlined within this document shall serve as official guidance for CMS employees, contractors, and other audiences identified as responsible for the creation, maintenance, management, use, retention, and disposition of CMS Federal records.

The Centers for Medicare & Medicaid Services combines the oversight of the Medicare program, the federal portion of the Medicaid program and State Children's Health Insurance Program, the Health Insurance Marketplace, and related quality assurance activities. The Office of Strategic Operations and Regulatory Affairs (OSORA), Division of Records and Information Systems (DRIS) provides direct services and develops policy, standards, and procedures for CMS' RIM Program operations throughout the Operational Division (OpDiv).

1. Program Scope and Objectives

Purpose

The purpose of this policy is to establish the principles, responsibilities, and requirements for managing CMS records and information. As the agency continues its transition to an electronic records and information management process, this policy provides the framework for the RIM Program guidance and operating procedures, which covers records and information in all formats, including both physical and electronic records.

This CMS Records and Information Management Policy is written in accordance with Title 44 Chapter 33 of the United States Code (U.S.C.), Title 36, Chapter 12 of the Code of Federal Regulations (CFR), and Federal Continuity Directives (FCD) 1 and 2.

Scope

This policy applies to all personnel (federal and contractor) at each CMS Component and conducting business for and on behalf of CMS through contractual relationships and service level agreements. Within this policy, the term Component includes all CMS Staff Offices and Regional Office locations.

All CMS personnel (federal and contractors) are obligated to meet the requirements of this policy. CMS is required to integrate records and information management into the overall information resources management program, in accordance with 36 CFR Subchapter B, Records and Information Management, and Office of Management and Budget (OMB) Circular A-130 (Revised), Management of Federal Information Resources.

This policy supplements HHS-OCIO-PIM-2020-06-004,the Department of Health and Human Services Records Management Policy, and provides CMS specific guidance for records and information management enterprise-wide at CMS. This policy also supplements HHS Policy for Implementing Electronic Mail (Email) Records Management, HHS-OCIO-PIM-2020-06-005, implemented in May 2020. More information regarding email records is included in Section 2.3.3 of this policy.

CMS Records and Information Management (RIM) Policy

The purpose of this document is to ensure compliance with applicable statutory and regulatory requirements that every employee is required to adhere to CMS records and information management program guidelines. This document establishes policy and assigns responsibility for the lifecycle management (creation, maintenance use, and disposition) of information as records regardless of media or format.

Background

Records and information management is the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved in records creation, maintenance and use, and disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations (44 U.S.C. 2901). Records and information management addresses the life cycle of records, (i.e., the period of time that records are in the custody of Federal agencies). The life cycle usually consists of three stages:

- Creation or receipt;
- Maintenance and use; and
- Disposition.

The National Archives and Records Administration (NARA) assists in preserving our nation's history by overseeing the management of all Federal records. The NARA Act of 1984 amended existing records and information management statutes and divided program oversight responsibilities between the NARA and the General Services Administration (GSA). Under the Act, NARA is responsible for adequacy of documentation and records disposition (44 U.S.C. 2904(a)), and GSA is responsible for economy and efficiency in records and information management (44 U.S.C. 2904(b)). Across the federal government, every RIM Program must comply with regulations promulgated by both NARA (36 CFR 1220.2) and GSA.

Records, data and information are key strategic assets of the agency and are the evidence of the operations and business transactions. A well-managed records and information management program is the foundation of a responsible, accountable organization and is the underpinning of public service transformation and innovation strategies such as data-driven evaluation and evidence-based decision-making. The agency RIM office must account for all agency records and have an effective RIM Program that captures the business activities of the agency to ensure compliance with Federal laws and regulations. Specific legal requirements for records and information management include:

- Creating and preserving records that contain adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the Agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the Agency's activities (44 U.S.C. 3101).
- Establishing and maintaining an active, continuing program for the economical and efficient management of the records of the agency (44 U.S.C. 3102).
- Establishing safeguards against the removal or loss of records and making requirements and penalties known to agency officials and employees (44 U.S.C. 3105).
- Notifying the Archivist of any actual, impending, or threatened unlawful destruction of records and assisting in their recovery (44 U.S.C. 3106).

All employees are responsible for records and information management and have three basic obligations regarding records under their control:

- Create records needed to document the business of CMS, record decision-making and actions taken, and document activities for which they are responsible.
- Manage records so that information can be found when needed. This means (1) establishing proper organization structures, metadata labels, searchable indexes, and navigation schemes and (2) filing materials (in any format) consistently and carefully to ensure safe storage and efficient retrieval.
- Carry out the disposition of records under their control in accordance with CMS Records Schedules, Federal regulations and agency policy. The preservation of records may be required under agency policy that this is not clearly stated in established records schedules or other Federal regulations.

RIM Authorities for CMS

CMS must follow strict laws, regulations, and policies regarding the management and protection of information, including:

- Health Insurance Portability and Accountability Act (HIPAA);
- Federal Records Act (FRA);
- Freedom of Information Act (FOIA);
- National Institute of Technology (NIST) mandates;
- International Organization for Standardization (ISO) standards;
- National Archives and Records Administration (NARA) guidance;
- Office of Management and Budget (OMB) mandates, including M-19-21 "Transition to Electronic Records";
- HHS mandates; and
- Executive RIM mandates.

The list of LRGWPs can be found in Appendix A. This list is not all inclusive and may be subject to review and update of this policy document.

1.1 Roles and Responsibilities

To provide a clear system of accountability and responsibility for record keeping and use:

1.1.1. Responsibilities for CMS Employees and Contractors

CMS employees are responsible for the protection of Federal records in their custody and following policies and guidance governing maintenance, use, and destruction of records. Following good records and information management practices benefits CMS in many ways including, but not limited to: improving access to information, effective stewardship of public funds, strengthening the nation's health care system, and modernizing the nation's health care system. There are legal implications for destroying records without the proper authority. (44 U.S.C. 3106).

Federal records shall be properly managed regardless of media or format. Some common formats of federal records created, received, and stored by CMS may include, but are not limited to: paper, electronic (including email), and audio-visual. Records document the organization's functions, policies, decisions, procedures, operations, and other activities.

Keys to good recordkeeping practices include but are not limited to retaining and managing only what is legally required to be managed, managing records in a way that facilitates access, retention, and disposition, and doing so consistently. This policy is designed to help employees and contractors understand their roles and responsibility in the management of CMS records/

When in doubt about whether information assets are records, employees and contractors should always contact their Component Records Liaison Officers (RLOs) and/or OSORA for assistance.

1.1.2. Updating the CMS RIM Policy

This policy must be adapted periodically to accommodate changes in rules and regulations, changes in organizational business requirements, and changes in technology. The CMS Records Officer shall determine when changes are necessary and will lead the effort to make those changes every three (3) years.

1.1.3. The Office of Strategic Operations and Regulatory Affairs (OSORA)

OSORA is responsible for the planning, development, and coordination of the Agency's records and information management program in accordance with Federal regulations (36 CFR 1220-1239). The Records and information management Program ensures that CMS is in compliance with federal laws and regulations, Department of Health and Human Services and CMS policies, and best practices for managing the Agency's records.

1.1.4. OSORA Director

The OSORA Director provides leadership, direction, and advocacy on behalf of the Administrator and other Senior CMS Executives on critical policy and operational decision documents and manages CMS' vetting process for all critical documents requiring the Administrator's signature. The OSORA Director serves as the CMS Senior Agency Official (SAO) for Records and Information Management.

1.1.5. CMS Records Officer (RO)

The CMS Records Officer (RO) (also referred to as the Agency Records Officer (ARO)) is responsible for leading and managing CMS national RIM Program and ensuring Senior CMS Executives are aware of their programmatic and individual records and information management responsibilities.

The CMS RO serves as the primary official who coordinates RIM Program matters with NARA and other oversight agencies and also provides leadership, guidance (developing policies, standards, and procedures), and training to ensure uniformity in records and information management activities throughout CMS.

1.1.6. CMS Freedom of Information Act (FOIA) Officer

The Freedom of Information Group (FIG) or the Office of General Counsel (OGC) can assist Components in determining if a document is discoverable under FOIA. Regardless of media type, all existing records in CMS' possession, custody and control are subject to the FOIA.

1.1.7. Component Records Liaison Officers (RLO)

Component Records Liaison Officers (RLOs) are responsible for creating and preserving records that adequately and properly document the organization, functions, policies, decisions, procedures, and essential transactions of CMS within their respective Components.

Additionally, RLOs are responsible for evaluating the value of records, creating and maintaining component file plans, assisting with disposition activities, supporting the development of records and information management training, creating and updating component specific procedures, reviewing records schedules and file plans, and evaluating their Component-level records programs.

1.1.8. Records Custodians (RC)

The Records Custodian is responsible for the management and disposition actions for a particular set of records for their Group/Division program or business requirements. The Records Custodian can potentially be designated as the Component Records Liaison Officer or another CMS employee.

1.1.9. Component Litigation Hold Coordinators

Component Litigation Hold Coordinators are responsible (in consultation with OSORA and the Office of General Counsel (OGC)) for the CMS policy direction and administrative management of litigation holds and document preservation for their Component. The Component Litigation Hold Coordinator liaises with other CMS Components to ensure compliance with 1) preserving relevant information under a litigation hold is an operational consideration rather than a legal requirement and 2) Litigation Hold Coordinators are making unilateral decisions rather than implementing established agency policy.

1.1.10. Essential Records Coordinators

The Essential Records Coordinator is responsible for a particular set of records for their Component's Essential Records program or business requirements. The Essential Records Coordinator receives specified training on the management and retrieval of their respective Component's essential records in the case of a Continuity of Operations (COOP) or disaster recovery instance. Essential records in this context may also be referred to as vital records for each Component.

1.1.11. Management and Supervisory Officials

Managers and Supervisory Officials are responsible for ensuring federal employees, contractors and intermittent employees (i.e., volunteers and interns) are aware of and adhere to CMS Records policies.

1.1.12. CMS Personnel

All CMS personnel (federal and contractor) shall follow CMS' records and information management policies, procedures, and guidance. CMS personnel are responsible for creating and managing the records necessary to document CMS' official activities and transactions (including records generated by CMS contractors and grantees), the disposition of records in accordance with approved records schedules, and other preservation obligations, and safekeeping (which includes non-removal of records from CMS without authorization). All CMS personnel must ensure that personal papers and non-record materials are stored separately from official CMS records.

(a) Telework

With the exception of agency-specific policies, the general records and information management responsibilities of a CMS employee do not change in the telework environment. Employees should remember that these responsibilities apply to the management of both federal records as well as non-records, such as reference copies. CMS employees shall follow agency policies for managing official records in a telework environment, such as returning files to its filing system and managing copies of records created in the course of teleworking. CMS policies may depend on approved telework methods (working on agency-supplied laptop computers, using a Virtual Private Network, emailing work to and from the telework site, etc.).

1.1.13. CMS Contractors

Use of contractor's site and services may require management of Federal records. If the Contractor holds Federal records, the Contractor must manage Federal records in accordance with all applicable records management laws and regulations, including but not limited to the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33), and regulations of the National Archives and Records Administration (NARA) at 36 CFR Chapter XII Subchapter B). Managing the records includes, but is not limited to, secure storage, retrievability, and proper disposition of all federal records, including transfer of permanently valuable records to NARA in a format and manner acceptable to NARA at the time of transfer. The agency also remains responsible under the laws and regulations cited above for ensuring that applicable records management laws and regulations are complied with through the life and termination of the contract.

1.1.14. The Office of General Counsel (OGC)

The Office of the General Counsel reviews proposed policy for official records and provides procedural guidance for implementing litigation holds. The Office of the Inspector General (OIG)

The Office of Inspector General assists in investigating the unauthorized removal and destruction of records and the actual and potential threats to records (e.g. removal, alteration, or deliberate or accidental destruction).

1.1.15. The Office of Information Technology (OIT)

The Director of the Office of Information Technology (OIT) and serves as the CMS's Chief Information Officer and is responsible for providing implementation services and operational support for CMS component-specific information technology (IT) needs and enterprise-wide services.

2. Identifying Records

Regardless of media, an assessment of agency records shall be conducted in accordance with 44 U.S.C. 3301, to properly identify them as official records, non-records or personal papers. Identifying the records that support the agency's work is the foundation of a successful RIM Program. The records shall be managed according to the Agency and General Records Schedule.

2.1. What is a Record?

The Federal Records Act defines a record as follows:

''records'' includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. (44 U.S.C. 3301)

A record accurately reflects what was communicated, what was decided, or what action was taken. An accurate record will support the needs of the business to which it relates. Furthermore, a record documents CMS' actions to the public, provides evidence for Congress and litigations, and is the motive for FOIA requests. A federal record is an information resource that is created in the course of business, received for action, or needed to document CMS activities. In some cases, the information resource can be identified as a record to various stakeholders, possibly under different records schedules. For example, a letter establishing a partnership between CMS and a state agency may be a record under general correspondence for the senior official who sends it, and a record under program management for the component managing the project. Please refer to the 'Is It a Record?' diagram, which provides additional guidance to help determine whether information created is a record.

2.2. Information as Records

Records can vary widely in forms or characteristics. Records include various forms such as paper, electronic, audiovisual, microform, or other media.

CMS records must contain documentation that is adequate and proper in accordance with applicable LRGWP. The documentation must show a clear picture of how CMS conducts its business and makes decisions. CMS Components should consider the following when determining if and how much documentation is necessary: legal risk, audit needs, day-to-day management, public access requirements, and historical significance.

Certain activities require extensive documentation. These activities potentially have statutory or regulatory requirements, in addition to CMS specific requirements. These activities include but are not limited to rulemaking, guidance to the regulated community, policy development, budget development,

enforcement activities, compliance activities, scientific research and publication, and activities of the Federal Advisory Committees.

The lifecycle of a record is the period of time records are in the custody of federal agencies from its inception to disposal (creation, maintenance, use, and disposition). Records are maintained and used throughout two lifecycle phases as active records and inactive records. Active records are used to conduct current CMS business and may be maintained in an office space, equipment or within designated information systems and records and information management repositories. Inactive records that are not needed for current business and are typically maintained in an off-site storage area or an electronic archive.

A record begins as a document that is created or received. The record must be captured in a recordkeeping system if that document meets the definition of a record. The record is considered as "closed" when the record is no longer needed for current CMS business. Once closed, if the record is permanent, it is retained indefinitely due to its historical significance, the record is transferred to the National Archives. Once closed, if the record is a temporary record, it has a finite lifecycle, the destruction of records in accordance with approved records schedules and other preservation obligations.

2.3. Types of Records

Federal records are treated the same whether they are analog or digital independent of their form and format.

2.3.1. Paper Records

Paper records are defined as physical records that are created in support of an agency's mission and functions. Paper and other analog types of records are managed according to well-established records management practices. Going forward, all processes and resulting records must become digital. This will typically involve the digitization of existing paper records as described in Electronic Records below.

2.3.2. Electronic Records

Electronic records or e-records are records stored in a form that only a computer can process. Records can be numeric, graphic, and text information; media can include, but are not limited to, magnetic media, such as tapes and disks, and optical disks. Examples of electronic records include, but are not limited to: websites, email, social media, digital images, databases, and documents created using desktop applications. Electronic records include information or data created using electronic mail, and other messaging applications, word processing, or presentation software which must be managed in a records and information management solution. Email records must be retained in an appropriate electronic system that supports records and information management and litigation requirements, including preservation and in-place models, when necessary

CMS is transitioning to an electronic records and information management approach to identify, digitize, and transfer to NARA any physical, hard-copy format or other analog records, such as microfiche,

microfilm, analog video, and analog audio, to be in compliance with the Presidential Memorandum and OMB Directive M-19-21 "Transition to Electronic Records." OMB Directive M-19-21 is supported by the Federal Electronic Records Modernization Initiative (FERMI), which emerged from the Automated Electronic Records and information management Plan. FERMI is NARA's effort to provide a government-wide, modern, cost-effective, standardized, and interoperable set of records and information management solutions and services for Federal agencies.

The enterprise-wide approach implements an electronic records management (ERM) solution throughout the agency by utilizing existing SharePoint software and an add-on of the Gimmal GRM software that deploys the SharePoint Records Center functionality to actively manage documents and official records. The use of the ERM tool incorporates the CMS Records Schedule (Big Bucket Schedule) and the NARA General Records Schedule (GRS) big bucket approach into SharePoint, Box, and any other CMS document repository which is not already scheduled, and applies the ERM functions and features which captures, manages, stores, and preserves documents and official records regardless of medium or location. The ERM tool enables the overall coordination of all records and information management activities and ensure compliance with legislative mandates. The ERM solution also integrates electronic records and information management practices with other information systems and repositories.

2.3.3. Email Records

Electronic mail systems are computer applications used to create, receive, and transmit messages and other documents. An email message is a record if it documents the CMS mission or provides evidence of CMS business processes. Both the sender and the recipient of an email message have a responsibility to document their activities and those of their organizations and must determine whether a particular email message is a necessary part of that documentation. CMS email accounts may contain Federal records. Emails received by employees directly to their CMS email addressed are not to be removed from their native email system.

Additionally, agency officials may inadvertently create Federal records if they conduct agency business on their personal email accounts. Emails sent on personal email accounts pertaining to agency business and meeting the definition of Federal records must be filed in the agency recordkeeping system most appropriate for the contents and record type of said email.

2.3.3.1. Capstone Email Approach

The Capstone email approach is a simplified and automated approach to managing email. Using the Capstone approach, CMS categorizes and schedules email based on the work and/or position of the email account owner, allowing the capture of records that should be preserved as permanent from the accounts of officials at or near the top of CMS Component.

CMS designates email accounts of specific positions as Capstone Officials when they are in roles that are likely to create or receive permanent email records. By utilizing this approach, CMS schedules emails in Capstone Officials accounts as permanent records. This approach supports the Presidential Memorandum on Managing Government Records and allows the agency to comply with the requirement in OMB/NARA M-19-21 "Transition to Electronic Records" Directive to manage both permanent and temporary email records in an accessible electronic format with appropriate metadata. An updated list of Capstone Officials can be retrieved by contacting DRIS.

2.3.4. Special Media Records

Special media records are maintained separately from other records because of their physical forms or unique characteristics which require unusual care. Examples of special media records include, but are not limited to: cartographic (maps, architectural & engineering drawings, aerial photography), motion pictures (film, sound and video recordings), still pictures (photographs). Special media records should include finding aids to provide context for the records and cross-references to and from related textual records.

2.3.5. Media Neutrality of Records

Federal records are no longer limited to physical, analog documents and may be in any format or medium, such as: paper, electronic, film, disk, maps, photographs, or other physical type or form. This concept is often referred to as media-neutral. The method of recording information may be manual, mechanical, photographic, electronic, or any combination of these, or other technologies. Regardless of the media type, federal records must be properly managed in accordance with the records lifecycle.

Records schedules submitted on or after December 17, 2007 are considered media neutral and apply to all formats of records. Unless otherwise specified, schedules approved prior to December 17, 2007 are not media neutral and apply only to paper records. Therefore, records identified in non-media neutral schedules can only be digitized for access and the paper records cannot be destroyed until reaching their designated retention period.

2.3.6. Social Media Records

CMS must manage record material produced or posted using social media such as Facebook, YouTube, Twitter, Instagram, and other similar technologies. The following records and information management considerations must be addressed with the use of these technologies:

CMS employees must capture and manage social media records in accordance with approved Records Control Schedule (RCS), information that meets the statutory definition of a federal record (44 U.S.C. 3301)

1. More than one office/agency may have a responsibility for the same records, depending on their use.

2. All records must be managed in accordance with the content captured and not the format or the records.

3. All records determined to have permanent value must be transferred to NARA in an approved format. Permanent records may have to be migrated from their original format to one accepted by NARA at the time of transfer.

For additional information and guidance, contact the CMS Office of Communications (OC) or reference the NARA Bulletin 2014-02: Guidance on Managing Social Media Records (2014) and HHS-OCIO-PIM-2020-06-004.

2.3.7. Agency Approved Electronic Messaging Systems

Electronic messaging systems should only be used for informal business communications and collaborations.

Examples of suitable use include but are not limited to:

a. Real-time, quick communications among employees relating to requests for information/status that require no follow-up actions or business decisions and do not form the basis for action or decision, such as communications to inform an employee that a document is ready for signature, a request to review draft work products (including attachments), or to inquire about an employee's availability for a phone call or meeting.

b. Casual reminders, such as notification about a change to one's schedule, reminder of a deadline, or scheduling of work-related trips and visits.

CMS employees should not use electronic messaging systems to engage in discussions regarding policy matters, business decisions, or documentation of other mission-critical functions. Doing so could result in the creation of a federal record that requires retention and disposition actions within the context of the overall records of the program to which the instant message relates and the business rules that may apply per the CMS Retention Schedule. Examples of unsuitable use include, but are not limited to:

a. Communications documenting CMS policy reviews and approvals, pre-decisional or decisional discussions.

b. Discussions about examinations and/or case processing and resolution.

c. Communications regarding personnel matters and performance (e.g., disciplinary actions, disputes, or grievances).

CMS / OIT has configured the automated capture of all instant messages sent or received via CMS owned and operated Electronic messaging systems. Instant messages that are subject to a litigation hold, regardless of whether the messages meet the definition of federal records, must be saved prior to closing out of the message to ensure preservation.

2.3.8. Text Messages and Mobile Communication Devices

The use of text messaging with government-furnished mobile devices or cellular phones is discouraged and should be limited to quick, information communications and reminders. Similar to agency approved electronic messaging systems, Users who create records via text messages on government-furnished mobile devices must document the information communicated as records and transfer to an approved recordkeeping system within 20 days of the original creation or transmission of the record (per the Federal Records Act), (44 U.S.C. § 2911) with all corresponding and appropriate record metadata. This may be accomplished by copying the text message into a government-provided email account. Text messages and other information on mobile communication devices may be subject to discovery and FOIA.

2.3.8.1 Text Message Auto-capture Retention

As applicable by OIT Enterprise Technology Solutions (ETS), CMS may leverage existing or future OIT software solutions to automate the capture, retention, and disposition of text messages and mobile device data as a federal record. Such actions shall be coordinated with OSORA to ensure all FRA, 44 U.S.C. § 2911, and 36 C.F.R. § 1236 requirements are adhered to.

2.4. Metadata for Records and Records Management

A key component of managing records and information assets is applying the right metadata, which is information about the information. Examples of metadata include document title, document identifier, author, date created, component, type of file, and more properties. Metadata must be managed just like any other part of the RIM program.

Metadata for records will be applied automatically to the greatest extent possible as the CMS RIM program continues to mature. This practice prevents putting an extra burden on information users to manually apply metadata in many circumstances. This practice also increases efficiency and accuracy of applying metadata to records and information assets.

Each component and process have their own metadata requirements for their specific types of records. The RIM program will work with components to ensure their metadata requirements are met for managing their records.

2.5. Judicial Use of Electronic Records

Electronic records may be admitted as evidence to federal courts for use in court proceedings if trustworthiness is established by thoroughly documenting the recordkeeping system's operation and the controls imposed upon it (Federal Rules of Evidence 803(8)). CMS Components should implement the following procedures to enhance the legal admissibility of electronic records:

1. Establish and document standardized processes to create and retrieve similar kinds of records generated and stored electronically;
2. Verify that security and audit procedures prevent unauthorized addition, modification, or deletion of a record and ensure system protection against such problems as power interruptions;
3. Identify the electronic media on which records are stored throughout their life cycle, the maximum time span that records remain on each storage medium, and the NARA-approved disposition of all records; and
4. Coordinate all of the above with the Office of General Counsel, the CMS Records Officer and senior OSORA RM staff as necessary.

2.6. Non-records

Non-records are government-owned documentary materials excluded from the legal definition of records. The materials are typically excluded for one of two reasons:

(1) The materials do not meet the general conditions of record status already described, and

(2) The materials fall under one of three specific categories of records.

   a. The first category of records includes extra copies of documents preserved only for convenience or reference.

   b. The second category records include reference copies of stocks of publications; however, CMS must maintain a record copy of publications, including annual and special reports, special studies, brochures, pamphlets, books, handbooks, manuals, posters and maps.

   c. The third category of records includes library and museum material created or acquired and preserved solely for reference or exhibition purposes.

Examples of non-records include: copies of correspondence, directives, forms and other documents on which CMS takes no administrative action, such as, but not limited to: routing slips, transmittal sheets, catalogs, trade journals, physical exhibits, artifacts, and other material objects lacking evidential value.

Typically, an information resource is a record for a single custodian, and all other copies are non-records. For example, a memorandum circulated agency-wide that does not require action is a record for the individual or organization issuing the memorandum but is a non-record for its recipients.

There are specific guidelines which apply to managing non-records. CMS staff should treat these materials as records when it is difficult to discern whether these documents are records or non-record material. Non-record material should not be interfiled with official records. Absent specific preservation obligations (e.g., litigation hold), non-records must be destroyed when they are no longer needed for reference, and extra copies may not be retained after the record copy is destroyed.

2.7. Personal Papers

Personal papers are materials which do not meet the definition of a record or non-record and belong to an individual. The materials are not used to conduct CMS business. These materials relate solely to an individual's personal and private affairs and are used exclusively for that individual's convenience. In contrast to records and non-records, the government does not own personal papers. The owner will clearly designate and manage all personal papers and keep them separate from all records and non-records. However, labeling documentary materials personal, confidential, or private, is not sufficient to determine the status of documentary materials.

Personal papers include various categories.

1. Personal papers include materials an individual accumulates before joining government service that are not used later to conduct government business.
2. Materials that relate solely to an individual's family matters, outside business pursuits, professional activities, or private associations are personal papers.
3. Work-related materials that an individual does not prepare, receive or use to transact CMS business are personal papers (e.g., reminders and personal observations about work and other topics).

Examples of personal papers include: political materials, insurance papers, medical papers, volunteer service records, manuscripts not related to CMS business, drafts of articles and books not related to CMS business diaries, journals, personal calendars, and appointment schedules.

2.8. Working Files

Working files are rough notes used to prepare or analyze business documents. Rough notes consist of calculations or document drafts. Working files are sometimes needed to adequately document CMS business activities. Staffs must give special attention to these files to ensure that they are not needed to supplement formal records.

Working files that must be preserved as records include: proposals or evaluations of options, alternatives and their implications in the development of policies and decisions, documented findings, supported recommendations, or comments received via a formal CMS comment process.

In many cases, employees may destroy working files once the content is incorporated into official records provided no specific preservation obligations apply (e.g., litigation hold). Working files that may be disposable once a document is finalized are those that: receive no official action themselves, are not reviewed or approved by others, and are only used to prepare documents for official action such as review or signature. Working files also relate to preliminary, interim, or ancillary activities that are not needed as part of the official record.

Some records schedules specifically identify working files as records, but components shall make their own determination whether or not to incorporate working files into the record. Copies of records must not be kept in working files beyond the approved retention of the record copy.

3. Scheduling Records

CMS Records Schedule provides mandatory instructions (disposition instructions) to all staff regarding how to maintain operational records and what to do with them when they are no longer needed for current business. The disposition instructions state whether individual series of records are "permanent" or "temporary," as well as how long to retain the records. Records with historical value, identified as "permanent," are transferred to the National Archives of the United States at the end of their retention period. All other records are identified as "temporary" and are eventually destroyed in accordance with approved Agency schedule or the General Records Schedule. The destruction of records in accordance with approved records schedules and other preservation obligations.

3.1. Records Inventory

A records inventory is a detailed listing of the volume, scope, and complexity of the component's records. The records inventory is compiled for the purpose of creating a records schedule. Conducting an inventory is necessary to find out what files are actually in your office. Records inventories shall be conducted in coordination with the DRIS and the CMS records staff. Components conducting a records inventory shall incorporate any updates, reconciliations, and / or adjustments identified as reflected in their Component File Plan. With support from DRIS, components seeking to conduct a records inventory shall:

1. Define the inventory's goals,
2. Define the scope of the inventory,
3. Obtain top management's support,
4. Decide on the information to be collected,
5. Prepare the inventory form,
6. Identify and train the individual conducting the inventory,
7. Identify the location of the agency's files,
8. Conduct the inventory,
9. Verify results, and
10. Analyze the results.

3.2. File Plans

A file plan is a stand-alone document which lists the records in a component, and describes how they are organized and maintained. The file plan should include identifying information about records including: person and component responsible for maintaining the records (i.e., custodian), agency file code, folder title, medium (e.g., paper, electronic, video), access restrictions, location of the records, date range of the records, and disposition dates.

CMS requires components to organize records according to the agency-wide file structure. File plans should organize the directories in the same way to facilitate retrieval if a component maintains electronic

copies of records (e.g., on a shared drive). Components shall review file plans annually and notify DRIS of any necessary updates or changes made.

3.3. Records Schedules

CMS works with NARA on establishing retention periods for unscheduled record materials and recommending to NARA retention periods for records. Although NARA is solely responsible for appraising Federal records and approving their final disposition, CMS records officers need an understanding of appraisal objectives and standards to prepare and implement schedules.

Appraisal is the process by which CMS and NARA evaluate records to determine their final disposition, designating them as either temporary (disposable) or permanent (archival).

3.4. CMS Bucket Schedule

The CMS retention schedule consists of nine records subject categories referred to as “buckets”. The retention of all CMS records fall under one of the buckets according to the type of record. The records schedule will identify the authorized retention period for that specific bucket.

See CMS Bucket Schedule for more information.

See NARA GRS for more information.

3.5. Reviewing Records Schedules

The ARO is required to review CMS records schedules annually and send updates to NARA as necessary. The Component RLO shall conduct an annual review of their Component file plan, and notify the ARO if file plans need to be revised.

3.6. Approval of Records Schedules

All records schedules undergo an approval process with records and information management stakeholders to ensure they meet administrative, legal, and audit requirements. Stakeholders include CMS Components, NARA, and the Government Accountability Office (GAO). CMS Records and information management Program staff posts changes made during this process to the CMS Records Schedule.

3.6.1. Internal Approval Process

For new retention authorities, the ARO collaborates with the records program staff, to develop a records schedule that applies to a specific program. The records schedule is submitted to the Component’s RLO for approval.

The Component RLO reviews the records schedule to ensure it adequately describes the records to which it pertains and confirms that the schedule's retention and disposition meet the program's business needs. If the Component RLO does not concur, the ARO revises the schedule as needed and then resubmits it for approval by the RLO.

When the Component RLO approves the records schedule, the ARO submits the draft schedule to NARA.

3.6.2. NARA Approval Process

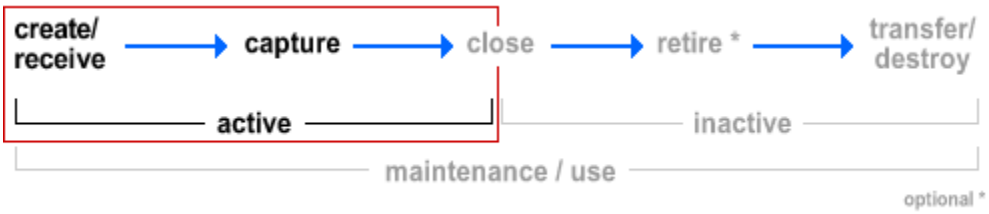
Record schedules exist for all CMS records. Final approval of the records schedules must be obtained from NARA in accordance with 36 CFR Chapter 12 Subchapter B. In most cases, NARA concurs in the disposition instructions agencies propose. However, issues may arise during the appraisal process that require revisions to a schedule prior to approval. These can stem from the appraiser's review of the schedule and/or the records they include, from input received from other NARA units which reviewed the schedule and appraisal report, or from the public. After CMS and NARA resolve any issues arising from

NARA review and Federal Register publication, the schedule is finalized and a dossier is created. The dossier is reviewed by NARA before being sent to the Archivist of the United States for approval. After the schedule is approved, NARA maintains the original (a permanent record) and posts on NARA's website.

CMS records must be listed and described in an approved records schedule, and shall be disposed of only as authorized by its disposition authority. CMS Components must update their file plans when there are program changes that will result in the establishment of new type of records and the transfer or termination of records, or an increase or decrease in the retention time of the records. (36 CFR § 1224.10(c)). CMS employees should alert their RLO and / or the ARO when these program changes occur.

4. Active Records

Active records are those used to conduct current CMS business, and are generally maintained in office space and equipment. The events in this phase of the lifecycle include creating or receiving records and capturing them in a recordkeeping system.



4.1. Creating and Receiving Records

Federal agencies are required to create and receive records that document how the agency is organized, the functions it performs, the carrying out of agency functions, its relation to other government agencies and the general public, or information of value to the agency.

CMS Components must determine what records they need to create or receive to meet these requirements. Records and information management points of contacts and CMS staff shall coordinate to ensure that complete and accurate records are created. Component RLOs should coordinate with DRIS in order to develop guidelines and procedures to incorporate the records creation and receipt process into their respective Component business functions.

4.2. Recordkeeping Systems

CMS Components must capture records in a recordkeeping system that facilitates maintenance and use of the records in an efficient and cost-effective manner. A recordkeeping system has various components:

1. OIT and System Owners: owners and maintainers of information systems which house either structured or unstructured data which is identified as a record.
2. People: RLOs and records contacts, who oversee aspects of records and information management, and custodians, who create, receive, and use records when conducting CMS business.
3. Processes: procedures to manage records throughout their lifecycle.
4. Tools: equipment and software used to capture, organize, store, track, and retrieve records, and
5. The records themselves.

4.2.1. Recordkeeping Systems

Recordkeeping systems assist in organizing records to facilitate their preservation, retrieval, use, and disposition. A recordkeeping system must allow records to be: organized for ready access and retrieval, configured to reflect approved records schedules, maintained for the time period required by the records schedules, and cross-referenced to related records stored on special media. Once records are organized within a recordkeeping system, the Component must regularly review the system to determine when records are ready to be closed, retired, and destroyed or transferred.

4.2.2. Special Considerations

(a) Verbal Conversations

Any verbal communication in which CMS business decision or commitment is made, and that is not otherwise documented, needs to be captured and placed in a recordkeeping system. Voicemail systems are not recordkeeping systems. These systems delete messages automatically. Verbal conversations may be documented via internal, formal CMS Memos.

Non-record material (transitory documents, copies, and drafts) may be retained in an e-mail file indefinitely in accordance with 36 CFR 1236.22. Authorized users are responsible for reviewing their e-mail regularly and for deleting all such material as soon as it has served its purpose provided no specific preservation obligations apply (e.g., litigation hold). Transitory refers to documents of short-term interest having no documentary or evidential value and which normally need not be kept indefinitely. Examples of transitory material include user-saved instant messages and Mp3 voicemail messages.

(b) Video Conferencing Tools

There are other special considerations for Video Conferencing tools such as WebEx or Zoom recordings which are subject to the Federal Records Act (44 U.S.C. 2911). Whether CMS personnel are located on-site or teleworking, videoconferencing tools are more commonly used to conduct meetings, seminars, training sessions, and other events have moved to a virtual environment. Employees should continue to manage the records created with these tools as they would have had the meetings been held with the same technology while in the office. For recorded meetings using WebEx or Zoom, the host is responsible for maintaining any official recordings of the meeting as a record if the meeting is not transcribed; thereby creating a final record. If not transcribed, the recording is considered the official record and must be retained by the host in their files for three (3) years or when it is no longer needed for agency business, including without limitation, preservation obligations (e.g., litigation hold). If the recording will be fully transcribed or is being created for the purpose of creating meeting minutes, the host must retain the final record in their files for the longer of 3 years or when it is no longer needed for agency business, including without limitation, preservation obligations (e.g., litigation hold).

(c) Departing Employees/ Exit Clearance Process.

Federal records may be stored on an employee's government furnished equipment (GFE), or government issued computer (PC) (e.g., e-mail, text, instant messages or a word/excel/ PowerPoint document, etc.) in paper form, stored in a file cabinet, or stored in film, tape, or other physical form. These records shall not be removed upon departure from CMS, except in special circumstances described below.

Prior to separation, all departing CMS employees, including Senior Officials, must conduct the following process in a timely manner:

1. Collect hard copy records and return them to their appropriate office locations (i.e., centralized file cabinet), the CMS Warehouse Mezzanine, or if "checked-out" return the records to the Federal Records Center (FRC) storage.

2. Review all electronic files, to include emails, PST files, word processing documents, spreadsheets, folders, etc. saved to a GFE hard drive for Federal records or other material that must be preserved or maintained, and move them to an accessible network storage location. Email messages identified as Federal records must be handled in accordance with guidance provided in Email section of this Policy and NARA-approved records retention schedules. If email records are saved to the network, employees should contact the OIT Service Desk for OIT guidance.

3. Verify that all permissions to password protected files/folders have been provided to supervisor or designated staff for access to electronic records.

4. Review with their manager the CMS Exit Clearance User Guide and complete the automated CMS 129 Form in CATS. Departing employees will contact their manager for certification that all records (regardless of media format) have been returned, secured, or saved to an appropriate recordkeeping system, such as a Component SharePoint Site, for ongoing preservation and maintenance, or transferred to staff assuming responsibility for a matter.

5. Coordinate any ongoing records preservation or maintenance needs with the OIT Service Desk, as necessary.

The departing employee's immediate supervisor is responsible for ensuring their employees comply with records and information management requirements prior to departure. This guidance applies to managers of separating employees, excluding outside agency contractors, which currently follow exit procedures. For additional instructions, see the CMS Exit Clearance User Guide.

If a CMS employee has paper or electronic files that are required to be preserved for litigation, the employee is required to provide those files to the ARO, their manager, or the OGC servicing attorney responsible for the litigation prior to their departure. A departing employee subject to litigation hold must notify their current supervisor, OSORA, and OGC of their intended departure. Upon notification, OSORA will complete and submit a CMS User Electronic Data Request Form to OIT to preserve the departing employee's electronic data. If OIT does not preserve the data before the employee's separation, the computer equipment must be stored by the manager until OIT conducts the preservation.

CMS employees are likely to have extra copies of records kept for convenience or reference in their office or workstation. CMS employees are not authorized to remove any materials unless said employee has completed the CMS Removal Certification and Non-Disclosure Agreement (Appendix B) and obtained prior approval from the ARO. Approval will only be granted if removal does not adversely impact the official records of CMS and is at no cost to the agency.

(d) Departing Employee Records Removal

Unless CMS is formally transferring an employee's business functional records to the employee's new agency, the removal of federal records other than personal documents which do not meet the federal definition of a record and do not contain CMS specific record or non-record content, is prohibited. NARA regulation, 36 CFR §1231, *Transfer of Records from the Custody of One Executive Agency to Another*, prohibits the release of records from one government agency to another without the approval of the Archivist of the United States, unless any or all of the following conditions exist:

a) Release or change in custody is required by statute, Executive Order (EO) or Presidential reorganization.

b) Records are permanent and are eligible for transfer to NARA.

c) Records are on temporary loan for official use.

Personal documents of a private and unofficial nature, that pertain to an employee's personal affairs such as: work aids, administrative task diaries, logs, and memoranda of conferences and telephone calls that are memorialized elsewhere by other, or more detailed or complete records, provided the material does not contain national security, beneficiary privacy, confidential information; and/or controlled unclassified information may be requested to be reviewed by the CMS Records Officer for potential removal by the employee prior to said employee's separation.

(e) Essential Records

CMS has created and implemented a plan to identify and protect records and information necessary to continue agency mission-essential functions and activities in the event of an emergency or disaster. OSORA is responsible for establishing and maintaining the Essential Records program. OSORA has established a central repository for all CMS essential records. Components are responsible for ensuring their essential records are uploaded to the central repository. Components and Staff Offices shall manage and maintain their respective essential records and provide OSORA with the most recent and up to date version of any essential records to be stored in the OSORA Essential Records Library.

(f) Litigation Holds

A litigation hold is a notification to employee, covered contractors, and grantees to retain potentially relevant information in the CMS' possession, custody, or control. Under a litigation hold, potentially relevant information, regardless of media format or physical location, must be retained in its original format, if practicable and may not be altered, destroyed, or otherwise disposed of for as long as the litigation hold is in effect. A litigation hold supersedes any otherwise applicable disposition instruction, including records schedules.

If a CMS staff member fails to comply with a hold that is in place because of a court order, this individual may be individually sanctioned or held in contempt by the court.

4.2.3. Centralized Records vs. Decentralized Records

CMS uses a combination of centralized and decentralized recordkeeping systems. A centralized recordkeeping system collects records for several custodians in one location and is controlled by a records point of contact. A decentralized recordkeeping system collects records in several locations throughout the Component and is controlled by the custodian who creates and/or receives the records.

A Component may choose to maintain specific types of records in a central location, while maintaining other types of records at individual work stations. Records maintained at individual work stations should be annotated in the recordkeeping system, so that everyone in the component can locate the records. All records created, stored, and managed by Components shall be reflected in the Component's file plan regardless of the Component's centralized or decentralized records and information management approach.

4.2.4. Electronic Information Systems

Electronic information systems are the collection of technical and human resources that provide the storage, computing, distribution, and communication for the information required by all or some part of

an enterprise. Electronic information systems automate certain business functions. Other programmatic electronic information systems may automate CMS mission-specific business functions and as such, may produce Federal records in the process. These electronic information systems may or may not incorporate all aspects of appropriate electronic recordkeeping, depending on their design characteristics.

There are three categories of information collected for EISs which include: (1) inputs, (2) the information on the electronic media, and (3) outputs. Along with these categories, CMS inventories and schedules may include associated indexes and documentation needed to manage the electronic records contained within the EIS. Any system documentation used for the electronic system is covered by NARA GRS 3-1, Item 050 for permanent records and Item 051 for temporary records. Systems input and outputs may also be covered by NARA GRS 5.1 and 5.2.

In order to comply with National Archives and Records Administration (NARA) regulations (36 CFR 1236.26). and to meet the business needs of the agency, CMS maintains a complete and current inventory of all its electronic records systems to meet the business needs of the agency and in order to comply EIS inventory includes 16 elements which includes: the name of the system, the system control number, the agency program supported by the system, its purpose, data input and sources; and major outputs to name a few. For more information regarding the elements included in the EIS Inventory, see the EIS Records Inventory on the NARA website.

4.3. Maintenance

After creating or receiving a record, CMS staff must capture it by filing, storing, or otherwise systematically maintaining it in a recordkeeping system. Capturing records ensures that the information is accessible to all authorized staff. It also assists components in dispositioning records in accordance with the applicable records schedules.

4.3.1. Storage

CMS Components can choose to store their active records on-site, or, with permission, in an off-site storage facility. All on-site records centers and off-site storage facilities CMS uses are required to protect federal records from threats such as fire, pests, theft, natural disasters and water damage.

Permanent records must be stored on archival-quality media and in containers and facilities appropriate to long-term preservation. Components should arrange records in storage media with like schedules and disposition dates.

(a) Records Maintained at Telework or Alternate Duty Station

All CMS employees, staff, contractors, interns, and personnel shall adhere to proper records management storage requirements for federal records and non-record material created, stored, and managed while working from a telework or alternate duty station (ADS) location.

4.3.2. Equipment

Filing equipment and supplies should be the most economical possible to meet recordkeeping requirements. In selecting equipment, components must consider: the media to be filed (e.g., CDs, slides, photographs, paper, oversized paper), the volume and rate of growth, activity (i.e., how often the records are retrieved and refiled), the cost of the equipment, the cost of moving (dismantling and reassembly), site characteristics, and the need to maintain confidential records in equipment that can be locked and/or stored in a secure location. Components should use equipment that accommodates letter-sized records unless there is a requirement for other sizes.

4.3.3. Imaging

Imaging is a process by which a paper document is converted from a human-readable format to microform or a computer-readable digital image file. Imaged pictures of documents can be stored on a variety of media. All imaging and digitization efforts by CMS Components shall be coordinated with OSORA to ensure appropriate records and information management requirements are adhered to. Components which solicit imaging or digitization procurement solutions with the intent to formally recognize the new electronic version of a document as the formal record shall ensure records and information management digitization contracts adhere to 36 CFR § 1236, the Federal Agencies Digital Guidelines Initiative, and the International Organization for Standardization (ISO) technical requirements (TR) 13028:2010, Information and documentation - Implementation Guidelines for Digitizing Records are met.

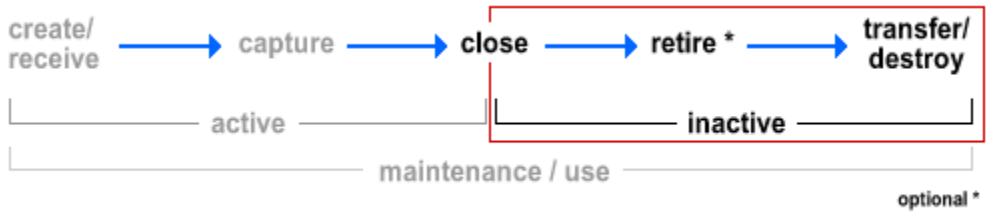
See the NARA Digital Preservation Strategy for more information.

4.3.4. Printing

CMS records printed from a CMS main office such as, but not limited to: CMS Headquarters, Regional Offices, and federal buildings shall be maintained in accordance with proper records storage requirements. CMS records printed from a telework or ADS location shall be considered reference material with the electronic version of said printed records being identified as the formal federal record. Should a CMS employee, staff, contractor, intern, or personnel print a federal record at a telework or ADS location and alter the printed record with sufficient changes as to justify creating a new federal record, the record must be properly secured, managed, and preserved as annotated in section 4.3.1(a) Records Maintained at Telework or Alternate Duty Station.

5. Inactive Records

Inactive records are those that are no longer needed to conduct CMS business. CMS records schedules provide instructions on how to handle events in this phase of the lifecycle. This includes closing records, optionally retiring them to off-site storage, and destroying or transferring them to the National Archives.



5.1. Closing Records

Records are closed when the current business activity has ended. Closure effectively makes the record immutable and begins the mandatory retention period for the records. Records schedules require records to be closed either: at the end of a defined time period (e.g., the end of the fiscal or calendar year) or when a certain event relating to the record has occurred (e.g., the denial of a permit or receipt of final payment).

Unless Components have a specific business requirement, all CMS records shall be considered closed at the end of each calendar year or in accordance with NARA approved GRS and CMS record schedule.

5.2. Retiring Inactive Records

5.2.1. Inactive physical records

OSORA may store inactive records on-site until the destruction or transfer date. The CMS Records and information management office retains legal custody of inactive records and controls access to the records while they are stored in the CMS Warehouse Mezzanine or NARA FRC. CMS Regional Offices may also use the FRC, which is operated by NARA for off-site storage. Components may need access to retired records to conduct CMS business. The CMS Records and Information Management Staff will assist Components with retiring and retrieving records.

5.2.2. Inactive electronic records in EISs

Inactive records housed in EISs will be managed using a Cross Reference Tool (CR) Tool. The CR Tool integrates with our electronic records and information management solution, Gimmal by notifying Component RLOs, system owners, business owners and RLOs of upcoming disposition actions for records held within information systems at the end of their retention period and the CMS Records Staff will receive a notification and status update applicable records from the system owners and RLOs. Final disposition actions are taken by the Component RLOs, system owners and business owners for applicable inactive records within the specific EIS.

5.3. Transferring Records

CMS records having sufficient historical or other enduring value to warrant continued preservation by the federal government are designated in the records schedule as permanent records to be transferred to NARA. Once the transferred records are received and approved by NARA, the legal and physical custody is officially transferred from CMS to NARA.

Permanent records are required to be transferred to the National Archives in accordance with the disposition instructions in the approved schedules. Documentation adequate to identify and interpret (metadata) permanent electronic records must be transferred with the records.

Records may be transferred early if they require special preservation. When transferring permanent electronic records, offices must keep a copy of the records until the National Archives notifies CMS that the transfer was successful and approved.

The Electronic Records Archives (ERA) is NARA's system that allows Federal agencies to perform critical records and information management transactions with NARA online for the first time. Agency records and information management staff will use ERA to draft new records retention schedules for records in any format, officially submit those schedules for approval by NARA, request the transfer of records in any format to the National Archives for accessioning or pre-accessioning, and submit electronic records for storage in the ERA electronic records repository.

See ERA for more information on the system.

5.3.1. Electronic Records

The National Archives Destruction forms are a uniform requires CMS to use only media that is sound and free from defects for transferring permanent electronic records. Approved methods of transferring records are open reel magnetic tape, magnetic tape cartridge, CD-ROM, and File Transfer Protocol (FTP). Records must not be dependent on proprietary software or hardware. Other accepted formats include: Portable Document Format (PDF) files, scanned images, digital photographs and Web content.

5.3.2. Audiovisual Records

Audio visual are records in pictorial or aural form. Permanent audiovisual records more than 10 years old must be reviewed for possible immediate transfer to the National Archives. Offices must contact OSORA immediately if any permanent or unscheduled motion picture films or still picture negatives are found to be deteriorating. Also, masters of videotapes, originals, and preprint material for motion pictures should be transferred to the National Archives. See NARA regulations (36 CFR §1237) for specific instructions.

Program offices must send two copies of posters that are distributed agency-wide or to the public and original artwork of unusual or outstanding merit, to the OSORA immediately after publication.

5.4. Destroying Records

CMS record schedules authorize destruction of temporary records when their retention period expires provided no specific preservation obligations apply (e.g., litigation hold). Temporary records with restrictions, such as those containing personal or confidential business information (CBI), must be shredded or otherwise definitively destroyed when their retention period expires. If those records are destroyed by outside contractors, a federal employee or, if authorized by CMS, contractor must witness the destruction. Executive Order (EO) 12356 governs the destruction of security-classified documents. Specific laws and regulations, including the Privacy Act of 1974 and NARA regulations (36 CFR § 1226.24), govern the destruction of other restricted records. See 32 CFR 2002 for more details on Controlled Unclassified Information.

Methods of destruction include: recycling, shredding, pulping, physical destruction of electronic media (e.g., hammering, smashing), demagnetization, and secure deletion of electronic records (i.e., overwriting data several times using specialized software).

Offices should develop procedures to notify records custodians responsible for the affected records of the impending destruction to prevent premature destruction.

When destroying imaged records, offices must remove the image itself from the storage media, or physically destroy the storage media. Removing index pointers to imaged files does not destroy an image. CMS must ensure that there are no records freezes or litigation holds on all records that are scheduled for destruction.

5.4.1. On-site Destruction

Destruction of records maintained at CMS sites must be tracked and documented. Destruction forms are a uniform method of documenting the decision and authority to destroy records, and provide safeguards to prevent unauthorized destruction.

Prior to disposal, each destruction should be approved by the: Component's Records Custodian, authorizing official (e.g., Component RLO, supervisor), person destroying the records, and witness (if restricted records are destroyed by an outside contractor).

Component RLOs must maintain documentation of on-site destruction.

5.4.2. FRC Destruction

When records maintained at FRCs are eligible for destruction, the FRCs initiates the following process:

The FRC notifies the CMS Records and information management Program office of a scheduled destruction 90 days prior with NA Form 13001, Notice of Eligibility for Disposal. The ARO notifies Component RLOs and Records Custodians of records that are due for destruction and requests concurrence. If CMS decides to concur, the ARO completes the NA 13001, indicating concurrence, signs

and dates the form, and returns it to the FRC. FRCs must receive written concurrence before destruction takes place. If the ARO does not concur, it must provide a justification, sign and date the NA 13001, and return it to the FRC. After the FRC receives the CMS' concurrence, it will destroy the records. Component RLOs must maintain documentation of FRC destruction in their files.

5.4.3. Unauthorized Destruction of Records

Centers / Offices must monitor their records to prevent unauthorized destruction, which is illegal under federal law (44 U.S.C. § 3106), and carries penalties of a fine and up to three years of imprisonment. CMS records and information management staff must report any unlawful or accidental removal, defacing, alteration or destruction of records to the ARO.

The report of unauthorized records destruction should include: a complete description of the records (along with volume and dates if known), the office of origin, an explanation of the exact circumstances surrounding the unauthorized action, details of the actions taken to salvage, retrieve or reconstruct the records, and a statement of safeguards established to prevent further losses. Other major risks associated with destruction are delayed and improper destruction.

(a) Delayed destruction:
Temporary records must be destroyed promptly on or shortly after the approved destruction date. If temporary records are retained when preservation is no longer required, CMS may be obligated to include those records in response to a discovery or FOIA request.

(b) Improper destruction method or incomplete destruction:
CMS must ensure that temporary records, especially security classified, CUI, or Privacy Act records, are destroyed in accordance with the applicable regulations, and that the records are destroyed completely. If destruction is not done properly, information in records may be compromised or stolen. Components must make certain any paper records and other media are completely destroyed, and that electronic records are obliterated through secured deletion.

(c) Penalties for Unlawful Removal, Alienation, or Destruction of Government Records

1. The penalties for unlawful removal, alienation, or destruction of government records may include a fine, imprisonment, or both.
2. This offense and related offenses are stated in:
    a. 18 United States Code (USC) 2071; and
    b. 18 USC 641, 793, 794, 798, and 952.

Failure to preserve operational records could constitute an unlawful destruction of records that must be referred to the Attorney General under 44 U.S.C. 2905(a) and 3106. Destruction of records under certain circumstances is potentially a criminal violation for which a staff member may be prosecuted under 18 U.S.C. 1519.

5.4.4. Suspending Destruction

Records eligible for destruction should not be maintained beyond their disposition date if no specific preservation obligations apply; however, special circumstances may require continued retention. These circumstances include: litigation holds, other records holds (due to audit, or FOIA requests), and when changes to the record's retention period are in process or have yet to be forwarded to the FRC.

If the above-mentioned circumstances apply, the normal disposition activities for applicable records, regardless of media, must be suspended until the preservation obligation is lifted and offices have been notified that disposition may be resumed.

CMS must request NARA's approval to temporarily extend a retention period if CMS requires retention of records stored at an FRC for more than one year past the scheduled destruction date. NARA shall notify CMS if the extension is approved. No formal extension is necessary for records kept less than one year past the destruction date.

5.5. Storage Facilities

Components may store both their active and inactive records on-site at the CMS Warehouse Mezzanine, at an FRC, or at a NARA-approved off-site storage facility. All on-site records centers and off-site storage facilities CMS uses must protect Federal records from threats such as, but not limited to: fire, pests, theft, natural disasters, and water damage. Permanent records must be stored on archival-quality media and in containers and facilities appropriate to long-term preservation. Offices should arrange records in storage media with like schedules and disposition dates. Components which opt to procure off-site storage for their active or inactive records shall notify OSORA of their intent to transfer the custody of records in accordance with applicable LRGWPs.

The National Archives and Records Administration administers the FRCs. There are 18 FRCs located throughout the country where records can be stored. See FRC for more information.

CMS records can only be stored at commercial storage facilities that meet the requirements established in 36 CFR § 1234. The standards outlined in this CFR ensure that records are stored in an environmentally safe and secure facility, which would mitigate potential losses and manage records throughout their lifecycle. Commercial storage facilities are required to certify that they meet the requirements set forth in 36 CFR § 1234 and must provide a facility inspection report.

See FRC Toolkit for more information.

5.6. Capital Planning and Investment Controls

In accordance with OMB Circular A-130, CMS must incorporate records and information management functions into the design, development, and implementation of information systems. In addition to ensuring the accessibility and proper accountability for their information systems, CMS must ensure that all electronic systems are evaluated through the Capital Planning and Investment Controls (CPIC) process.

Electronic System Shutdown [related to projects that follow the Target Life Cycle (TLC) process]. Electronic system owners must follow appropriate shutdown procedures when a system is scheduled for cancellation. The process is defined through the following series of actions to ensure orderly and efficient performance of essential shutdown activities.

1. If information is to be migrated to another system, you must:
    a. Notify the OSORA RM program office of changes to system (i.e., name change, or changes in functionality, etc.);
    b. Determine if any changes should be made to the disposition of the new system based on changes in functionality; and
    c. Manage the new system in accordance with an approved disposition authority.

2. If the information is not being migrated to a new system, you must:

    a. Notify the RM program office that this information will no longer be collected; and

    b. Establish a plan to manage any legacy record data that has not yet met its approved disposition.

6. Training and Evaluations

6.1. Annual Records and Information Management Training

CMS must provide records and information management training annually to all staff to ensure they are aware of their responsibilities to maintain and safeguard Department records, including the obligations under this Policy and the HHS Litigation Holds Policy. The records and information management training must be completed by the established completion date in accordance with 36 CFR 1220.34(f).

All Contractors who have access to (1) HHS Federal Information or a Federal information system or (2) personally identifiable information shall complete the CMS provided Records management training required by the Department of Health and Human Services (HHS) before performing any work under their contract. Thereafter, the Contractor must complete annual Records Management training throughout the life of the contract. The Contractor shall also ensure subcontractor compliance with this training requirement.

6.1.1. New Employee Orientation

Each CMS new employee shall receive records orientation training within their first 30 days of duty.

6.1.2. Records Liaison Officer Training

Component Records Liaison Officers shall attend quarterly CMS RLO meetings and discussions to ensure that they are aware of their role and responsibilities to manage Component-level RIM Program activities.

6.1.3. Senior Official Awareness Training

Incoming Senior Officials and Political Appointees shall be trained on the importance of appropriately managing records under their immediate control. Components shall coordinate with OSORA to ensure new Senior Officials and Political Appointees receive appropriate training no later than 120 calendar days after their appointment.

Appendix A: References

Resource	Hyperlink
36 CFR Chapter XII, Subpart B - Part 1222 - Agency Records and information management Responsibilities	https://www.govinfo.gov/content/pkg/CFR-2011-title36-vol3/pdf/CFR-2011-title36-vol3-chapXII-subchapB.pdf
36 CFR Chapter XII, Subpart B - Part 1235 - Transfer of Records to the National Archives of the United States	https://www.govinfo.gov/content/pkg/CFR-2011-title36-vol3/pdf/CFR-2011-title36-vol3-chapXII-subchapB.pdf
36 CFR Chapter XII, Subpart B - Part 1236 - Electronic Records and information management	https://www.govinfo.gov/content/pkg/CFR-2011-title36-vol3/pdf/CFR-2011-title36-vol3-chapXII-subchapB.pdf
44 U.S.C. Chapters 21, 29, 31, and 33	https://uscode.house.gov/view.xhtml?path=/prelim@title44/chapter31&edition=prelim
Circular A-130, Managing Information as a Strategic Resource	https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource
CMS Bucket Schedule (Records Retention)	https://www.cms.gov/Regulations-and-Guidance/Guidance/CMSRecordsSchedule/index.html
CMS Intranet Webpage	https://intranet.cms.gov/
CMS Records Crosswalk	https://cmsintranet.share.cms.gov/JT/Pages/RecordsManagement.aspx
Code of Federal of Regulations (CFR)	https://www.govinfo.gov/
Code of Federal of Regulations (NARA Linked)	https://www.archives.gov/federal-register/cfr
Federal Continuity Directive (FCD 1)	https://www.fema.gov/sites/default/files/2020-07/January2017FCD1.pdf
Federal Continuity Directive (FCD 2)	https://www.fema.gov/sites/default/files/2020-07/Federal_Continuity_Directive-2_June132017.pdf
Federal Electronic Records Modernization Initiative (FERMI)	https://www.archives.gov/records-mgmt/policy/fermi
HHS Policy for Implementing Electronic Mail (Email) Records Management, HHS-OCIO-PIM-2020-06-005	https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-ocio-policy-for-implementing-email-records-management.html
HHS Records Management Policy, HHS-OCIO-PIM-2020-06-004	https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-ocio-policy-for-records-management.html
NARA Bulletin 2012-02, Guidance on Managing Content on Shared Drives	https://www.archives.gov/records-mgmt/bulletins/2012/2012-02.html
NARA Bulletin 2013-02, Guidance on a New Approach to Managing Email Records	https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html
NARA Bulletin 2014-02, Guidance on Managing Social Media Records (2014)	https://www.archives.gov/records-mgmt/bulletins/2014/2014-02.html
NARA Bulletin 2014-04, Revised Format Guidance for the Transfer of Permanent Electronic Records	https://www.archives.gov/records-mgmt/bulletins/2014/2014-04.html

NARA Bulletin 2014-06, Guidance on Managing Email	https://www.archives.gov/records-mgmt/bulletins/2014/2014-06.html
NARA Bulletin 2015-02, Guidance on Managing Electronic Messages	https://www.archives.gov/records-mgmt/bulletins/2015/2015-02.html
NARA Bulletin 2015-04, Metadata Guidance for the Transfer of Permanent Electronic Records	https://www.archives.gov/records-mgmt/bulletins/2015/2015-04.html
NARA General Records Schedule (GRS)	https://www.archives.gov/records-mgmt/grs.html
National Archives Records Administration (NARA) Records and information management website	https://www.archives.gov/records-mgmt
OMB M-19-21, Transition to Electronic Records	https://www.archives.gov/files/records-mgmt/policy/m-19-21-transition-to-federal-records.pdf

Appendix B:
Centers for Medicare & Medicaid Services
Materials Removal Certification and Non-Disclosure Agreement

Name: _____ Office: _____

Telephone Number: _____ Planned Departure Date: _____

1. Records that May Not be Removed.

(1) Any material, regardless of the media, that meets the definition of a Federal Record. **(2**) Any information not normally released to the general public, unless prior approval has been obtained from the Records Officer and the Freedom of Information Act (FOIA) Officer.

2. Documentary Materials that May Be Removed: Personal Papers.

Examples of personal papers include: papers accumulated by an official before joining Government service that are not used subsequently in the transaction of Government business; materials relating solely to an individual's private affairs, such as outside business pursuits, professional affiliations, or private political associations that do not relate to CMS business; diaries, journals, personal correspondence, or other personal notes that are not prepared or used for, or circulated or communicated in the course of transacting Government business (36 C.F.R., Section 1222.36(a), (b), and (c)). Copies of Federal Records, if appropriate, for release to the general public as determined by the FOIA Officer.

3. Penalties for Unlawful Removal of Records.

Criminal penalties are provided for the unlawful removal or destruction of Federal records (18 U.S.C. 641 and 2071) and for the unlawful disclosure of certain information pertaining to national security (18 U.S.C. 793, 794, 798 and 952).

4. If you are removing any non-record documents such as extra copies of agency records, complete the certification below with the CMS Records Officer.

Appendix C:
Centers for Medicare & Medicaid Services
Certification and Non-Disclosure Agreement

I certify that the documents that I am removing from the Centers for Medicare & Medicaid Services have been reviewed and approved for removal. They do not include any documents relating to any pending or contemplated civil, criminal, or administrative proceeding or other program information, if released, would impair or prejudice the outcome of the proceeding or Government policy determinations, decisions, or other actions (Examples: classified documents; record copies; documents, even though judged to be a non-record, that will create a gap in the files; and indexes and finding aids necessary to use the official files).

I agree to keep all non-public materials absolutely confidential and will not disclose their contents or existence without prior permission from the appropriate Centers for Medicare & Medicaid Services Reviewing Official.

_____ _____

Printed Name and Signature Date

_____ _____

Signature of CMS Reviewing Official Telephone Number

_____

Name and Title of CMS Reviewing Official

Description of documents (with dates) _____

_____

_____

_____

_____