



DEPARTMENT OF HEALTH & HUMAN SERVICES

---

FOIA Office  
Health Resources and Services Administration  
5600 Fishers Lane, Room 13N86  
Rockville, Maryland 20857

April 5, 2018

*Sent via Email*

Kimberly Hertz on behalf of Aaron Siri  
Siri & Glimstad LLP  
200 Park Avenue, 17th Floor  
New York, NY 10166  
[khertz@sirillp.com](mailto:khertz@sirillp.com)

Re: HRSA Freedom of Information Act (FOIA) Request Number 18F130

Dear Ms. Hertz/Mr. Siri:

This is the final response to your FOIA request received in our office on March 14, 2018. In summary, you requested copies of HRSA's current document, communication, and email retention policies.

A records search was conducted in the Office of Information Technology (OIT) and responsive records were located. Upon further review, I have determined that all 89 pages can be released in their entirety.

Please note that an additional document, which originated from the National Archives and Records Administration (NARA), that may be responsive to your request is available online at the following address: [https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-health-and-human-services/rg-0512/daa-0512-2014-0004\\_sf115.pdf](https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-health-and-human-services/rg-0512/daa-0512-2014-0004_sf115.pdf)

There will be no charges in this instance because the billable costs are less than our threshold of \$25.

If you have any questions regarding this response, please contact me at [FOIA@hrsa.gov](mailto:FOIA@hrsa.gov), or at (301) 443-9425.

Sincerely,

*DFWallace*

For Thomas Flavin  
Freedom of Information Officer

Enclosure



# HRSA Records Management Policies and Procedures Manual

*Office of Information Technology, Division of Capital Planning, Architecture, Project  
Management, Section 508 & Records Management*

## Table of Contents

I OVERVIEW.....	3
1. Purpose .....	3
2. Background .....	3
3. Scope.....	3
4. Technical Assistance.....	4
5. Effective Date and Authority.....	4
II ROLES AND RESPONSIBILITIES .....	5
1. RACI Matrix .....	5
2. Chief Information Officer (HRSA CIO) .....	6
3. HRSA Records Officer (ARO) .....	6
4. Advisory Committee Management Officer (CMO) .....	7
5. HRSA Bureaus and Office Heads .....	7
6. Bureau/Office Records Liaisons (RL).....	8
7. HRSA Employees .....	9
III POLICIES AND PROCEDURES .....	10
1. General Filing Procedures .....	10
2. Management of Records and Information .....	10
3. Packing and Shipping Procedures for R/O Transfer of Records.....	16
4. Withdrawing Records from the FRC .....	20
5. Records Freezes and, Litigations.....	21
6. Employee Departure Procedures.....	25
IV ELECTRONIC RECORDS MANAGEMENT .....	31
1. Electronic File Folder Structures .....	31
2. Electronic Transfer Records .....	32
3. Email and Calendars.....	33
GLOSSARY.....	41
REFERENCES.....	45

## I OVERVIEW

### 1. Purpose

The purpose of the Health Resources and Services Administration (HRSA)'s Records Management Policy and Procedures Manual is to establish principles, standards, responsibilities, procedures and requirements for managing HRSA records materials.

### 2. Background

The Federal Records Act of 1950, as amended, requires all Federal agencies to make and preserve records containing adequate and proper documentation of the organization, function, policies, decisions, procedures, and essential transactions. These records are Agency property and must be managed according to applicable laws and regulations. The Federal Records Act also requires agencies to establish a records management program. This program is defined as a planned, coordinated set of policies, procedures, and activities needed to manage HRSA's records.

### 3. Scope

This Policy applies to HRSA and organizations conducting business for and on behalf of the HRSA, whether owned and operated by HRSA, or operated on behalf of HRSA, or through contractual relationships. It applies to all HRSA personnel, contractors, visitors who have access to HRSA supported facilities or HRSA information, interns, other non-government employees through incorporation by reference in contracts, service level agreements (SLA) or memoranda of understanding (MOU) as conditions for using Government provided IT resources. All HRSA Bureau and Office (HRSA B/O) are obligated to meet the minimum requirements of this Policy and is authorized to develop and implement more specific policies and procedures consistent with this Policy.

This Policy applies to the management of all records, regardless of medium on which the records are created, used, stored, or retrieved. This Policy does not apply to HRSA grantees. Physical locations include but are not limited to audit sites, field offices, headquarters, Federal Records Centers (FRC), individual and central office spaces, agency-specific storage locations, contractor offices, HRSA Continuity of Operations [COOP] sites, and electronic information back-up sites.

"Formats" and "media" refer to the physical characteristics of documentary materials. Types of formats and media may include, but are not limited to:

- Paper/hardcopy
- Electronic formats and storage media:
- E-mail messages
- Personal electronic devices used to conduct official HRSA business, including but not limited to, portable digital assistance/devices (e.g., Blackberry)
- Word processing files, spreadsheets, and databases
- Digital images

- Web pages
- Network server information, including metadata
- Voice mail messages
- Back-up tapes
- Hard drives
- Removable computer storage media (e.g., CD-ROMs, tapes, disks, thumb drives, and cards)

#### **4. Technical Assistance**

Questions about HRSA records management policies and procedures should be addressed to the Records Liaison (RL) in each B/O, or to the Agency Records Management Officer. Any violation of the statutory and regulatory limitations placed on the removal of documentary materials by HRSA employees or individuals conducting business on behalf of HRSA under agreements, who are separating from the Agency, should be forwarded to the Office of Human Resources.

#### **5. Effective Date and Authority**

This manual is effective the date the policy is approved. Requirements stated in this Policy are consistent with law, regulations and other Department policies applicable at the time of its issuance. Actions taken through the implementation of this Policy must comply with the requirements of pertinent laws, rules and regulations, as well as the lawful provisions of applicable negotiated agreements for employees in exclusive bargaining units.

## II ROLES AND RESPONSIBILITIES

All employees are required to know their major roles and responsibilities as mandated by Federal Records Management policies and procedures. This section outlines these roles and responsibilities within HRSA.

### 1. RACI (Responsible, Accountable, Consulted, Informed) Matrix

- a) RACI matrix describes the participation by various roles in completing tasks or deliverables for a project or business process. In addition to the defined Records Management roles and responsibilities, all HRSA employees should be able to determine:
- (1) R: Who's Responsible?
  - (2) A: Who's Accountable?
  - (3) C: Who needs to be Consulted?
  - (4) I: Who needs to be Informed?

Table 1: HRSA RACI Matrix

Task	Employee	Supervisor	Bureau/ Office Heads	Records Officer	Senior Officials
Understand all existing day-to-day RM policies and procedures	R, A	C, I	C, I	C	C, I
Provide guidance for maintenance of records and proper disposition	I	A, I	A, I	C, I	C, I
Ensure all personnel receive annual records management training	C, I	I	R	R, A	R
Institute standards, policies, procedures, and techniques to ensure compliance	I	I	I	R, A	C, I
Advise on records management implications for HRSA initiatives, IT systems, and policies	C, I	C, I	C, I	R, A	C, I
Records Liaison appointment	I	C, I	C, I	A, I	A, R, I

## 2. Chief Information Officer (HRSA CIO)

- a) Directs and administers the records program for the HRSA B/O.
- b) Provides guidance to the HRSA Bureau/Offices (B/O) on the creation, organization, maintenance, use, and disposition of records.
- c) Cooperates with NARA in developing and applying standards, procedures, and techniques designed to improve the management of records and information; ensures the maintenance and security of records of continuing value; and facilitates the identification, segregation, and disposal records of temporary value.
- d) Ensures compliance with Federal and Agency requirements.
- e) Establishes work groups to ensure that records management policy pertaining to information technology (IT) and electronic records.
- f) Ensures the HRSA B/O ability to control the disclosure of official information is not impaired through unauthorized removal.
- g) Major RACI Role: C, I

## 3. HRSA Records Officer (ARO)

- a) Serves as the office of record and the Federal Agency Records Officer for records and activities for HRSA B/O.
- b) Establishes and revises a comprehensive HRSA records and information management program to support the requirements.
- c) Ensures positive control over the organization, maintenance, use, designation, and disposition of HRSA B/O records regardless of media (paper, electronic, audiovisual, etc.).
- d) Maintains and updates the HRSA Records Disposition Schedule online as NARA approves changes to the HRSA disposition schedule or revises the General Records Schedule (GRS) citations.
- e) Develops and applies standards, procedures, and techniques for improving records management; ensuring the maintenance and timely retirement of records; transfer, and destruction of records.
- f) Oversees the implementation of this manual as the Federal Agency Records Officer.
- g) Acts as the liaison official with NARA, other government agencies, private industry, and private citizens on records matters of HRSA B/O.
- h) Institutes and oversees a records management evaluation program to ensure compliance of the HRSA B/O and to provide for improvements to existing procedures and records schedules to reflect current mission and organizational requirements.
- i) Provides HRSA employees and contractors with basic records management training.
- j) Monitors the acquisition of IT systems within HRSA enterprise architecture to ensure compliance with records management laws and regulations.
- k) Provides the HRSA B/O with advice and management assistance when creating, and updating paper and electronic schedules, to include including implementing electronic systems are adequately documented, secure, and accessible.
- l) Provides advice and assistance to the HRSA B/O on the identification, segregation, retention, and disposition of personal papers.
- m) Coordinates, controls, and supervises access to HRSA records essential for historical research, ensuring that appropriate safeguards for information security and personal privacy.

- n) Ensures HRSA employees, contractors, and senior Officials do not remove federal records (paper or electronic) from government custody that was not cleared for public use.
- o) Manages the transfer of HRSA B/O records to and retrieval from the Federal Records Centers (FRCs) using the approved NARA system online.
- p) Maintains a record on all current suspension actions to normal disposition instructions, such as records holds, freezes, moratoriums, or preservation orders.
- q) In consultation with the Advisory Committee Management Officer (ACMO), determines which advisory committee records are subject to processing through the HRSA Records Officer to NARA.
- r) Provide technical advice and assistance to the HRSA Bureau/Office heads in order to support the inclusion of electronic records management functions into the design, development, enhancement, and implementation of Electronic Information Systems (EIS) in accordance with the HRSA Records Disposition Schedule.
- s) As part of the capital planning and systems development lifecycle process ensures that:
  - 1) Records management controls are planned and implemented in the system in accordance with HHS policies.
  - 2) All records in the system will be retrievable and usable for as long as needed to conduct HRSA business in accordance with the HRSA Records Disposition Schedule.
- t) Assist in the transfer of permanent electronic records to NARA in accordance with the HRSA Records Disposition Schedule.
- u) Major RACI Role: R, A, C, I.

#### **4. Advisory Committee Management Officer (CMO)**

- a) The ACMO will ensure all records of advisory committees established or supported by the HRSA B/O, including those advisory committees exempted from FACA by an act of Congress, are managed in accordance with this AI. Records of the committee and any respective subgroups should be handled in accordance with the General Records and HRSA records disposition schedule. These records will be available for public inspection and copying subject to the Freedom of Information Act, 5 U.S.C., Section 552

#### **5. HRSA Bureaus and Office Heads**

- a) Establish and sufficiently resource a records and information management program within their organization to support National and HRSA regulations.
- b) Use standards, procedures, and techniques to ensure the most economical, efficient, and reliable means for creation, retrieval, maintenance, preservation, and disposition of records, regardless of media.
- c) Institute measures to ensure that records of continuing value are preserved and records no longer needed for current use receive appropriate disposition in accordance with the HRSA Records Disposition Schedule.
- d) Appoint an individual to be the Record Liaison (RL) to perform the records management functions; serve as the Accountable records custodian in their organization, and liaison with Records Management Team (RMT). The RLs must have knowledge of applicable laws and regulations governing records management. This appointment will be made in writing and furnished to the HRSA Records Officer. All appointments will state the organizations supported by the RL. Appointment memos will be updated upon the departure or change of the individual.



- e) Ensure RLs have a critical performance task contained in their yearly PMAP that detail their performance of the records management functions within their organization.
- f) Ensure all B/O employees and contractors within their organization receive basic records management training annually to maintain compliance.
- g) Ensure all training is documented and forwarded to the HRSA Records Officer.
- h) Ensure all offices within their organization have approved file plans that are accessible to employees and contractors.
- i) Evaluate current and developing EISs and databases, ensuring that the record information contained within the systems is retained as required by the HRSA Records Disposition Schedule. Record information created or received during the conduct of business and maintained in these systems that is not identified in the HRSA Records Disposition Schedule will be brought to the attention of RMT.
- j) Plan and budget for the migration of records and their associated metadata maintained in an EIS or database to new storage media or formats to avoid loss of record data due to media decay or technology obsolescence.
- k) Ensure essential documents, Vital Records needed for continuity of operations are identified and preserved in compliance.
- l) Ensure the requirements the Privacy Act of 1974 (PA) are satisfied if creating records or systems of records that are subject to section 552a.
- m) Annually remind and caution all employees not to transfer or destroy records in their custody, to include e-mail, except as allowed IAW HRSA Records Disposition Schedule.
- n) Ensure that records and information maintained on network shared drives (also known as shared drives), websites, SharePoint sites, or portals are maintained in accordance with the HRSA Records Disposition Schedule.
- o) Report to the HRSA Records Officer any actual, impending, or threatened unlawful removal, alteration, or destruction of federal records.
- p) Ensure HRSA employees and Senior Officials manage their personal papers in accordance with the HRSA Records Disposition Schedule.
- q) Ensure that records and information posted to commercial and government-owned social media sites (Web 2.0) are maintained in accordance with the HRSA Records Disposition Schedule.
- r) Direct contractors performing HRSA program functions on behalf of the organization to create and maintain records to document these functions. Contracts must specify the delivery to the government of all the information required for the adequate documentation of the contractor-operated program. The contractor will apply the appropriate file identification from the HRSA Records Disposition Schedule.
- s) Major RACI Role: R, C, I.
- t) Direct in a contract vehicle support contractor personnel within their organizations to:
  - 1) Maintain government records and information created and received in the course of their day-to-day responsibilities. Ensure that each record set is complete and that enclosures or related papers are retained or accounted for in both paper and electronic filing systems in accordance with the HRSA Records Disposition Schedule.
  - 2) Maintain electronic mail and attachments that document work related activities in accordance with the HRSA Records Disposition Schedule.

## 6. Bureau/Office Records Liaisons (RL)

- a) Complete the HRSA Records Officer sponsored training within 3 months of their appointment.

- b) Ensure every office within their organization has an office file plan. RLs are to prepare and submit file plans to the HRSA Records Officer for approval.
- c) Annually review and approve the file plan for each office within their organization to ensure that records are accurately identified.
- d) Conduct records searches, implement preservation orders, and ensure organization offices are aware of the responsibilities to safeguard records and information identified in existing preservation orders.
- e) Assist their organizations with the application of disposition procedures, to include the destruction and retirement of their records.
- f) Notify the HRSA Records Officer of the unauthorized destruction, damage, alienation, or removal of official records.
- g) Notify the HRSA Records Officer when senior officials are hired or prior to their departure.
- h) Ensure the proper maintenance of records generated by their program offices.
- i) Ensure all employees and contractors receive annual basic records management training to maintain compliance with HHS policy.
- j) Evaluate their records management program every year to ensure compliance with the guidance in this Manual.
- k) Attend quarterly RL update meetings.
- l) Assist RMT to successfully conduct records assistance visits, records audits, and inspections.
- m) Bi-annually submit updated file plan to the HRSA Records Officer.
- n) Major RACI Role: I, C.

## 7. HRSA Employees

- a) Maintain records and information created and received in the course of their day-to-day responsibilities. Ensure that each record set is complete and that enclosures or related papers are retained or accounted for in both paper and electronic filing systems in accordance with the HRSA Records Disposition Schedule.
- b) Maintain e-mail and attachments documenting work related activities in accordance with the HRSA Records Disposition Schedule.
- c) Ensure personal files, non-record material, and work-related records and information are maintained separately.
- d) Complete annual records training.
- e) Mend or reinforce torn or frayed temporary papers with transparent tape. Do not tape nor attempt to mend permanent documents.
- f) Bring forward documents needed to conduct current business or still pending action; combine documents of a later date that relate or refer to documents of an earlier date only when reference to them is necessary. A reference to an earlier document does not necessarily require that documents be combined.
- g) Prepare information for filing when all actions are completed, when record information is self-identifying, required by a business process, federal law or regulation, or HRSA issuance or an official has requested that documentation be maintained.
- h) Ensure that each record set is complete and that enclosures or related papers, to include e- mail, are retained or accounted for in both paper and electronic filing systems.
- i) Remove or destroy identical or duplicate copies of information before filing. Ensure that duplicate copies of such records retained for convenience are identified as such and any duplicates or versions

of records retained in computers that are no longer needed for reference are deleted in accordance with the HRSA Records Disposition Schedule

- j) Prepare information for filing when all actions are completed, when record information is self-identifying, required by a business process, federal law or regulation, or HRSA issuance or an official has requested that documentation be maintained.
- k) Ensure that each record set is complete and that enclosures or related papers, to include e-mail, are retained or accounted for in both paper and electronic filing systems.
- l) Remove all mail control forms, transitory e-mail, classified cover sheets, envelopes, and routing slips, except those containing remarks or information of significant record value.
- m) Major RACI Role: A, I, R.

## III POLICIES AND PROCEDURES

### 1. General Filing Procedures

### 2. Management of Records and Information

- a) HRSA FUNCTIONAL FILES SYSTEM. The HRSA schedule is broken into two parts. The mission specific records disposition schedule resides here on the Records Management SharePoint Site: <https://sharepoint.hrsa.gov/oo/oit/dcppm/recordsmanagement/siteassets/RecordsManagement.aspx>. The HRSA Record Schedule is the NARA-approved schedule that applies to common records found throughout the Executive Branch. The link to the GRS schedule is <http://www.archives.gov/records-mgmt/grs.html>. The implementation of the schedule is based on function. This is the only filing system authorized for the HRSA B/O; modification of the numbering system is not permitted. This enclosure details how to create and maintain filing systems.
- b) RECORDS ARRANGEMENT. Primary considerations are making the files accessible, minimizing duplication, preserving permanent records, and disposition. The factors that must be considered in the storage and maintenance of hardcopy records are:
  - Access. Records will be kept sufficiently accessible and make maintenance of duplicate files unnecessary.
  - Security. PII material maintained with access restricted on a need-to-know basis.
  - Space. Reserve adequate space for present and anticipated needs, factoring in the safety and health of office personnel.
  - Arrangement. Position files equipment and supplies to provide control and convenience to the maximum number of users.
  - HHS policy: <http://www.hhs.gov/ocio/policy/2007-0004.001.html>
- c) FILE PLAN DESIGNATION. Every office within the HRSA each HRSA B/O must have a file plan. Records accumulated and used in performing a function will be located in the organizational element performing the function.
  - The file plan will provide a comprehensive system of identification, maintenance, and disposition of all record information.
  - At a minimum, each file plan must identify the file number, title and brief file description, disposition instructions, media (paper or electronic (see Figure 1)).

Additional information, including record examples, classification, or records custodian, may be added as required by the business process.

- File plans will be updated annually OR office missions are added, changed, relocated, deleted or reorganization.
- RLs are to forward one copy of the file plan to the HRSA Records Officer for review and approval. The RL will maintain a record for all approved file plans. RMT place the approved file plan accessible to all employees and contractor personnel on the [Records Management SharePoint](#) site.
- Offices are to review the HRSA Records Disposition Schedule in the First quarter of each Calendar year OR upon major reorganizations or functional changes to ensure that all records are properly identified and the HRSA schedule is accurate.
- HRSA may centrally locate specialized files of organization-wide interest use. The organizations may also establish decentralized records systems in their offices if they are more effective and convenient. See Section # of this manual for the management of shared drives.
- Each office is responsible for the custody, maintenance, retirement, and disposition of current records and information systems of the office it serves.
- Each office will conduct a records evaluation using the, Records Management Assistance Checklist. Each office will be evaluated at a minimum of every 3 years or when there is reorganization. The form will be maintained with the record copy of the office file plan.

d) RECORDS CATEGORIES. There are three categories of federal records: Temporary (TEMP), Permanent (PERM), and Unscheduled ([See Glossary](#)). The evaluation process (also called scheduling) is participative and includes the RL, RMT, and NARA appraisers, as required.

Figure 1: Sample File Plan

HRSA Schedule ID (HRA or HAS) and code	Related GRS schedule	Record Title/System Title	Description	Disposition Instructions	Format
HRA 19.4		Agency Sponsored Training	General file of agency -sponsored training, EXCLUDING record copy of manuals, syllabuses, textbooks, and other training aids developed by the agency.	Destroy when 5 years completion of a specific training program.	
HRA 19.4	GRS 1.29.a.1	Training records excluding formally established schools	Correspondence, memoranda, agreements, authorizations, reports, requirement reviews, plans, and objectives relating to the establishment and operation of training courses and conferences.	Destroy when 3 years old/ HRA cutoff at end of year, dispose after 1 year	
	GRS 1.29.a.2	Training records excluding formally established schools	Background and working files	Destroy when 3 years old/ HRA cutoff at end of year, dispose after 1 year	
	GRS 01.29.b	Training records excluding formally established schools	Employee training, correspondence, memoranda, reports, and other records relating to the availability of training and employee participation in training programs sponsored by other governmental agencies or non-Government institutions.	Destroy when 5 years old or when superseded or obsolete, whichever is sooner.	Paper, electronic
	GRS 21.14	Video Recordings: Programs Training Acquisitions.	Programs acquired from outside sources for personnel and management training.	Destroy 1 year after completion of training program.	
	GRS 21.17.a	Video Recordings:	Programs that do not reflect the mission of the Department. (These include "role-play" sessions, management and supervisory instruction, etc.)	Destroy 1 year after completion of training program.	

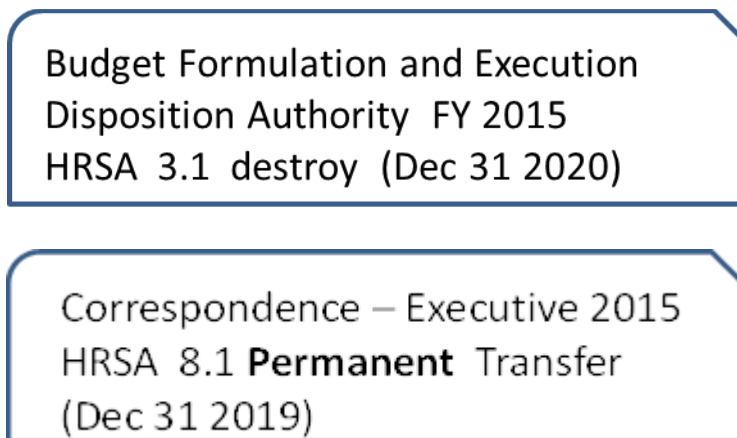
- e) **BASIC FILE GROUPING.** Arrange or group files so that they can effectively document the action, event, decision, or process of the record. Documentation applies to records in all media (paper, electronic, microform, audiovisual, etc.). File arrangement is the relative positioning of information in a file.
- 1) **Subject Files.** Subject files consist of general correspondence but may also be applied to forms, reports, and other material that relate to programs and functions. The subject file provides complete documentation in the appropriate subject area.
  - 2) **Case or Project Files.** A case or project file contains material on a specific action, transaction, event, person, project, or other subject.
    - The information may cover one or more subjects on a case or project but must always be filed by a specific title or number.
    - A distinguishing feature of a case or project file is the similarity of the information within the case folders.
    - Information is arranged within each case file in chronological order with the most recent documentation in front, or by subject, such as statement of work, deliverables, invoices, and modifications.
    - Case or project files are closed upon occurrence of an event or action and placed in an inactive file.
    - Case files may be maintained alphabetically by name, title, country, organization or numerically to permit ease of filing.
  - 3) **Chronological Arrangement.** These files are arranged by date when the date is the primary means of reference. The retention of chronological filing arrangements must correlate to the disposition for mission files in the HRSA Records Disposition Schedule.
  - 4) **Reference Files.** Reference files may include extra copies of documents that are officially stored elsewhere, such as books, pamphlets, and catalogs. Review these files periodically to retain only those that are current and of significant reference value in accordance with the HRSA Records Disposition Schedule.
- f) **FILING ARRANGEMENTS.** The first step in arranging a group of files is to determine the major functional categories that apply. These are listed in the HRSA Records Disposition Schedule. The RMT can also assist in making this determination.
- **Numerical Arrangement.** Files identified and retrieved by sequential number.
  - **Chronological Arrangement.** Files identified and retrieved by date.
  - **Alphabetical Arrangement.** Files identified and retrieved by subject and name.
  - **Name.** Files arranged by names of persons, companies, organizations, or agencies.
  - **Geographical.** Files arranged by a geographical location such as region, country, state, or county.
  - **Subject.** Subject titles are arranged alphabetically.
  - **Alpha Numeric Arrangement.** Alphanumeric files are identified and retrieved by an alphabetical numeric arrangement, such as contract files.
  - **Functional Arrangement.** Files identified and retrieved by the function to which the information relates and not necessarily the subject.
- g) **FUNCTIONAL FILE SYSTEM CONCEPT**
- The functional file system is based on the concept that an office maintains records documenting the performance of each of its functions.
  - The HRSA functional file system identifies and arranges records following the principle that identification or coding of records, papers, correspondence, and communications are related to the agency mission.
  - Select the proper file designation (see Table 1) by referring to the series and title descriptions listed in the HRSA Records Disposition Schedule.

Table 2: HRSA Records Schedule Categories

1	Administrative and Program Related
2	Program Records
3	Budget Formulation
4	Advisory Committee
5	Legislative Affairs
6	HRSA E Systems

- h) **APPLICABILITY.** The HRSA records disposition schedule system will apply to all records and information, regardless of media.
- i) **FILES CONTROL**
  - The management of information depends upon establishing continuous and systematic control over the creation, maintenance and disposition of agency records and information.
  - File folders must be established and labeled with all the information required to identify the information or papers in the folders, but they do use, and not necessarily have to be in the exact format shown in Figures 2 through 6.
- j) **FILES CUTOFF PROCEDURES.** “Files cutoff” is the point when active files no longer needed for current business operations are moved to an inactive status on a calendar or fiscal year basis, whichever is appropriate, all offices will cut off files and separate active from inactive; retire, transfer, or destroy eligible material according to disposition procedures contained in the HRSA Records Disposition Schedule, and review and destroy all duplicate or extraneous materials.
  - Calendar year files on December 31.
  - Fiscal year files on September 30.
  - Files with a retention period of less than 1 year on a monthly or quarterly basis.
  - Files maintained as case or project files upon the occurrence of a certain event, such as separation of personnel, final contract payment, or project completion. Upon cutoff, move files to an inactive file until they are eligible for destruction or transfer to an FRC, in accordance with disposition procedures in the HRSA Records Disposition Schedule.

Figure 1 - Examples of Guide Cards and File Drawer Entries



- k) **PREPARING AND USING GUIDE CARDS, FILE FOLDERS, AND LABELS**

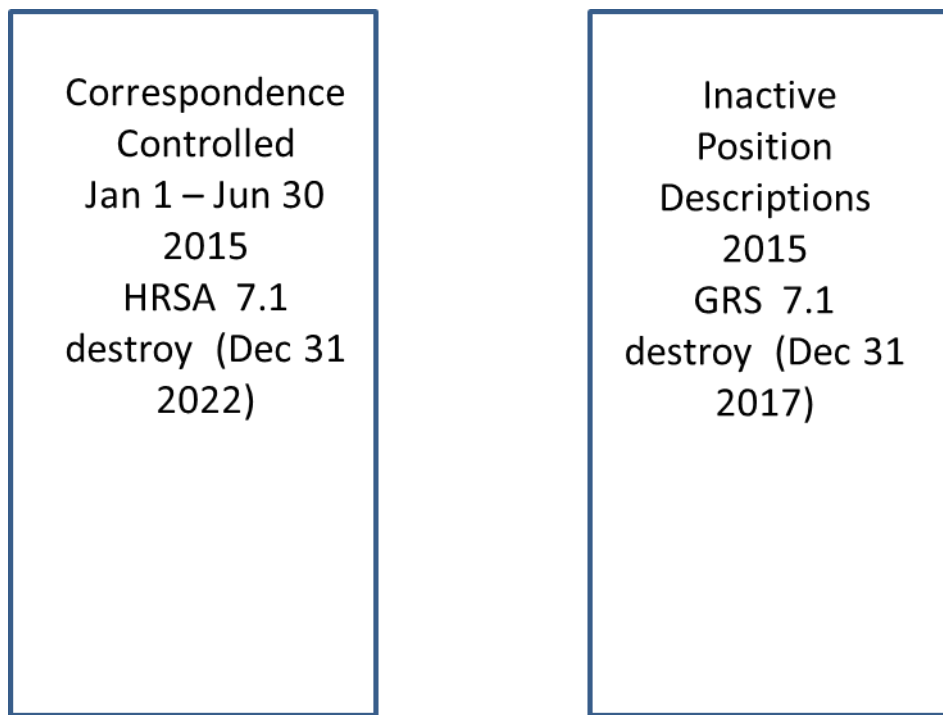
- Guide Cards. Prepare and use guide cards to identify each major file series or to identify and support portions of the series: type standard labels and attach them to the guide card tab; do not retire or discard file guides when files are disposed of; they should be reused (Figure 1).
- File Folders. Type identifying data on standard labels, positioning them on the folders as outlined in Figure 3. This saves repeating all the same information on the succeeding folders in that series, which require only the basic series number followed by the file name (see Figure 3).

Figure 2 - Samples of Folder Label Entries



- Preparation of Labels. Label all file folders, binders, or electronic media with the file number, title, year file created, disposition instructions, and PA SORN number, if applicable (see Figures 4 through 5)

Figure 3 - Samples of Label Entries for Binders



l) LABELS FOR ELELECTRONIC MEDIA

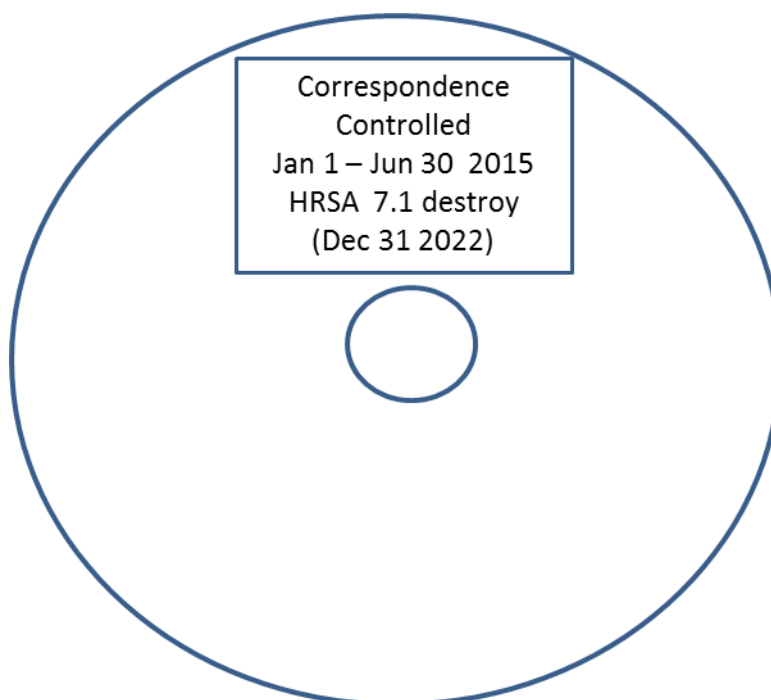
- Type data on standard labels. Position them on the media (e.g., diskettes, compact disks (CDs), digital video disks (DVDs), external hard drives) as shown in Figure 5. Labels should contain file number, title, date, author or creator, office name, type of record or name of office (if applicable), PA SORN or security classification (if applicable), software version, and file extension. All files should have a standardized naming convention (example: X:\Research Services\Meetings\2005\_01\_01\_04Agenda.doc) and date format (i.e., YYYYDDMM). In addition the following files must be included in ASCII text format in the media.
- A readme.txt file which contains the author’s name, agency, and specific information on the diskettes, CDs, or DVDs. Example: Information was prepared by John Doe, B/O XYZ. Information herein contains the Audit Reports for the first quarter of 2002.
- A directory for CDs, DVDs, and external hard drives only if they contain various types of information. The directory should contain the number of diskettes, CDs, or DVDs (if more than one is required) and type of information contained, for example: Audit reports, background information, and HRSA Inspector General or Government Accountability Office responses. LABELING FILE DRAWERS. Label file drawers to facilitate retrieval, and use discretion to prevent revealing the classifications of material stored therein. Only the major file series and inclusive dates of the material will be indicated (see Figure 3).

m) MANAGEMENT OF DOCUMENTS AND INFORMATION. Personnel will:



- Prepare information for filing when all actions are completed, when record information is self-identifying, required by a business process, federal law or regulation, or HRSA issuance or an official has requested that documentation be maintained.
- Ensure that each record set is complete and that enclosures or related papers, to include e- mail, are retained or accounted for in both paper and electronic filing systems.
- Remove or destroy identical or duplicate copies of information before filing. Ensure that duplicate copies of such records retained for convenience are identified as such and any duplicates or versions of records retained in computers that are no longer needed for reference are deleted in accordance with the HRSA Records Disposition Schedule.

Figure 4 - Sample of Label Entries for Electronic Media



- n) LABELING FILE DRAWERS. Label file drawers to facilitate retrieval, and use discretion to prevent revealing the classifications of material stored therein. Only the major file series and inclusive dates of the material will be indicated (see Figure 3).

### 3. Packing and Shipping Procedures for R/O Transfer of Records

- a) PACKAGING RECORDS FOR TRANSFER TO FRC. Records are transferred in standard General Services Administration (GSA) cardboard boxes each holding 1 cubic foot.. No exceptions are permitted. The boxes will accommodate either letter- or legal-sized material. Special containers may be obtained for oversized materials or magnetic tapes.
- b) SHIPPING CONTAINERS AND RELATED SUPPLIES.

- For additional assistance on how to use ARCIS, contact the RMT at: [recordsmgmnt@hrsa.gov](mailto:recordsmgmnt@hrsa.gov)
  - The standard record shipping container to be used for the transfer of files is a fiberboard (lock bottom with reinforced hand holes on each side); 275-pound test; Style 2, Size C; FSN: 8115-00-117-8249. These boxes can be ordered from the GSA website: [https://www.gsaadvantage.gov/advantage/catalog/product\\_detail.do?gsin=11000004924238](https://www.gsaadvantage.gov/advantage/catalog/product_detail.do?gsin=11000004924238)
  - Half-size box, 14-3/4 X 9-1/2 X 4-7/8 inches, NSN: 8115-00-117-8338. For shipping 3 by 5-inch card files when strips of cardboard are placed between rows of cards and wadded paper is used to fill any open space in the box. In addition, this box is suitable for shipping punched cards.
  - Magnetic tape box, 14-3/4 x 11-3/4 x 11-3/4 inches for magnetic tape records, NSN: 8115-00-117-8347.
  - Microfiche box, 14-3/4 x 6-1/2 x 4-1/2, NSN: 8115-01-025-3254.
- c) REQUISITIONING. Boxes can be ordered through Program Support Center (PSC), using the B/O CAN number.
- d) TRANSFER FORM (SF 135). The electronic SF 135 can be accessed from the RM SharePoint site: <https://sharepoint.hrsa.gov/oo/oit/dcppm/recordsmanagement/siteassets/Records%20Management.aspx>
- The SF 135 serves as a packing list; shelf location, disposition, and a receipt.
- The SF 135, numerates s a block of records with the same disposal authority and disposal date.
  - Detailed instructions for completion of the SF 135 are on the [RMT SharePoint site](#) or contact [RMT](#) for assistance.
  - The electronic version SF 135 is prepared by the Bureau /Office RL.
  - The box list is prepared by the B/O RL (see Figure 1).
  - The box list must describe the records at the folder level.
  - Do not list information protected under the Privacy Act on the SF 135. The SF 135 and box list is considered a publicly accessible record.
  - Limit the number of boxes on the SF 135 to 100.
  - Submit the completed SF 13 5 via ARCIS.

# HRSA Records Management 2016

Figure 5 - Completed SF 135

RECORDS TRANSMITTAL AND RECEIPT				Complete and send original and two copies of this form to the appropriate Federal Records Center for approval prior to shipment of records. See specific instructions on reverse.				PAGE <b>1</b>	OF PAGES		
<b>1. TO</b> <i>(Complete the address for the records center serving your area as shown in 36 CFR 1228.150.)</i>  <div style="text-align: center;"><b>Federal Records Center</b></div> <div style="font-size: x-small; text-align: center;">                     WASHINGTON NATIONAL RECORDS CENTER                      9305 SUTLAND ROAD                      SUTLAND MD 20746-8001                 </div>				<b>5. FROM</b> <i>(Enter the name and complete mailing address of the office retiring the records. The signed receipt of this form will be sent to this address)</i>  Attn: Records Management Officer Department of Health and Human Services Health Resources and Services Administration IT Security and Records Management 5600 Fishers Lane Room 16-95 Rockville, MD 20857							
<b>2. AGENCY TRANSFER AUTHORIZATION</b> TRANSFERRING AGENCY OFFICIAL <i>(Signature and title)</i> HRSA, Agency Records Officer Jane Dough, 301-555-1212		DATE 02/08/2016									
<b>3. AGENCY CONTACT</b> TRANSFERRING AGENCY LIAISON OFFICIAL <i>(Name, office and telephone No.)</i> HRSA, Agency Records Officer John Smith 301-555-1234 jsmith123@hrsa.gov											
<b>4. RECORDS CENTER RECEIPT</b> RECORDS RECEIVED BY <i>(Signature and title)</i>		DATE									
Fold Line											
<b>6. RECORDS DATA</b>											
ACCESSION NUMBER			VOLUME <small>(cu. ft.)</small>	AGENCY BOX NUMBERS	SERIES DESCRIPTION <small>(With inclusive dates of records)</small>	RESTRICTION <small>(ρ)</small>	DISPOSAL AUTHORITY <small>(Schedule and item number)</small>	DISPOSAL DATE <small>(-)</small>	COMPLETED BY RECORDS CENTER		
RG <small>(*)</small>	FY <small>(b)</small>	NUMBER <small>(c)</small>							LOCATION <small>(j)</small>	SHELF PLAN <small>(k)</small>	CONT. TYPE <small>(l)</small>
512	16		54	54	Motion Picture Films: Video Tapes from 2003 -2010	R	HSA B-351 2.B.1	Perm			
Attachments below. .Box Listing in(last) Box# 54											

e) General Packing Guidance

- Destroy any records eligible for destruction as authorized in the HRSA Records Disposal Schedule.
- Pack records leaving approximately 2 inches.
- Pack records with identical retention.
- Do not pack records on different media (CD-ROM, diskettes, and microfilm) with paper records.
- File labels and folders must be readable and in good condition.
- Do not place rubber bands or clips on records.
- Arrange folders in the order identified on the box list.
- Print legibly.
- Use a permanent black magic marker.
- Information required on the front end of box::
  - accession number TOP Left Hand Corner
  - Agency box number and the total number of boxes (TOP right corner)
  - Customer Reference n (CRN) Number Center below hand hold
  - Number the boxes consecutively in the upper right hand corner of the front end of the box.

Figure: 6 - Front of Retirement Boxes

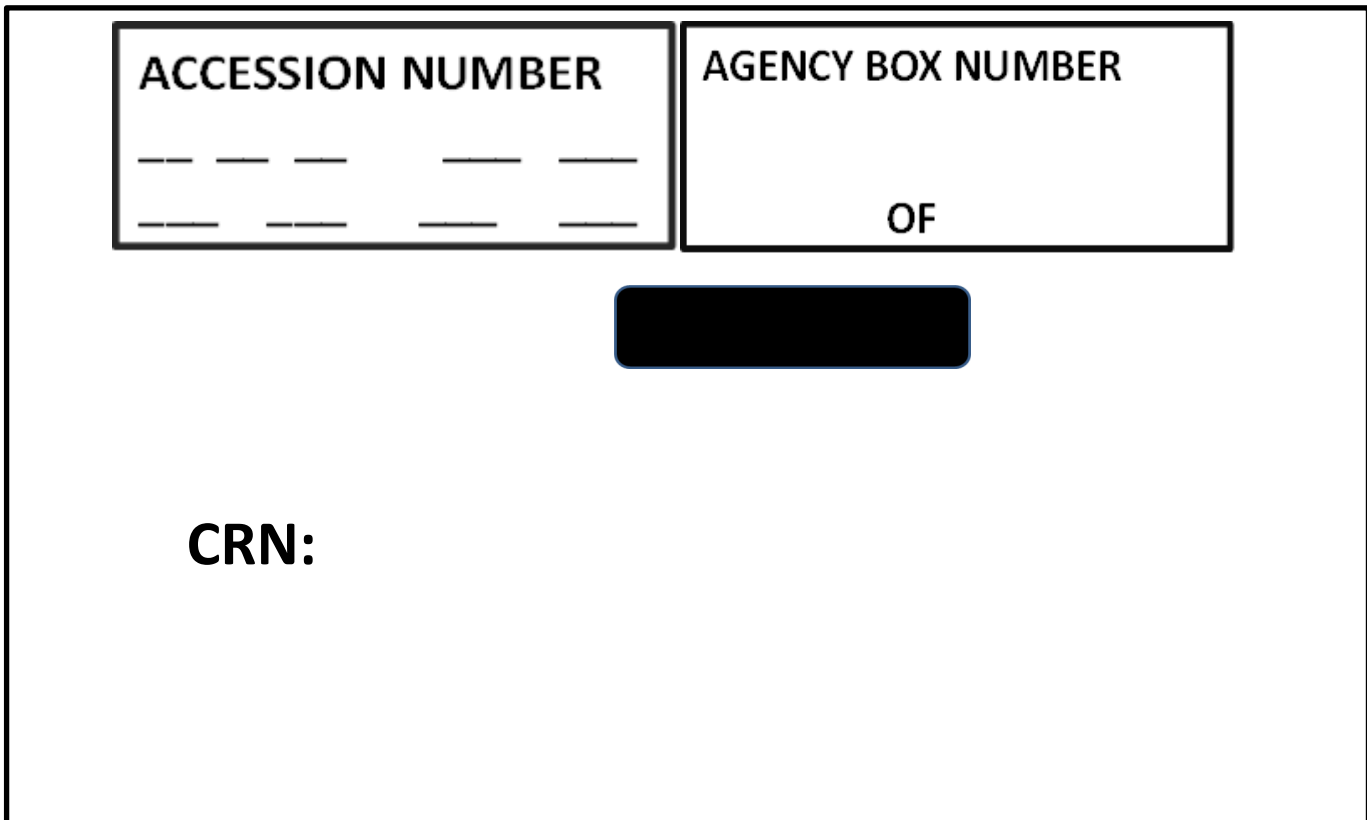
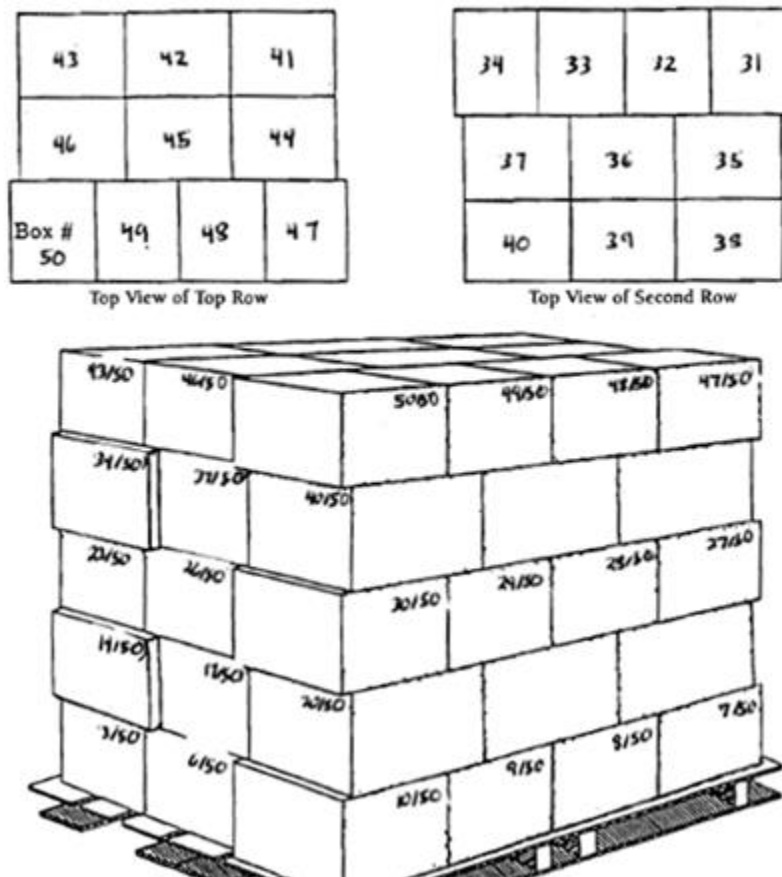


Figure 3: Example and Instructions for a Properly Stacked Pallet



## Instructions:

- 1) Face the boxes as shown in diagram.
- 2) Stacking pattern for palletized records in 10 standard records center cartons per row, 5 rows per pallet, 50 cartons per pallet. Box 50 is in the top row, and box 1 is in the bottom row.
- 3) Four boxes on each row are placed perpendicular to the rest of the boxes in that row.
- 4) Numbered end not facing the front of the pallet should face right.
- 5) When records are boxed before pallets are available, keep the boxes in numerical order so they can be loaded on pallets properly.
- 6) Failure to load pallets properly will be cause for the FRC to refuse the records.
- 7) Pallets should be banded with steel, plastic, or cord strapping before shipping

A list of Federal Records Center locations can be found here: <http://www.archives.gov/frc/locations.html>

## 4. Withdrawing Records from the Federal Records Center (FRC)

- a) OFFICIALS AUTHORIZED TO MAKE RECALLS. The HRSA Records Officer will maintain the authorized personnel authorized by each B/O to recall records. This list will be used to update the [Archives and Records Centers Information System \(ARCIS\)](#) access, and provide training to designee.

The RMT will serve as the approving authority to ARCIS. Access and training will be updated annually. Each B/O designee is responsible ordering, and returning recalled records.

- b) **NORMAL RECALL PROCEDURES.** The ARCIS request will be approved by RMT. RMT will be the approving authority for all ARCIS requests. Offices will submit requests via the RL by e-mail, listing accession number, box numbers, file title (if requesting folder), office address, pick-up date and time (if records are to be picked up by office staff). The request will state whether it is a temporary or permanent withdrawal, and provide POC information (no location number needed for ARCIS) to RMT. For records being picked up at the FRC by office staff, a minimum 3 days' notice is required for non-emergency requests.

*\*Customers having high-volume requirements may obtain an ARCIS account through RMT and access the system directly. For more information about ARCIS, RLs should contact the RMT POC.*

- c) **URGENT REQUESTS.** Urgent requests must be kept to a minimum. An urgent request recalls records needed to complete testimony before Congress, required as part of a legal proceeding, or specifically requested by the Administrator. RMT will arrange all emergency recalls.
- d) **RETURNING RECORDS.** To avoid the misplacing, inadvertent destruction of permanent records, or re-assimilation of recalled records into the current file system, return records to the FRC as soon as they are no longer needed. RMT will report the location of recalled records and the reason for their retention to the HRSA Records Officer when recalled records are retained for more than a year.
- e) Return records in their original folder or box to allow accurate refiling. If the record box or folder is not reusable for shipment, copy the information on the previous container to its replacement. Write the word "REFILE" on the white copy of the ARCIS documentation form that accompanied the records. If these documents are no longer attached to the records, specify the refile action in a brief note or cover letter and attach it to the records being returned. The memo should include the same information used to request the records. The RL or records requestor will notify RMT when records are returned to the FRCs.

## 5. Records Freezes and, Litigations

Numerous situations arise where government records may be required for litigation; an administrative procedure; an audit or an investigation; or to respond to Congressional and public inquiries. Government records and non-records may be critical to the resolution of these matters. Normal records disposition schedules are suspended or held in abeyance and employees are notified that any related materials must be retained until such time that those records are deemed no longer needed for litigation, administrative, audit or investigative purposes and normal disposition may resume.

A "freeze" is essentially a more specific implementation of the broader "hold" concept. A freeze refers to a set of standard procedures whereby the National Archives and Records Administration (NARA) Federal Records Centers (FRCs), upon receipt of notification from a Federal agency or the Department of Justice, temporarily suspend disposition actions of an agency's records and other documentary materials that are in the physical custody of FRCs, but for which legal custody resides with the originating agency.

- a) **CIRCUMSTANCES WHICH MAY WARRANT THE ISSUANCE OF A HOLD**  
A hold may be issued when:

- 1) HRSA is a party to a lawsuit that names HRSA expressly as a party or in which the United States is participating as a plaintiff or defendant. The Office of the General Counsel (OGC), working with the Department of Justice (DOJ), acts as attorney for HRSA and its officials
- 2) DOJ is investigating a matter and HRSA has relevant records in its possession.
- 3) An administrative proceeding, such as a case involving an equal employment opportunity (EEO) or a Merit Systems Protection Board (MSPB) matter, may require the preservation of designated records and related documentary materials.
- 4) A Freedom of Information Act (FOIA) request that is pending or ongoing.
- 5) The Office of the Inspector General (OIG) conducts a financial, performance, or contract or grant audit.
- 6) The General Counsel leads an administrative (non-criminal) or criminal investigation.

## b) RECORDS AND OTHER MATERIALS SUBJECT TO HOLDS

This Policy applies to relevant HRSA programmatic and operational records and non-record materials, in all media, that may constitute evidence in a particular lawsuit or administrative proceeding, or serve as supporting information in an audit or investigation.

- Operational records are records created and maintained throughout Federal agencies to conduct the day-to-day business of the Federal government.
- Programmatic records are records created and maintained in the course of unique programmatic activities of an agency.
- Non-record materials - Those Government-owned documentary materials that do not meet the statutory definition of "records" (44 U.S.C. 3301) or that have been excluded from coverage by the definition. Non-record materials expressly excluded from the statutory definition of records are:
  - Library and museum materials made or acquired and preserved solely for reference or exhibition purposes,
  - Extra copies of documents kept only for convenience of reference, and
  - Stocks of publications and processed documents.
- "Working files and similar materials," including preliminary drafts, rough notes, worksheets, correspondence and memos, reports, and other similar materials (see 36 CFR 1222.12(c)), fall within the scope of programmatic or operational records, if: (1) They were circulated or made available to employees, other than the creator, for official purposes such as approval, comment, action, recommendation, follow-up, or to communicate with agency staff about agency business; and (2) They contain unique information, such as substantive annotations or comments that adds to a proper understanding of the agency's formulation and execution of basic policies, decisions, actions, or responsibilities.

## c) OWNERSHIP, FORMATS AND MEDIA OF RECORDS COVERED BY THIS POLICY

Records created and maintained by HRSA, regardless of physical location and physical format, can be subject to hold/discovery. Particular holds, as each case arises, may call for retention of information in various electronic formats or media to be determined. After consultation with the HRSA Records Management Officer, supervisors and managers must provide to their staffs more specific information regarding formats and media for records and other documentary materials subject to a hold.

## d) AUTHORIZATION TO ISSUE AND REMOVE A HOLD

HRSA Records Management Website:

<https://sharepoint.hrsa.gov/oo/oit/dcppm/recordsmanagement/siteassets/Records%20Management.aspx>

The HRSA OGC is the HRSA official authorized to issue and remove, subject to consultation with DOJ, records/documentary materials holds. However, in the absence of the HRSA General Counsel, an acting HRSA designee is authorized to issue and remove legal holds in circumstances 1 and 2, including the HRSA Department RMO.

- In circumstance 3 (e.g., an administrative proceeding), the HRSA OGC is responsible for notifying the appropriate HRSA office(s) to which the administrative matter applies and for the issuance and removal of legal or administrative holds. The HRSA Department RMO has no role in matters associated with circumstance 3; however; HRSA OGC may be in contact with HRSA's Records Management Officers if determined by OGC to be appropriate.
- In circumstance 4 (e.g., Freedom of Information Act (FOIA) requests), the Department's FOIA Officer is the HRSA official authorized to issue and remove records/documentary materials holds.
- In circumstances 5 and 6 (e.g., HRSA OIG program review, audit, inspection, or investigation), the Department's OIG is the HRSA official authorized to issue and remove records/documentary materials holds. The Office of Counsel to the Inspector General (OCIG) is the legal representative in administrative proceedings in which the HRSA OIG has been cited as a party.
- Where appropriate, the OCIG will issue records holds within the OIG. In FOIA and legal matters where both the HRSA OGC and the OIG OCIG are involved, the OGC and OCIG will discuss the issues and reach a consensus on the implementation of a hold and on internal and external communications.

e) HRSA OGC NOTIFICATION OF A HOLD

When HRSA is a party to a lawsuit that names HRSA expressly as a party, when the United States Government is participating as a plaintiff or defendant, and when DOJ is investigating a matter and HRSA has relevant records in its possession (circumstances 1 and 2 of this Policy), the HRSA OGC, working with the Department of Justice, acts as attorney for HRSA and its officials. The HRSA OGC notifies by written memo (and by more formal means as necessary) the HRSA Executive Secretariat, the HRSA Department RMO, and the HRSA Administrator. As appropriate and based on advice from HRSA OGC, the HRSA Department RMO notifies the HRSA CIO.

- These officials will ensure the distribution to staffs of the information contained in the hold order and ensure the prevention of the destruction of records of all media.
- In circumstance 3 (administrative proceeding, such as a case involving an equal employment opportunity (EEO) or a Merit Systems Protection Board (MSPB) matter), the HRSA OGC notifies the appropriate office(s) affected by the administrative matter.
- The Department's FOIA Officer provides this notification in circumstance 4, and the Department's OIG provides this notification in circumstances 5 and 6.
- The HRSA Department RMO does not need to be notified in circumstances 3, 4, 5 and 6.

f) INITIATING A HOLD REQUEST

In those cases where HRSA managers are aware of the need for the issuance of a records disposition hold as described in circumstance 3, written information must be submitted to the HRSARMO and OGC.



- When circumstance 4 is implicated, written information must be submitted to the HRSA's FOIA Officer.
- When circumstances 5 and 6 are implicated, written information must be submitted to the HRSA Records Office and the department's OIG.
- The HS Department RMO does not need to be notified in circumstances 3, 4, 5 and 6.

## g) NOTIFICATION FROM THE DEPARTMENT

As appropriate and based on advice from HRSA OGC, the HRSA Department RMO notifies the HRSA Records Management Officers and the HRSA CIO for circumstances 1 and 2. HRSA's Records Management Officer notifies affected Bureau's and Offices to preserve textual records and all other non-electronic records and coordinates with OIT to require the preservation of all electronically stored information (ESI).

- For circumstances 1 and 2, the Records Management Officers notify the National Archives and Records Administration (NARA) of a records hold and the NARA implementation of a "freeze." This results in a temporary extension of retention period(s):
  - 1) As stated in 36 C.F.R. § 1226.20, Agencies must secure NARA written approval to retain records series or systems that are eligible for destruction under NARA-approved schedules except when: (1) The agency has requested a change in the records schedule in accordance with § 1225.26 of this subchapter, in which case the agency is authorized to retain records eligible for destruction until the new SF 115 [records schedule] is approved; (2) The records will be needed for less than one year; or (3) A court order requires retention of the records.
  - 2) The HRSA Records Management Officer notifies NARA of records stored at any or all FRCs (including WNRC). NARA's Federal Records Center Program (NR) then carries out the hold by placing a "freeze" on disposition actions affecting those subject records and documentary materials stored at the FRC(s).
  - 3) For circumstances 3, 4, 5 and 6, the HRSA Records Management Officer, in consultation with OGC, OIG, FOIA, and other functions as appropriate, notifies NARA of a records hold. The HRSA Department RMO does not need to be notified.

## h) HRSA STAFF DUTIES AND RECORD HOLDS

Until receiving notice from HRSA OGC, HRSA FOIA Officer, HRSA OIG, or HRSA RMO:

- Do not destroy any documentary materials, including working papers and those temporary records that are eligible for destruction in accordance with the HRSA Records Retention Schedule, this Policy and Procedures Manual and the NARA General Records Schedules.
- Follow instructions about maintaining records and other documentary materials subject to the hold (e.g., centralizing or keeping the records and materials in place; sending the records and materials to OGC, OIG, HRSA FOIA Officer, HRSA RMO, etc.).
- Do not transfer permanent records to the National Archives of the United States, unless a transfer is permitted in accordance with the hold instructions and is approved by the HRSA CIO.
- Do not transfer records to an FRC, unless a transfer is permitted in accordance with the hold instructions and is approved by the HRSA CIO.

## i) CONSEQUENCES FOR NON-COMPLIANCE

Non-compliance with a hold could result in penalties on individual staff and the agency.

- Failure to preserve operational records could constitute an unlawful destruction of records that must be referred to the DOJ Attorney General under 44 U.S.C. 2905(a) and 3106.
- If a HRSA staff member fails to comply with a hold that is in place because of a court order, this individual could be individually sanctioned or held in contempt by the court. Finally, destruction of records under certain circumstances is potentially a criminal violation for which a staff member could be prosecuted under 18 U.S.C. 1519 (see Policy for The HRSA Records Management Program).

j) CONSEQUENCES WHEN NOT ADHEARING TO A HOLD

HRSA and HRSA could be subject to sanctions if records and other documentary materials, deemed as materially re-leant to the issues in litigation, are missing. For instance, the court could:

- Issue an adverse finding (e.g., a court order) against HRSA on the merits of the case;
- Instruct a jury to draw an "adverse inference" against HRSA, meaning that the judge would rule that the content of the missing records and materials would have supported whatever argument that the opposing party has put forward;
- Preclude HRSA from introducing certain evidence and/or calling certain witnesses;
- Hold individual HRSA officials and HRSA in contempt; and impose monetary sanctions against HRSA.

k) HOLD REMOVAL AND NOTIFICATIONS

When the need for the hold has expired, HRSA OGC notifies by memo (and by more formal means as necessary) in circumstances 1 and 2 in this Policy the HRSA Executive Secretariat, the HRSARMO, and HRSA via a SWIFT notification. If not already contacted by the HRSA OGC, the HRSA Department RMO informs the HRSA CIO Community, and HRSA Records Management Officers, who then inform appropriate Bureau's and Offices.

- In circumstance 3, OGC notifies by memo and by more formal means as necessary the affected office(s).
- The HRSA FOIA Officer provides the notification in circumstance 4, and the HRSOIG provides the notification in circumstances 5 and 6.
- The HRSA Records Management Officers notify the National Archives and Records Administration of the removal of the hold.

## 6. Employee Departure Procedures

HRSA records are the property of the government, not the property of individual employees or contractors acting as an agent for the government, and may not be removed from HRSA without proper authority. The purpose of this Policy is to ensure that all material created, received or maintained during an employee's employment or appointee's tenure with the Federal Government that meets the criteria for a Federal record remains in Federal custody when an employee or appointee departs the Agency. It also reiterates the special consideration given to Presidential Records Retention requirements (44 U.S.C. 22).

This Policy applies to all departing employees, contractors, volunteers and political appointees, regardless of the type or duration of appointment. The scope includes employees who are reassigned to new official duty locations within HRSA, those who are transferred to other Federal agencies, and those who leave Federal service. Agency officials shall apply this Policy to employees, contractor personnel,

volunteers, and political appointees by incorporating references in contracts or memorandums of agreement.

HRSA staff and contractors working for or on behalf of the Federal Government create and maintain several types of Federal records. All employees and contractors shall maintain records and non-record documentary materials separately from one another: different file folders, email folders, etc. Co-mingling of Federal record and non-record materials means FOIA requests can and will include Federal records and non-record materials.

a) **HRSA DEPARTING EMPLOYEE AGREEMENT AND MATERIALS REMOVAL**

The HRSA Departing Employee Agreement and the Materials Removal Certification should be signed by a departing employee, contractor, volunteer or political appointee that all Federal records, regardless of media, have been identified and transferred to the records management liaison or custodian, Contracting Officer's Representative (COR), or have been reassigned to another employee. These documents are available on the HRSA Forms SharePoint site and at the end of this section. The departing employee and the Records Management Officer, Supervisor and a review official must sign these documents.

b) **MAINTAINING DOCUMENTARY MATERIALS.** Follow the steps listed below to meet your record keeping requirements:

- Sort: Record material; Non-record material; and Personal material.
- As you sort material, destroy extra copies; destroy reference material that only you would need.
- Create a personal (.pst) folder for your personal information. Move your personal information from your mail box to that folder. You should also delete all information that is not a record.
- Give access to your mail box to your support staff with instructions to contact the subject matter experts for disposition guidance for the remaining messages.
- Transfer custody – Deliver all federal record materials to your supervisor or designated custodian. You must meet with your supervisor to certify that all federal records have been identified and transferred to your supervisor, designated custodian, or reassigned to another employee. Complete and sign the employee departure form and attachments as applicable.
- Seek permission – You are likely to have extra copies of records kept for convenience of reference in your office or workstation. Please note that non-record materials may NOT be removed from HRSA, only if:
  - 1) Removal would not diminish the official records of the agency;
  - 2) The material does not contain confidential information;
  - 3) The information removed is not subject to the Privacy Act of 1974
  - 4) You have the approval of your supervisor and RMO or the Freedom of Information Act (FOIA) Officer or legal counsel.

The record copy you leave provides the evidence and history of the work you performed. It must be organized in a meaningful manner; and, when appropriate, transferred to NARA. For assistance contact your B/O HRSA Records Management Liaison or RMO.

c) **REMOVING DOCUMENTARY MATERIALS.** The following types of documentary materials may NEVER be removed:

- Any Federal record;
- The only copy of any documentary materials involved in the conduct of the affairs of HRSA or any other components of the Federal Government, whether or not judged to be records (including any copy that is unique, for example, because it contains the signature or initials of the writer, reviewers, and/or concurring parties);
- Any documentary materials (whether or not judged to be records) the removal of which will create such a gap in the files as to impair the completeness of essential documentation. Indexes, or other finding aids, necessary for the use of the official files may not be removed;
- The only copy of indexes or other finding aids (whether or not judged to be records) that are necessary to the use of office files;
- Portions of documentary materials (whether or not judged to be records) that constitute information subject to the Privacy Act of 1974, 5 U.S.C. § 552a;
- Portions of other documentary materials (whether or not judged to be records) that constitute information the disclosure of which is prohibited by law, such as grand jury, tax, and trade secret information.
- All other types of nonpublic Federally-owned documentary materials, including privileged materials, may be removed only with specific approval from the appropriate Agency Records Management Officer.
- Departing or former employees and political appointees of HRSA may request the following:
  - Removal of or access to documentary materials that are reasonably related to the requester's official responsibilities while an employee.
  - All records, originals and copies, are under the control of HRSA, regardless of how and by whom they were created or obtained. Removal of documentary material must be approved in accordance with the preceding provisions to ensure that HRSA's ability to claim privileges in litigation, to claim Freedom of Information Act (FOIA) exemptions, and to protect sensitive and classified information.
  - Records will not be disposed of or removed while they are the subject of a pending request, appeal, subpoena, litigation or lawsuit under the FOIA or the Privacy Act, as provided for in General Records Schedule 14 and HRSA Policy.

#### d) RESPONSIBILITIES

The Agency Records Management Officer and Bureau and Office Records Liaisons shall:

- Ensure that non-record material being removed by a departing employee or official is examined by the Records Management Officer or a Records Liaison for the purpose of providing the appropriate protection for information that is restricted from release under the Privacy Act or other statutes, regulations or executive orders
- Obtain and maintain signed form: "HRSA Document Materials Removal Certification with Non-disclosure Agreement."
- Ensure that the signed agreement and related documentation are retained in a centralized file by the Records Management Officer or Records Liaison; and
- Receive the detailed inventory list of records and non-records to ensure that no departing official, employee, contractor or volunteer removes records or non-record materials relating to any pending or contemplated civil, criminal, or administrative proceeding, FOIA or Privacy Act request or appeal, or subpoena without clearance of the Office of the General Counsel (OGC) or relating to another program activity without clearance of the responsible program official.

## Supervisors shall:

- Ensure that departing employees, contractors and volunteers departure dates are identified as soon as possible and these individuals are made aware of their records responsibilities;
- Ensure that non-record material that is the subject of a request for removal or access by a departing individual is examined by the agency head (or his or her designee) for the purpose of providing the appropriate protection for information that is privileged or restricted from release under the Privacy Act or other statutes, regulations or executive orders;
- Decide upon requests made for removal of, or access to, documentary materials;
- Ensure the departing or former employee's request is for copies of or access to only documentary materials that are reasonably related to the requester's official responsibilities while an employee;
- Ensure the request by a former employee for copies of or access to documentary materials pursuant to this manual is received no more than one year after the employee leaves the HRSA's employment. Any requests for documentary materials after such date may be submitted in accordance with the FOIA;
- Obtain and maintain signed form: "HRSA Document Materials Removal Certification with Non-disclosure Agreement" from all departing employees, contractors or volunteers under their purview. Ensure that the signed agreement and related documentation (including requests or authorizations for removal or access) are retained by the agency;
- Approve every request submitted in writing and in sufficient detail to identify which documents may be removed or accessed, under what conditions or restrictions, and for which documents removal or access is denied;
- Ensure the departing employee, contractor or volunteer only removes personal papers that have been properly segregated. Any question as to whether materials constitute personal papers or are publicly available should be referred to the Agency Records Management Officer and the OGC.

## Senior Officials:

Although Federal records may not be removed, departing senior officials are allowed to create a limited number of duplicate copies of unclassified documents for personal use when warranted by the level of the position, significance of the work or research. Such copies are considered non-record material and must be reviewed and approved by the Records Management Officer or Records Liaison before they may be removed. Classified and Privacy Act documents may not be duplicated or removed from Federal custody.

## Prior to departure, senior officials and political appointees shall:

- Identify Federal records of which they have custody.
- Records regardless of media shall be inventoried and those on file servers, hard drives, and in electronic mail systems shall be copied and removed or reassigned.
- Inactive records shall be transferred to a records management custodian and active records shall be reassigned to another employee.
- All file searches for which the employee has been tasked must be completed or reassigned, such as FOIA, Congressional or litigation-related document requests.

## Employees, Contractors and Volunteers:

- All employees are responsible for the Federal records in their custody. This responsibility applies to employees separating from as well as transferring to another HRSA agency. Prior to departure, employees, contractors, and volunteers shall identify

Federal records for which they have custody and are responsible for any applicable procedures described herein:

- Records, regardless of media shall be inventoried and those on file servers, hard drives, and in electronic mail systems shall be copied and removed or reassigned.
- Inactive records shall be transferred to a records management custodian and active records shall be reassigned to another employee.
- Depending on the status of the contract, the departing contractor employee's records shall be reassigned to another contractor or Federal employee or incorporated into HRSA's official files.
- All file searches for which the employee, contractor, or volunteer has been tasked must be completed or reassigned, such as FOIA, Congressional or litigation- related document requests.
- Maintain record and non-record documentary material according to prescribed HRSA Policy and procedures.
- Safeguard records until they are authorized for disposition. The unauthorized removal, concealment, falsification, mutilation, or disposition of official records is prohibited by law and is subject to penalty (18 U.S.C. 2071).
- Clearly designate as personal those papers of a private or nonofficial nature pertaining solely to personal affairs. Those papers shall be filed separately from the records of the office.
- Report any apparent instances of unauthorized disposition to his/her supervisor.
- Request permission to remove copies of materials prior to leaving HRSA. The request must be submitted in writing to the head of the component in which the requester is or was employed. The request must describe the documentary materials with sufficient detail to permit their retrieval. Departing employees should assemble the requested material and attach them to the request, or if the materials are voluminous a detailed inventory list should be attached explaining how the requested material may be readily assembled.
- Meet with their Federal supervisor or Contracting Officer's Representative (COR) and the Agency Records Management Officer prior to departing HRSA.

e) STATUTORY PENALTIES AND REQUIREMENTS

The disposal of Federal records in agency custody is governed by specific provisions of Chapter 33 of Title 44, United States Code (Disposal of Records). Criminal penalties are provided in 18 U.S.C. § 641 (Public Money, Property or Records) and §2071 (Concealment, Removal, or Mutilation of Records) for the unlawful removal or destruction of Federal records.

Figure 7 – Employee Departure Form

**Health Resources and Services Administration Employee Departure 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 agency business; diaries, journals, personal correspondence, or other personal notes that are not prepared or used, 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, prior approval have been obtained from the Records Officer and the Freedom of Information Act (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. Are you removing any non-record documents, such as extra copies of agency records, from Health Resource and Service Administration (HRSA)?**

a. YES \_\_\_\_\_ Complete attachment 1 certification with the Reviewing Official.  
Initial \_\_\_\_\_

b. NO \_\_\_\_\_  
Initial \_\_\_\_\_

By my signature below, I certify that I am not removing any federal record from HRSA

## IV ELECTRONIC RECORDS MANAGEMENT

### 1. Electronic File Folder Structures

Each Office and Bureau within HRSA has a file plan. The file plan identifies record types that are specific to that Office/Bureau, locations of records, and records dispositions. The dispositions (how long to keep records) come from the HRSA Records Schedules and the GRS. Similar to a physical file cabinet, files stored on the shared drive are organized by folder, and labeled according to document type. Records Liaisons and the Records Management Team will assist with the setup of an electronic file folder structure that meets the business needs of the Office/Bureau. Once an agreed upon structure has been established, it will be the responsibility of each Records Liaison, Office, Bureau, Division, and Branch to:

- Ensure that records are captured and maintained on the shared drive pursuant to their file plan
- Apply appropriate disposition authorities to electronic records stored on shared drive
- Dispose of non-record, unstructured data as appropriate
- Prevent the unauthorized access, modification, or deletion of declared records
- Identify and label new record content in accordance with the file plan
- File related records appropriately (e.g., grants, contracts, PMAPS etc.)

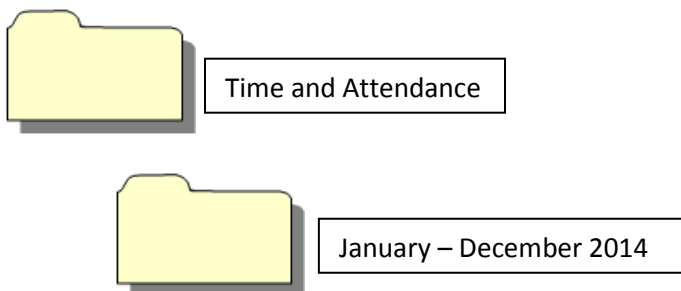
a) Records Disposition:

Standardized naming conventions for files, and file folder structures organized by date will help determine when to delete electronic records. Related records will be grouped together, making the deletion process easy and convenient for each Records Liaison. HRSA staff will follow the disposition specified in the Office/Bureau file plan for that particular group of records. In this example below, the files can be destroyed in Fiscal Year 2020:

Time and Attendance Input Records.

Records in either paper or machine readable form used to input time and attendance data into a payroll system, maintained either by agency or payroll processor.

Destroy after GAO audit or when 6 years old, whichever is sooner.  
(N1-GRS-92-4 item 8)



b) Social Media, Web Content, and Databases:



Electronic records include not only commonly used formats (PDF, Word, Excel); but also web content, databases, and other lesser-known file types. This electronic content is to be managed in the same way as other electronic records. NARA is in the process of releasing a GRS that will cover web site records. This schedule will cover the many HRSA SharePoint web records that are currently housed on the shared drives across the organization. The Records Management Branch will partner with Records Liaison and disseminate guidance on proper procedures for capturing social media and web content classified as record material.

Databases are used to automate processes and to store information. If the files (records) that makeup the inputs and outputs to the database have an existing GRS or HRSA disposition authority that covers the information, then the system owner is expected to follow the corresponding retention requirements. Please consult the Records Management Team if you have an electronic information system that may require scheduling.

## 2. Electronic Transfer Records

### a) Permanent Records:

Permanent electronic records are transferred to NARA at the end of their lifecycle. The procedure is as follows:

- B/O Records Liaison notifies the HRSA Records Management Team when data is eligible for transfer.
- The Records Liaison completes the [SF258](#).
- The Records Liaison prepares records for transfer to include the following:
  - Electronic records in the format specified by NARA (PDF is the preferred format)
  - System documentation that provides information on how the system captures, manipulates, and outputs data (e.g. data layouts, data models, and code lists).
- If the system documentation is available only in paper, then make a complete copy and send to NARA with the electronic data.
- The completed [SF258](#) is sent to the HRSA Records Officer, along with the electronic files to be transferred. The electronic files maybe received via email, or other approved storage media (CDs, DVDs, etc.).
- The Records Officer reviews the [SF258](#) and the files for accuracy and completeness.
- If there are no necessary changes, the Records Officer then uploads the files into [NARA's ERA System](#).
- Once the transfer is complete, the Records Officer receives a copy of the completed transfer paperwork via email.
- A copy of the completed transfer paperwork is also sent to the Records Liaison.

### b) NARA's Electronic Format Requirements:

NARA has special format requirements as stated in [36 eCFR 1235 Subpart C](#). In addition to the formats specified in the Code of Federal Regulations (CFR), NARA is now accepting other formats:

- [Portable Document Format \(PDF\) files](#)
- [Email](#)
- [Digital photographs](#)
- [Geospatial information](#)
- [Web content](#)

Standard Form 258, "Agreement to Transfer Records to the National Archives of the United States," is used to transfer records to NARA for permanent storage.

Figure 8: SF-258, Agreement to Transfer Records to the National Archives of the United States

<b>AGREEMENT TO TRANSFER RECORDS TO THE NATIONAL ARCHIVES OF THE UNITED STATES</b>		AUTHORIZED FOR LOCAL REPRODUCTION 1. INTERIM CONTROL NO. (NARA Use Only)
TERMS OF AGREEMENT		
The records described below and on the attached _____ pages are deposited in the National Archives of the United States in accordance with 44 U.S.C. 2107. The transferring agency certifies that any restrictions on the use of these records are in conformance with the requirements of 5 U.S.C. 552.	use of these records will be imposed other than the general and specific restrictions on the use of records in the National Archives of the United States that have been published in 36 CFR Part 1256 or in the Guide to the National Archives of the United States. The Archivist may destroy, donate, or otherwise dispose of any containers, duplicate copies, unused forms, blank stationary, non-archival printed or processed material, or other non-record material in any manner authorized by law or regulation. Without further consent, the Archivist may destroy deteriorating or damaged documents after they have been copied in a form that retains all of the information in the original document. The Archivist will use the General Records Schedule and any applicable records disposition schedule (SF 115) of the transferring agency to dispose of non-archival materials contained in this deposit.	
2A. AGENCY APPROVAL	3A. NARA APPROVAL	
Signature _____ Date _____	Signature _____ Date _____	
2B. NAME, TITLE, MAILING ADDRESS	3B. NAME, TITLE, MAILING ADDRESS	
RECORDS INFORMATION		
4A. RECORDS SERIES TITLE		

### 3. Email and Calendars

This policy applies to all users who have been assigned an e-mail account on the HRSA e-mail system. Because e-mail is potentially a Federal record, all government employees, appointees, contractors, and others working on behalf of HRSA must decide whether e-mail messages sent or received should be kept, and if so, preserve them.

Information in e-mail may include, but is not limited to, correspondence, file attachments, calendar schedule invitations, and electronic forms. An e-mail communication may constitute a Federal record when the message meets the definition under the Federal Records Act. It can carry records or non-records.

Electronic messages will contain content which raise them to the level of an official record that is subject to established Agency retention and disposition policies based upon content.

Information transmitted may be considered a record if it serves as evidence of an office’s activities, events, or business transactions. E-mail, including attachments, and instant messages, must be identified, managed, protected, and retained as long as needed for continuing operations, audits, legal proceedings, etc.

a) OWNERSHIP OF E-MAIL

E-mail transmissions declared as Federal records are Government property and may not be disposed of except in accordance with approved records schedules.

In accordance with HHS Email policy, effective December 1, 2014, ALL Senior Executive Service will be treated as a permanent record. Senior Executive Service e-mail account holders will not be permitted to create Personal Storage Table or .pst files

## b) POLICY

- Each e-mail user (i.e., creator or recipient) shall take responsibility for identifying whether an e-mail communication fits the definition of a Federal record. If deemed to be evidence of one's activities, the message shall be retained, preserved, and disposed of in accordance with a NARA-approved records schedule.
- Employees should not have the expectation of privacy in anything they create, send, receive or store on the HRSA e-mail system. This includes instant messaging. Messages stored on, but not limited to the Outlook Exchange Mail server, Personal Storage Table (.pst) files residing on a shared network drive or local drive, and messages saved to portable storage devices (e.g., DVD, flash or USB drive) are subject to search for purposes of responding to disclosure requests (e.g., FOIA, litigation holds, etc.).
- All employees shall manage Federal records created in or transmitted using the HRSA e-mail system in a manner that allows each to be accessible and readable for the NARA-approved record retention period. Be aware that your decision to retain or destroy an e-mail message may become an issue in a legal matter.
- E-mail is a transport mechanism only. Large amounts of retained messages use finite information technology resources and may adversely impact the efficient function of HRSA computer systems. For these reasons, the e-mail system is not intended to be used for permanent storage of messages. It is not an approved recordkeeping system. Until HRSA adopts a software solution for archiving e-mails, messages considered records must be printed and filed in a paper recordkeeping system or stored in an electronic form other than e-mail.
- No records (attachments, policies, PAL, PINS) shall exist solely in a user's active e-mail Inbox, Sent or Deleted items folder.
- Users shall open their e-mail on a regular basis (at least daily, if possible), delete unneeded items, classify, and file items needed for future reference appropriately so as not to fill up their incoming mail file (inbox).
- Any e-mail message that is required to be kept beyond six (6) months shall be printed out and filed in similar fashion to paper records or transferred to a portable storage device (e.g., DVD, flash drive) and appropriately stored.
- E-mail messages shall be kept with any attachment(s). The e-mail shall contain the following header information:
  - Who sent the message
  - To whom the message was sent.
  - The date and time that the message was sent.
  - The subject of the message
  - Users shall keep receipt data which is information in e-mail systems regarding date and time of receipt of a message, and/or acknowledgement of receipt or access by addressee(s) will not be kept beyond six (6) months.
  - If a distribution list was used to send a message, a list of the names of individuals who are part of the distribution list needs to be kept. This provides a way to identify the actual recipients if the e-mail record simply lists the group name in the recipient field. Expanding the distribution list is the responsibility of the sender of the record.

- E-mail calendars and task lists that meet the definition of a Federal record will be identified, maintained, and retained using the appropriate retention value.
  - Print documentation containing information about the receipt of the message when required for recordkeeping purposes, and attach it to the message. (If the sender requested a receipt for recordkeeping purposes in accordance with agency criteria, he or she will retain the printed message and transmission document until receipt is received.)
  - Preserve electronically transmitted messages that are Federal records where an acknowledgement of receipt or an acknowledgment that an addressee opened the message was requested. Preserve the acknowledgement with the record copy if returned. Preservation of receipts is part of the “sender’s” record copy.
  - Certain information containing sensitive or restricted (e.g. Personally identifiable information) data shall not be stored, transmitted, or processed using email infrastructure unless appropriate information security mechanisms (e.g. message encryption) are used.
  - The e-mail account of a separating employee shall be disabled and not purged by OIT. The account shall not be purged until notice is received from the departing employee’s manager or supervisor.
  - Records created using e-mail shall be retained based on the content of the e-mail, not the medium. E-mail messages fall within three (3) broad categories: Transitory, Temporary, and Permanent records.
- **Transitory:** Casual and routine communications should not be retained due to their limited value. Most e-mails are transitory and should be deleted in six (6) months. The following types of e-mail can be deleted because they are transitory:
    - Personal e-mails unrelated to HRSA business.
    - Incoming listserv messages.
    - Spam or unsolicited advertisements must be sent to the junk email.
    - Scheduled meetings, invitations and responses to meetings.
    - Announcements, acknowledgments, and thank-yous
    - Circulating copies of agency instructions, circulars, internal newsletters, other than master copies provided as a courtesy.
    - Out of Office automatic replies.
    - Attachments to e-mail that are identical to records that are stored and managed outside the e-mail system pursuant to a NARA-approved records schedule.
    - Agency wide electronic broadcasts, alerts, news, and newsletters.
  - **Temporary records** created have documentary value but will eventually be deleted/destroyed. These records will be maintained IAW the HRSA approved records schedule or the National Archives General Record Schedule <http://www.archives.gov/records-mgmt/grs.html>
    - E-mail documenting answers to audit questions must be retained for 10 years.
    - E-mail communications discussing employee awards must be retained for 2 years.

- E-mail discussing administration of a personnel security program must be retained for 2 years.
- E-mail discussing the installation and testing of individual information technology projects must be retained for 3 years.
- Email transferred to the EHB electronic system through the plug in can be destroyed after 180 days
- **Permanent** retainable records have significant administrative, legal, and/or fiscal value. Examples are:
  - Correspondence providing key substantive comments on a draft memorandum, if the e-mail adds to a proper understanding of the formulation or execution of Agency action.
  - Messages documenting oral exchanges, such as meetings or telephone conversations, during which policy was discussed or formulated or other agency activities were planned, discussed and not otherwise documented in Agency files.
  - Messages that convey information of value on important Agency activities, if the e-mail message adds to a proper understanding of Agency operations and responsibilities.
  - E-mail, calendars, and instant messages regarding the conduct of business SES officials conducting Agency business.

## c) ROLES AND RESPONSIBILITIES

- **E-mail Users:** It is the responsibility of the user of the e-mail system, with guidance and training from the Records Management Officer, to manage e-mail messages according to the Government's established retention periods. All e-mail users are expected to:
  - Read, understand, and follow the e-mail retention policy.
  - Create records that provide complete and accurate documentation of one's activities.
  - Utilize training to determine which e-mail transmissions should be kept and preserve them.
  - Classify e-mail messages to determine which records series defines how long the message should be kept.
  - Organize their e-mail messages so they can be located and used.
  - Not retain messages longer than required. When the need no longer exists, the message should be deleted.
  - Protect records from loss, damage, improper destruction, and unauthorized disclosure.
  - Preserve all e-mail content that falls within the scope of a litigation hold regardless of where the data resides. This includes, but is not limited to content stored in e-mail inboxes, portable devices, and on network drives.
- **Office of Information Technology (OIT)**
  - Establish and publish standards for e-mail account administration and storage allocations.
  - Ensure that staff is trained and informed about use of e-mail in the workplace.
  - Provide helpdesk support.
  - Implement automated data purge mechanisms in the Agency's email service.

- Manage server implementations of legal holds that are issued by the Office of General Counsel (OGC).
  - Eliminate the automatic deletion processes that may be in place for SES to preserve e-mail messages, records and information that reside on active mail servers.
  - Ensure that older e-mail messages remain accessible as technology is upgraded or changed. Each time technology upgrades and changes take place information technology staff will ask agency administrators for information about the existence and location of older messages so they can be migrated to the new technology.
  - Provide Record management support to HRSA customers.
  - Provide the Records management branch with the assistance and resources to transfer permanent email to the National Archives.
  - **Heads of Office Components**
    - Ensure that all employees with e-mail accounts are aware of the e-mail policy and comply.
    - Meet with departing employees to determine all storage locations for e-mail messages and ensure that messages meeting the definition of a Federal record are captured prior to alerting the E-mail Team to delete the user's account.
    - Notify the appropriate OIT E-mail Team when the account(s) of former employees can be closed.
    - Provide Training and/or ensure that all staff is aware of the training resources that are available to them.
- d) RESPONSIBILITY FOR KEEPING E-MAIL
- When deciding who has responsibility for keeping the “official copy” of an email record, the following practices should be observed. Consider this a general rule, as there might be exceptions.



**Staff to staff (Internal):** Originator or sender is responsible for keeping email message. If recipient makes changes to the message (e.g., responds to, edits, add attachments, etc.), then the recipient is also responsible for keeping a record on the issue communicated. If the email provides documentation of a team project or collaborative effort that is copied to multiple addresses, the team must assign responsibility to a specific individual for filing the record. E-mail messages on a particular subject can become a string of replies until a matter is finalized. In such cases users shall either: (a) place all e-mails into the file folder separately as they occur and relate them to each other or (b) capture the final message – in which case user needs to make sure that the final message contains the whole thread of the discussion.



Staff to Person Outside of Agency: The originator or sender is responsible for keeping the record copy.

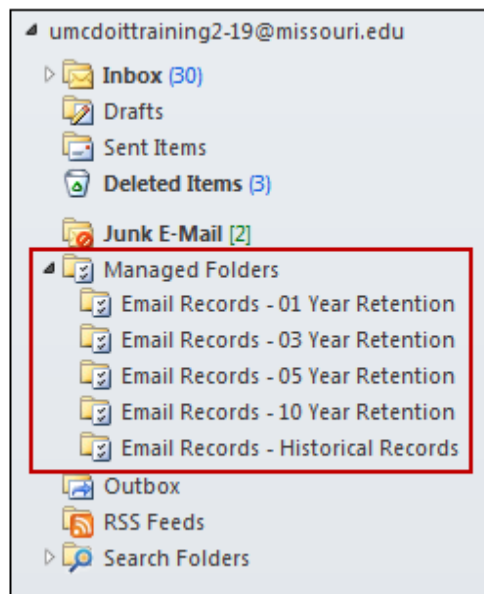


Email Received from Outside Agency (External): Email to recipient (i.e., HRSA user), is responsible for keeping the record. Email to several recipients: Often several offices, divisions, sections, etc. in an agency may receive an email message and not know who should handle the action. In these matters, the agency must establish who has recordkeeping responsibility so that the record is maintained officially by an office or person for its established retention period.

### e) MANAGING E-MAIL

- In addition to the Inbox and Sent Items boxes, automatically a part of the e-mail system, users are encouraged to organize e-mail by folders and subfolders. After brief periods in inboxes, messages should be transferred to titled folders or subfolders, specific to a record series. An example is provided below:

Figure 9 – Example of Email Folder Hierarchy



### f) RETENTION OF E-MAIL MESSAGES

The HRSA e-mail system will not automatically delete e-mails or that are 180 days old. This automatic deletion applies to e-mails within the Inbox folder, Sent folder, Draft folder, etc. Employees are encouraged to delete messages on a daily basis, immediately after reading, replying, or taking other action concerning a particular message. If, according to Federal mandated records retention schedules, the content of an e-mail

message possesses temporary or permanent retainable value, employees are required to print the message and place it in the appropriate paper file for further retention.

## g) BACKUPS

- All e-mail servers are backed up on a daily basis and are for disaster recovery purposes (i.e., total loss of the server). The backups will not be used for the recovery of lost e-mail. Retaining email is left to the individual user, who may print and download e-mail items.

## h) LITIGATION HOLDS

- When litigation is pending or threatened against HRSA or its employees, the Agency by law is required to preserve all data and information that pertain to the issues. Agency staff in receipt of a litigation hold directive are responsible for preserving electronically stored information (ESI), including all e-mail communications sent, received, stored or maintained in an Agency e-mail account, including data or information existing on a network shared drive, local computer, and portable storage devices. Employees may not alter or delete an e-mail that they have downloaded and saved, or moved to some other storage account or device, including copies in paper form.
- A litigation hold overrides the e-mail policy, as well as any records retention schedules that may have otherwise called for the transfer, disposal, or destruction of relevant documents, until the hold has been cleared by OGC.
- Accounts of separated employees that have been placed on legal hold status will be maintained by the departing individual's supervisor and OIT until the hold is released.

## i) MANAGING E-MAIL OF DEPARTING EMPLOYEES

- HRSA does not routinely review the content of an employee's e-mail account; however, these are files that reside on Agency computer systems, local drives and HRSA reserves the right to retain and access them as part of its responsibility for maintaining its technology infrastructure or when deemed necessary for business reasons. It is important, therefore, that when an individual leaves the Agency, the following procedures are followed to ensure that all necessary files are transferred from these individual spaces to the appropriate person in HRSA. The "appropriate person" will be identified by the departing individual's supervisor.
- The following procedures will outline the treatment of e-mail and other files stored on an individual's Agency-issued computer or assigned space on the HRSA network when an individual's employment with HRSA ceases.
- Voluntary Departure: A "voluntary termination" is characterized by mutual agreement between the employee and their supervisor or manager about the terms and timing of the departure, and by a willingness to work cooperatively to ensure a harmonious transition. In all good-will departure cases, the following procedures shall apply:
  - Upon notice of termination, an individual's supervisor shall work with the departing employee to arrange for the preservation of all business-related files both from the employee's network space, email box, and portable storage devices.



- Each employee is responsible for organizing and filing e-mail before departing the Agency.
- It is the responsibility of the manager to submit to OIT any requests to access e-mail or to transfer e-mail from the departing employee to a different individual in the office, even if this is on a temporary basis.
- It is the responsibility of the departing employee to delete all e-mail messages that are of a personal or transitory nature.
- The Human Resources Office will include an item on its “employee exit” checklist for the supervisor to indicate that the above steps have been completed.
- Business-related e-mail of the departing employee shall be reviewed and properly stored within a recordkeeping system six (6) months from the date of departure.
- Upon receipt of notice from the Human Resources Office, Records management, the e-mail account of departed employees will be disabled immediately.
- In terms of e-mail, the manager may choose to have a message put in place that goes to future senders of messages to the departed employee’s @HRSA.gov e-mail address indicating that the person is no longer in the employ of the Agency and indicating to whom messages should be sent if the message pertains to Agency business. This process would bounce the original message back to the sender along with the new HRSA contact information.
- Involuntary Departure: “Involuntary departure” usually involves little or no notice on the part of the employee and/or the supervisor/manager, under circumstances that warrant prudent measures to protect the business interests of the Agency. In all cases of involuntary departure, the following procedures shall apply:
  - It is the responsibility of the manager to inform the OIT in advance of any involuntary termination so that appropriate arrangements may be made to secure all files that reside in the employees e-mail account or on network space, and the timely disabling of the e-mail account of the person to be terminated.
  - If so desired, OIT will arrange to transfer all files and e-mail messages of the terminated employee to a portable storage device. It shall be retained by the supervisor and OIT.
- Supervisors or a designated individual will be responsible for evaluating the employee’s e-mail records for required retention and taking appropriate action to retain email as required. After 180 days post termination, remaining e-mail messages will be permanently deleted.

## GLOSSARY

**Alienation** – Losing care and custody. Not protecting from loss or access.

**Disposal** – The action taken regarding temporary records after their retention periods expire and consisting usually of destruction or occasionally of donation. Also, when specified, “disposal” refers to the actions taken regarding non-record materials when no longer needed, especially their destruction. (See NARA, “A Federal Records Management Glossary.”)

**Disposition** – The action taken with regard to records no longer needed for current Government business. The actions include transfer to agency storage facilities or Federal records center; transfer from one Federal agency to another; transfer of permanent records to the National Archives; and disposal of temporary records. “Disposition” is also the action taken regarding non-records materials when no longer needed, including screening and destruction.

**Electronic Records** – Any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record in 44 U.S.C. 3301. Electronic records include numeric, graphic and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record.

This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks. Unless otherwise noted, recordkeeping requirements apply to all electronic records systems, whether on microcomputers, minicomputers, or mainframe computers, regardless of storage media, in network or stand-alone configurations. (FIRMR Bulletin B-1).

**Electronic Records System** – An electronic system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use and disposition. The system must meet strict NARA standards for use as an Electronic Records System. Bureau’s and Offices must seek NARA approval for a system and should coordinate with the HRSA Records Management Officer to do so.

**File** - A collection of related documents or papers arranged so that they can be consulted easily.

**Files Plan** – A classification scheme describing different types of files maintained in an office, how they are identified, where they should be stored, how they should be indexed for retrieval, and a reference to the approved disposition for each file. A file plan lists of all files in a container (regardless of the media), office or organization.

**FISMA**- Federal Information Security Management Act.

**Freeze** - A "records freeze" is essentially a more specific implementation of the broader "hold" concept. A freeze refers to a set of standard procedures whereby the National Archives and Records Administration (NARA) Federal Records Centers (FRCs), upon receipt of notification from a Federal agency or the Department of Justice, temporarily suspend disposition actions of an agency's records and other documentary materials that are in the physical custody of FRCs, but for which legal custody resides with the originating agency.

**Hold** – For the purposes of this Policy, “hold” means the temporary suspension of HRSA records disposition actions for all records and documentary materials in the custody of HRSA, regardless of physical location and format.

**Information System** – Is defined by the Office of Management and Budget (OMB) in Circular No. A-130 as “a discrete set of information resources organized for the collection, processing, transmission and dissemination of information in accordance with defined procedures, whether automated or manual.”

**Life Cycle of a record** - The concept that records pass through: Creation, Maintenance and use, and disposition.

**Non-record Materials** – are extra copies of documents retained specifically for personal reference. They are those Federally-owned informational materials that do not meet the statutory definition of records (44 U.S.C. 3301), or that have been excluded from coverage by the definition. Excluded materials are extra copies of documents kept only for reference, stocks of publications and processed documents, and library or museum materials intended solely for reference or exhibit. (36 CFR 1220.14)

**OMB Exhibit 300** - Capital Asset Plan and Business Case Summary – As prescribed and described in OMB’s Circular A-11, Preparation, Submission and Execution of the Budget.

**OMB Circular A-130** - Management of Federal Information Resources – Establishes policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies. The policies in this Circular apply to the information activities of all agencies of the executive branch of the Federal government.

**Permanent Records** - Records appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time it is needed for administrative, legal, or fiscal purposes.

**Personal Papers** – Documentary materials belonging to an individual that are not used to conduct Agency business. This includes professional materials created by the official before entering Government service, files relating to previously held positions and reference files; private materials brought into the office that were not created or received in the course of transacting Government business, such as family and personal correspondence, drafts of articles and books, and community service records; and work related personal papers that are not used in the transaction of Government business or as documentary reference for legal issues such as diaries, notes, or personal appointment schedules. Also called personal files or personal records.

**Programmatic and Operational Records** – Operational records are records created and maintained throughout Federal agencies to conduct the day-to-day business of the Federal government. Programmatic records are records created and maintained in the course of unique programmatic activities of an agency.

**Records** – A unit of information generated or received by an entity on behalf of the organization, which acts as evidence and provides a history of activities. This 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, decision, procedures, operations or other activities of the Government, or because of the information value of the data in them. (44 U.S.C. 3301).

**Records Control Schedule** – A document providing mandatory instructions for what to do with records (and non-record materials) no longer needed for current Government business, with provision of authority for the final disposition of recurring or nonrecurring records. Includes the SF 115, agency records schedules for Agency specific program records, and the General Records Schedules (GRS) for common administrative records. Also called, records disposition schedule, records retention schedule, or schedule.

**Records Disposition** – is any activity with respect to:

- disposal of temporary records no longer needed for the conduct of business by destruction or donation to an eligible person or organization outside of Federal custody;
- transfer of records to Federal agency storage facilities or records centers;
- transfer to the national Archives of the United States of records determined to have sufficient historical or other value to warrant continued preservation; or
- transfer of records from one Federal agency to any other Federal agency. (44 U.S.C. 2901(5)).

**Records Inventory** - A "records inventory" is a detailed listing of the volume, scope, and complexity of an organization's records, usually compiled for the purpose of creating a records schedule (A Glossary for Archivists, Manuscript Curators, and Records Managers). The results of this survey can be used to analyze the records for various purposes including retention and protection.

**Records Management** – the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records 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(2)).

**Records Schedule** – Means:

- An SF 115, "Request for Records Disposition Authority," that has been approved by NARA to authorize the disposition of records;
- A General Records Schedule (GRS) issued by NARA; or
- A printed agency manual or directive containing the records descriptions and disposition instructions approved by NARA on one or more SF 115s or issued by NARA in the GRS. (36 CFR 1220.14).

**Records Series** – file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access and use.

**Reference Material** – materials maintained solely for convenience of reference. These may include extra copies of items created by the Agency, documents received from other agencies, copies of published books or articles, and other documentation used by staff for reference.

Material shall be clearly marked and maintained separately from the records of the office.

**Reviewing Official** – either the employee’s manager of record; a Records Management Officer; or, a Freedom of Information Act (FOIA) Officer.

**Scheduling** – the process of developing schedules for the disposition of records, along with disposition instructions for nonrecord materials.

**Sensitive Data** – Sensitive data are data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

**Temporary Records** - Records approved by NARA for disposal after a specified retention period.

**Vital Records** – There are two types of vital records:

- Emergency Operating Records – Documents needed immediately, such as orders of succession.
- Legal and Financial Rights Records – Documents essential to protect the legal and financial rights of the Government and of the individuals directly affected by its activities, such as social security records.

## REFERENCES

- a. HRA Appendix B-341, Records Management Manual, (11/28/83) (hereby cancelled)
- b. HSA Appendix B-351, Records Management Manual, (10/31/83) (hereby cancelled)
- c. HRSA Records Management Program – Record Schedule,” (YYYY/MM/DD)
- d. OFFICE OF MANAGEMENT AND BUDGET, Managing Government Records Directive M-12-18 August 24, 2012
- e. Presidential Memorandum – Managing Government Records, November 28, 2011,
- f. Title 44, United States Code 44 USC 3301 - Sec. 3301. 44 USC 3302 - Sec. 3302., 44 USC 3303 - Sec. 3303. TITLE 41--Public Contracts and Property Management SUBCHAPTER G-- ADMINISTRATIVE PROGRAMS
- g. PART 102-193--CREATION, MAINTENANCE, AND USE OF RECORDS, §102-193.5, §102-193.10, §102-193.15, §102-193.20, §102-193.25
- h. OFFICE OF MANAGEMENT AND BUDGET, Policies for Federal Agency Public Websites M-05-04, December 17, 2004
- i. Chapter XII, subchapter B of Title 36, Code of Federal Regulations, 1220.1 to 1238.32
- j. Title 5, United States Code (section 552 is also known as “The Freedom of Information Act,” section 552a is also known as “The Privacy Act of 1974,” and Appendix 2 is also known as “The Federal Advisory Committee Act of 1972”)
- k. Title 41, Code of Federal Regulations
- l. HRSA “HHS Privacy Program,” May 8, 2007, as amended
- m. HHS Records management Program May 8, 2007, as amended
- n. DoD 5015.02-STD, “Electronic Records Management Software Applications Design Criteria Standard,” April 25, 2007
- o. Federal Records Act of 1950, as amended (44 U.S.C. Chapter 21, Chapter 29, Chapter 31, Chapter 33).
- p. National Archive and Records Administration Act of 1984 (Public Law 98-497, 44 U.S.C. Chapter 21).
- q. Concealment, Removal, or Mutilation of Records (18 U.S.C. 2071)
- r. 36 CFR Chapter XII, Subchapter B especially Part 1234, “Electronic Records Management.”
- s. 36 CFR Chapter XII, Subchapter G, “Damage to, Alienation and Unauthorized Destruction of Records”.
- t. HHS OCIO-2007-0004 “HHH Policy for Records Management”, dated January 30, 2008.
- u. 44 U.S.C. Chapter 31 – Records Management by Federal Agencies
- v. 44 U.S.C. Chapter 33 – Disposal of Records
- w. 5 U.S.C. Section 552 – Freedom of Information Act (FOIA)

- x. Federal Rules of Civil Procedure (FRCP) – Govern civil procedure in the United States district courts, or more simply, court procedures for civil suits. The FRCP are promulgated by the United States Supreme Court pursuant to the Rules Enabling Act (28 U.S.C. §§ 2071 – 2077), and then approved by the United States Congress. Relevant rules from the FRCP include the following.
- y. FRCP, Title III, Pleadings and Motions, Rule 16, Pre-Trial Conferences; Scheduling; Management
- z. FRCP, Chapter V, Depositions and Discovery, Rule 26(a), Duty to Disclose, General Provisions Governing Discovery; Required Disclosures

**Office of Information Technology  
Policy For  
Electronic Mail (Email) Records Management**

December 14, 2017

U.S. Department of Health and Human Services (HHS)

Health Resources and Services Administration (HRSA)

Office of Information Technology (OIT)





**Version History**

<b>Version Number</b>	<b>Revision Date</b>	<b>Description of Change</b>	<b>Changed by</b>	<b>Approved By</b>
0.0	7/24/2017	Update HRSA OIT Email Policy to incorporate Capstone Approach and usages of electronic messaging mobile applications tools and services.	Evelyn Reid	Valerie Wampler
1.0	10/11/2017	Updates, corrections, etc.	Judy Wight	

**Table of Contents**

1. Nature of Changes ..... 1

2. Purpose ..... 1

3. Background/Significant Changes ..... 1

4. Scope ..... 2

5. Ownership of Email..... 2

6. Policy for Electronic Mail (Email) Records Management ..... 3

7. Retention Practices ..... 11

8. Litigation Holds ..... 13

9. Systems Requirements..... 14

10. Access Requirements..... 14

11. Disposition Requirements ..... 14

12. Managing Social Media and Electronic Messages Records: ..... 15

13. Roles and Responsibilities..... 16

14. Applicable Laws/Guidance..... 19

15. Additional Information and Assistance ..... 20

16. Effective Date/Implementation..... 20

Approvals..... 21

Appendix A: Key Terms ..... 22

Appendix B: Glossary ..... 23

**1. Nature of Changes**

This policy supersedes and replaces Health Resource and Services Administration (HRSA) Records Management Email Retention Policy, dated February 19, 2015.

**2. Purpose**

2.1. The purpose of this policy is to provide guidelines for managing electronic mail (email) and “electronic messages” related to social media and mobile messaging applications (i.e. Short Message Service (SMS)/text messaging, Skype chat, twitter, etc.) as well as techniques for retaining and preserving transmissions.

2.2. In addition, this policy implements the General Records Schedule (GRS) 6.1, Email Managed under a Capstone Approach and identifies its authorities, scope and objectives.

**3. Background/Significant Changes**

3.1. Email is a tool for exchanging messages and documents using telecommunications equipment and computers. There is not a specific category within the HRSA-specific Records Schedule for managing email. However, an email message may contain content that makes it an official Federal record subject to established National Archives and Records Administration (NARA) and HRSA retention and disposition policies.

3.2. Email communications are considered Federal records when the message meets the definition described in the Federal Records Act (FRA). Information sent via email may be considered an official agency record if it serves as evidence of an office’s activities, events, or business transactions. Email, including attachments, and instant messages, chats, twitters, etc. must be identified, managed, protected, and retained as long as needed for continuing operations, audits, legal proceedings, etc.

3.3. This policy implements Office of Management and Budget Managing Government Records Directive (OMB M-12-18). HRSA will manage all email records in an appropriate electronic recordkeeping system that supports records management and litigation requirements (which may include preservation-in-place models), including the capability to identify, retrieve, and retain the records for as long as they are required.

3.4. This policy also addresses recordkeeping requirements when using personal or non-HRSA communication tools to conduct HRSA business.

- 3.5. HRSA employees are responsible for the creation or receipt, maintenance, use and disposition of Federal records. Users are required to use the retention policy in the email system to manage email messages that are official records and remove email records that are non-records.

#### **4. Scope**

- 4.1. This policy applies to all users who have access to the HRSA network, usage of HRSA-owned mobile devices, applications and services. Because email is potentially a Federal record, all government employees, appointees, contractors, and others working on behalf of HRSA must appropriately preserve messages sent and received.
- 4.2. The Capstone policy applies to all HRSA Bureaus and Offices (B/Os) Senior Officials, and contractors conducting business for, and on behalf of the Agency through contractual relationships and service level agreements. National Archives and Records Administration (NARA) has an approved NA-1005 (on file) and HRSA will adhere and comply with the NARA GRS 6.1, Email Managed under a Capstone Approach disposition authority. HHS supplemental preservation requirements that apply to HRSA records and other documentary materials that are potentially relevant for litigation, investigations and audit matters may be found in the HHS Policy for Records Holds and HRSA Records Management Policies and Procedures Manual.
- 4.3. This policy does not supersede any other applicable law, court order, existing labor management agreement, and more stringent retention standard or agency directives.
- 4.4. NOTE: Currently, Capstone applies only to email records, as defined in this policy. All other records, including paper, electronic, or other media are governed by the GRS or the HRSA-specific records schedule.

#### **5. Ownership of Email**

- 5.1. The definition of “Electronic message” means a self-contained piece of digital communication that is designed or intended to be transmitted between physical devices. An electronic message includes, but is not limited to, email, a text message, an instant message, skype, social media, voice mail, etc.
- 5.2. Email transmissions declared as Federal records are Government property and may not be disposed of except in accordance with approved records schedules. In accordance with HHS policy effective December 29, 2016, the email of all

Capstone Officials listed on an approved NARA Form 1005 (NA 1005) will be treated as permanent records and retained indefinitely.

## **6. Policy for Electronic Mail (Email) Records Management**

### **6.1. Electronic Mail (Email):**

6.1.1. HRSA employees routinely create, send, and receive electronic mail (email, instant messages, mobile applications, etc.) to communicate information related to the operation or administration of the agency. Email containing content that is evidence of the functions, policies, decisions, procedures, operations, or other activities of HRSA Bureaus and Offices are records and must be maintained based on recordkeeping requirements for retention and disposition.

6.1.2. Email often meets the definition of a Federal record as provided in the Federal Records Act (44 U.S.C., 3301) that includes: all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

### **6.2. Categories of Electronic Mail (Email) Retention:**

6.2.1. Records in the form of email messages made or received in connection with the transaction of HRSA business may be transitory, temporary, or permanent. The records are kept for business, financial, legal or historical reasons, based on the content, originator, and function of the email message, which determines the retention period for that message.

6.2.2. Transitory, casual, and routine communications should not be retained due to their limited value. Most emails are transitory and should be deleted in six (6) months, however, longer retention is authorized if required for business use. The following types of email can be deleted because they are transitory:

- (a) Personal emails unrelated to HRSA business.
- (b) Incoming listserv messages.
- (c) Spam or unsolicited advertisements must be sent to the junk email.
- (d) Scheduled meetings, invitations and responses to meetings.
- (e) Announcements, acknowledgments, and thank-you.

- (f) Circulating copies of agency instructions, circulars, internal newsletters, other than master copies provided as a courtesy.
- (g) Out of Office automatic replies.
- (h) Attachments to email that are identical to records that are stored and managed outside the email system pursuant to a NARA-approved records schedule.
- (i) Agency wide electronic broadcasts, alerts, news, and newsletters.

6.2.3. Temporary records have documentary value, but will eventually be deleted/destroyed. These records will be maintained in accordance with the HRSA approved records schedule (available on the [OIT Records Management Site](#)) or the NARA [General Records Schedule](#). Examples are:

- (a) Email documenting answers to audit questions must be retained for 10 years.
- (b) Email communications discussing employee awards must be retained for 2 years.
- (c) Email discussing administration of a personnel security program must be retained for 2 years.
- (d) Email discussing the installation and testing of individual information technology projects must be must be retained for 3 years.
- (e) Email transferred to the electronic handbooks (EHBs) system through the plug in can be destroyed after 180 days, since this system preserves the official HRSA records.

6.2.4. Permanent records are retainable and have significant administrative, legal, and/or fiscal value. Examples are:

- (a) Correspondence providing key substantive comments on a draft memorandum, if the email adds to a proper understanding of the formulation or execution of Agency action.
- (b) Messages documenting oral exchanges, such as meetings or telephone conversations, during which policy was discussed

or formulated or other agency activities were planned, discussed and not otherwise documented in Agency files.

- (c) Messages that convey information of value on important Agency activities, if the email message adds to a proper understanding of Agency operations and responsibilities.
- (d) Email, calendars, and instant messages regarding SES officials conducting Agency business.

6.2.5. Implementation of the "Capstone" approach - Under the Capstone approach, HRSA manages email records based on the role of the account holder rather than on the content of each email record. Capstone officials include all those positions listed on the NARA Form 1005 "Verification for Implementing GRS 6.1" approved by NARA on May 4, 2017. This includes those officials in an acting capacity for any of the positions listed on the NA 1005 longer than 60 days. The form serves as a list of permanent officials included and excluded from HRSA's Capstone implementation.

- (a) Email records captured and managed under the Capstone approach must use an existing records retention schedule or be maintained as unscheduled records until the re-approval of the NARA Form NA 1005. For example, if there is a major re-organization or changes within the structure, HRSA will not implement GRS 6.1 until NARA reviews and approves the HRSA re-submission of NARA Form 1005.
- (b) The verification process will require HRSA to develop an updated NA-1005 and the HRSA Agency Records Officer (ARO) will coordinate with NARA to gain their approval prior to implementing any items on the updated GRS.
- (c) The verification process for identifying Capstone officials is located in the record description of GRS 6.1. The definition of Capstone (permanent) accounts in item 010 of the GRS defines the ten categories of senior officials and acknowledges that different divisions often have different titles for similar positions. This approach is meant to assist HRSA in properly identifying senior officials within their Bureaus and Offices that correlate to each category.

6.2.6. Email records are captured and managed according to user role using the following retention approach:

- (a) Email Records of Designated Capstone Officials - Email records (e.g., email messages and attachments, calendar appointments, and tasks captured by the electronic recordkeeping system) from designated Capstone official's email accounts are retained as permanent. These email records will be transferred to NARA according to General Record Schedule 6.1, Section 010. The HRSA Agency Records Officer maintains the official list of Capstone officials' email accounts and will forward a copy of the list to the Bureau/Office Records Liaisons annually.
- (b) Email Records Captured from Email Accounts Not Designated as Capstone Officials - Email records (e.g., email messages and attachments, appointments, and tasks captured by the HRSA electronic recordkeeping system) of all other account holders are retained as temporary according to General Record Schedule 6.1, Sections 011 or 012 and destroyed within the electronic recordkeeping system (NOTE: Precluding records under preservation obligation, such as a litigation hold). If HRSA decides not to use NARA GRS 6.1, than a records disposition schedule must be created and submitted to NARA for approval.
- (c) Each email user (i.e., creator or recipient) shall take responsibility for identifying whether an email communication fits the definition of a Federal record. If deemed to be evidence of one's activities, the email user shall retain, preserve, and dispose of messages in accordance with the HRSA records schedule.

6.2.7. Non-Record Emails. HRSA employees may delete "non-record" emails that do not contain information documenting HRSA actions or activities. Non-records include items such as non-business related, personal, broadcast messages (e.g., HHS messages to all staff) and advertisements (NOTE: Precluding records under preservation obligation, such as a litigation hold).

6.2.8. Transitory Email Records. Transitory records are records of short-term (180 days or less) interest which have minimal or no documentary or evidential value. Email records that are transitory may be deleted when

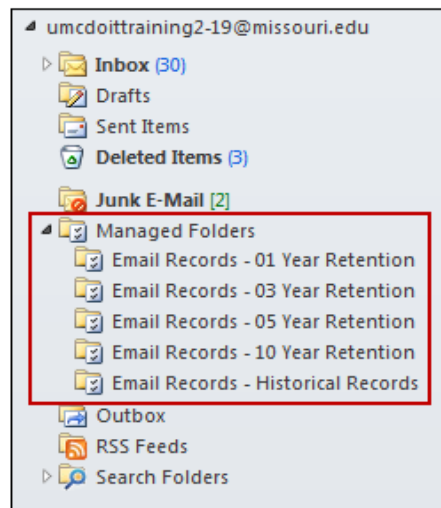


no longer needed (NOTE: Precluding records under preservation obligation, such as a litigation hold).

6.2.9. Email Containing PII. Certain information containing sensitive or restricted (e.g. Personally Identifiable Information) data shall not be stored, transmitted, or processed using email infrastructure unless appropriate information security mechanisms (e.g., message encryption) are used.

6.2.10. Managing Email Records Manually. When automated tools or features are not available within the email system to auto-categorize folders and emails, employees must manually create folders within their email inbox and manage records by record type. (NOTE: For best retention and disposition practices, a folder should be created for each record type the employee creates. Additionally, sub-folders may be created to manage records into more specific categories).

- (a) In addition to the Inbox and Sent Items boxes (which are automatically a part of the email system), users are encouraged to organize email by folders and subfolders. After brief periods in the Inbox, messages should be transferred to titled folders or subfolders, specific to a record series. An example is provided below:



6.2.11. Email Retained with Related Records. When business needs require email records be retained within another electronic recordkeeping system (such as part of a case file), a copy of the email should be kept with those files. Capstone does not replace existing business practices

that require email messages and other related records to be retained together in established electronic recordkeeping systems.

- 6.2.12. Search and Auditing of System. System-wide email searches may be conducted by designated OIT Security personnel with the approval of the General Counsel or Chief Information Officer (CIO) as part of an internal or external investigation or in response to an access request as needed.
- 6.2.13. Unauthorized Destruction of Email Records and Reporting Loss. If there is an instance of unauthorized destruction of email records, the user should first contact their supervisor and then the IT Helpdesk to attempt recovery. If recovery is not possible, the user or office must report the incident to the HRSA ARO. The ARO will subsequently report the incident to the HRSA Chief Information Officer (CIO). Per 36 CFR 1230.14, the report should describe the records, the circumstances in which the unauthorized destruction took place and the corrective steps being taken to properly manage the records in the future.

### 6.3. Email of Departed Employees and Contractors.

- 6.3.1. The email account of a separating employee will be disabled by HRSA OIT. The account will not be purged until notice is received from the departing employee's manager/supervisor and Executive Officer or according to the HRSA Life Cycle and Password Policy.
- 6.3.2. Accounts of separated employees that have been placed on legal hold status will be maintained by the departing individual's supervisor and OIT until the hold is released.
- 6.3.3. HRSA does not routinely review the content of an employee's email account; however, these are files that reside on Agency networks, and HRSA reserves the right to retain and access them as part of its responsibility for maintaining its technology infrastructure or when deemed necessary for business reasons. It is important, therefore, that when an individual leaves HRSA, proper procedures are followed to ensure that all necessary files are transferred from these individual spaces to the appropriate person in HRSA. The "appropriate person" will be identified by the departing individual's supervisor.
- 6.3.4. The following procedures outline the treatment of email and other files stored on an individual's HRSA-issued computer or assigned space on

the HRSA network when an individual's employment with HRSA ceases.

(a) Voluntary Termination: A "voluntary termination" is characterized by mutual agreement between the employee and their supervisor or manager about the terms and timing of the departure, and by a willingness to work cooperatively to ensure a harmonious transition. In all good-will departure cases, the following procedures shall apply:

- Upon notice of termination, an individual's supervisor shall work with the departing employee to arrange for the preservation of all business-related files both from the employee's network space, email box, and portable storage devices.
- Each employee is responsible for organizing and filing email before departing the Agency.
- It is the responsibility of the manager to submit to HRSA OIT any requests to access e-mail or to transfer email from the departing employee to a different individual in the office, even if this is on a temporary basis.
- It is the responsibility of the departing employee to delete all email messages that are of a personal or transitory nature.
- The Human Resources Office will include an item on its "employee exit" checklist for the supervisor to indicate that the above steps have been completed.
- Business-related email of the departing employee shall be reviewed by the supervisor and properly stored within a recordkeeping system until the retention period has been met.
- Upon receipt of notice of the email account of departed employees from the Executive Officer, HRSA OIT will disable accounts.
- The manager may choose to have a message put in place that goes to future senders of messages to the departed employee's @HRSA.gov email address indicating that the person is no longer in the employ of the Agency and indicating to whom messages should be sent if the message pertains to Agency business. This process would bounce the original message back to the sender along with the new HRSA contact information.

(b) Involuntary Departure An “Involuntary departure” usually involves little or no notice on the part of the employee and/or the supervisor/manager, under circumstances that warrant measures to protect the business interests of the Agency. In all cases of involuntary departure, the following procedures apply:

- It is the responsibility of the manager to inform the Office of Information Technology of any involuntary termination as soon as possible so that appropriate arrangements may be made to secure all files that reside in the employee’s email account or on network space, and the timely disabling of the email account of the person to be terminated.
- If so desired, OIT will arrange to transfer all files and email messages of the terminated employee to a portable storage device. It shall be retained by the supervisor and HRSA OIT.
- Supervisors or a designated individual will be responsible for evaluating the employee’s email records for required retention and taking appropriate action to retain email as required. After 180 days post termination, remaining email messages will be permanently deleted.

#### 6.4. Conducting Agency Business via Unauthorized External Information Systems

Transmission of HRSA "sensitive" information via personal email is prohibited. In the interest of both protecting the HRSA employee’s personal privacy and increasing transparency for the public, HRSA employees assigned a HRSA-provided computer and/or email, or online storage account must use those government provided resources for conducting any and all official business. Under no circumstances should HRSA employees conduct official business using a personal computer, email or personal online storage accounts while conducting HRSA business.

#### 6.5. Email Records Management (Capstone) Training

The HRSA Agency Records Officer is responsible for ensuring that appropriate staff in HRSA’s Bureaus and Offices receive email records management (Capstone) training to ensure they are aware of their responsibilities to maintain and safeguard agency email records, including the obligations under this Policy and the HHS Records Holds Policy.

#### 6.6. New Employees Orientation

HRSA employees whose positions have been designated as Capstone (permanent) will receive an initial and departure briefing as part of their training on their email records management responsibilities.

#### 6.7. Annual Training

HRSA personnel must complete Records Management training annually, which must include a section on email records management (Capstone Approach).

### 7. Retention Practices

7.1. Certain information containing sensitive or restricted (e.g., Personally Identifiable Information) data shall not be stored, transmitted or processed using email infrastructure unless appropriate information security mechanisms (e.g., message encryption) are used.

7.2. Email messages that qualify as a Federal record shall be kept with any attachment(s). The email shall contain the following header information:

- (a) Who sent the message (first and last name of sender in the "From" line)
- (b) To whom the message was sent (first and last name of all recipients in the "To" line as well as all recipients copied on the email in the "CC" line)
- (c) The date and time that the message was sent.
- (d) The subject of the message.
- (e) Email system receipt data that captures date and time, acknowledgement, and access/readable receipts will not be retained beyond six (6) months.

7.3. Users email calendars and task lists that meet the definition of a Federal record will be identified and preserved according to the appropriate records control schedule.

7.4. Transmitted email messages that are sent requiring an acknowledgement of receipt or an acknowledgment that an addressee opened the message are considered Federal records and must be preserved. Preserve the

acknowledgement with the record copy if returned. Preservation of receipts is part of the “sender’s” record copy.

7.5. When required for recordkeeping purposes, print documentation containing information about the receipt of the message and attach it to the message. (If the sender requested a receipt for recordkeeping purposes in accordance with agency criteria, he or she will retain the printed message and transmission document until receipt is received.)

7.6. When deciding who has responsibility for keeping the “official copy” of an email record, the following practices in Table 1 “Responsibility for Keeping Email” should be observed. Consider this a general rule, as there might be exceptions.

Email Origin		Responsibility
Staff to Staff	Internal	<ul style="list-style-type: none"> <li>• Originator (sender) is responsible for keeping email message.</li> <li>• If a recipient makes changes to the message (e.g., responds to, edits, adds attachments, etc.), then the recipient is also responsible for keeping a record on the issue communicated.</li> <li>• If the email provides documentation of a team project or a collaborative effort that is copied to multiple addresses, the team must assign responsibility to a specific individual for filing the record.</li> <li>• Email messages on a particular subject can become a string of replies until a matter is finalized. In such cases users shall either:               <ul style="list-style-type: none"> <li>• Place all emails into the file folder separately as they occur and relate them to each other or</li> <li>• Capture the final message – in which case; the user needs to make sure that the final message contains the whole thread of the discussion.</li> </ul> </li> </ul>

Email Origin		Responsibility
Staff to Person Outside of Agency	Internal	The creator or recipient of the email can both be responsible for keeping the Federal record, depending on the business use and/or action taken.
Email Received From Outside Agency	External	<ul style="list-style-type: none"> <li>• Email to the recipient (i.e., HRSA user) is responsible for keeping the record.</li> <li>• Email to several recipients. Often several offices, divisions, sections, etc. in an agency may receive an email message and not know who should handle the action to be dealt with in the email. In these matters, the recipient of the email must establish who has record keeping responsibility so that the record is maintained officially by an office or person for its established retention period. If the office or person is not identified and is unaware of their responsibility, the agency may find that no one retains the email or that every recipient retains the message. Neither of these scenarios is acceptable.</li> </ul>

**TABLE 1 RESPONSIBILITY FOR KEEPING EMAIL**

**8. Litigation Holds**

8.1. When litigation is pending or threatened against HRSA or its employees, the Agency by law is required to preserve all data and information that pertain to the issues. Agency staff in receipt of a litigation hold directive are responsible for preserving electronically stored information (ESI), including all email communications sent, received, stored or maintained in an Agency email account, including data or information existing on a network shared drive, local computer, and portable storage devices. Employees may not alter or delete an email that they have downloaded and saved, or moved to some other storage account or device, including copies in paper form.

8.2. A litigation hold overrides the email policy, as well as any records retention schedules that may have otherwise called for the transfer, disposal, or destruction of relevant documents until the hold has been cleared by Office of General Council (OGC).

- 8.3. Accounts of separated employees that have been placed on legal hold status will be maintained by the departing individual's supervisor and HRSA OIT until the hold is released.

## **9. Systems Requirements**

The National Institutes of Health (NIH) is the HRSA email service provider, and we abide by their standard policies.

## **10. Access Requirements**

### **10.1. Retrievable**

Access supports an agency's ability to carry out its business functions. Access must address internal agency needs and accommodate responses to requests for information. As such, email records must remain usable and retrievable throughout their life cycle. All employees shall manage Federal records created in or transmitted using the HRSA email system in a manner that allows each to be accessible and readable for the specific record retention period.

### **10.2. Preservable**

Email records must be maintained in a system that 1) preserves their content, context, and structure, 2) protects against their unauthorized loss or destruction, and 3) ensures that they remain discoverable, retrievable, and usable for the period of its life cycle. NIH is the HRSA's email provider, and we abide by their standard policies.

### **10.3. Searchable**

Employees do not have privacy in anything they create, send, receive or store on the HRSA email system. This includes Instant Messaging. Messages stored in the Office 365 (Outlook), Personal Storage Table (.pst) files residing on a shared network drive or local drive, and messages saved to portable storage devices (e.g., DVD, flash or USB drive) are subject to search for purposes of responding to disclosure requests (e.g., FOIA, litigation holds, etc.). All messages sent to or received using Government systems are subject to search.

## **11. Disposition Requirements**

### **11.1. Schedule**



HRSA has a NARA-approved agency-specific schedule in place to carry out the disposition of permanent and temporary records, approved in September 2016.

11.2. Retention Period

HRSA has identified appropriate retention periods for email records and implemented systems and policies to support the disposition as specified in the approved GRS 6.1 records schedule.

11.3. Manual Deletions

Employees are encouraged to delete non-records messages on a daily basis, immediately after reading, replying, or taking other action concerning a particular message.

**12. Managing Social Media and Electronic Messages Records:**

12.1. There are two types of applications related to this topic:

12.1.1. Web-based – Social media allows individuals to collaborate, create, organize, edit, comment on, combine and share content, which may result in the creation of Federal records. Social Media refers to the various activities integrating web technology, social interaction and user-generated content. Social media tools include Instagram, twitter, blogs, social network, photo libraries, virtual worlds, location-based service, and video sharing sites.

- (a) HRSA uses social media externally to share information, support business processes, and connect to other Federal agencies. The Federal Records Act (44 U.S.C. 3301) defines Federal records as any material that is recorded, made or received in the course of Federal business, regardless of its form or characteristics and is worthy of preservation.
- (b) Social media content that meets this definition must be managed and retained per the Federal Records Act and NARA and HRSA records schedules. HRSA does not currently have an approved records schedule for social media, and as such, all content must be retained until an associated agency records schedule is created and approved by NARA.

12.1.2. Mobile Devices and Applications – HRSA employees work in mobile environments and utilize electronic messages to conduct agency

business daily. All government employees, appointees, contractors, and other working on behalf of HRSA must comply with the Mobile Devices Office of Information Technology policy.

- (a) HRSA mobile solutions offer several ways for employees to create, maintain and dispose of Federal records and information, and this is the risk to HRSA. Unlike official email or organizational email, a user is not required to authenticate their identity to send or receive text messages or instant messages. Without authentication, there is repudiation; which means a user can deny that they are creator or receiver of the text message or instant message.
- (b) Only with non-repudiation, such as a digital signature attached to an email or an electronic documentation can be used as an official record. All other forms of electronic message content must be retained until a records schedule is created and approved by NARA. HRSA Records Management policy prohibits the use of text messages and instant messenger as official records.

### **13. Roles and Responsibilities**

#### **13.1. HRSA Agency Records Officer:**

- 13.1.1. Collaborates with stakeholders, evaluates and assigns positions as Capstone or Non-Capstone and forwards to the HHS Department RO.
- 13.1.2. Ensures that Capstone designations are kept current with organization changes.
- 13.1.3. Provides training to HRSA staff on Capstone records management implementation.
- 13.1.4. Ensures NARA-approved schedules are in place that identify systems that contain Federal email records.
- 13.1.5. Transfers permanent email records to the NARA in accordance with approved records schedules and applicable laws, regulations, and NARA Transfer Guidance.

#### **13.2. HRSA Records Liaison Officers**

Monitor personnel changes within their offices and inform the Agency Record Officer of changes relevant to Capstone status designations.

13.3. HRSA Chief Information Officer

13.3.1. Ensures email systems retain components of email messages identified in RFC 5322 including email attachments.

13.3.2. Ensures current and departed employees email records remain accessible throughout the record's life cycle as determined by the records schedule or legal hold, whichever is longer.

13.3.3. Ensures searches across multiple email accounts or multiple systems are available to find emails needed for agency business.

13.3.4. Prevents unauthorized access, modification, or destruction of email records.

13.4. Office of Information Technology (OIT)

13.4.1. Establish and publish standards for email account administration and storage allocations.

13.4.2. Ensure that staff is trained and informed about the use of email in the workplace.

13.4.3. Provide helpdesk support.

13.4.4. Ensure that older email messages remain accessible as technology is upgraded or changed. Each time technology upgrades and changes take place information technology staff will ask agency administrators for information about the existence and location of older messages so they can be migrated to the new technology.

13.4.5. Provide Records Management support to HRSA customers.

13.4.6. Provide the Records Management branch with the assistance and resources to transfer permanent email to the National Archives.

13.5. Heads of HRSA Bureaus/Offices

13.5.1. Ensure that all employees with email accounts are aware of the email policy and comply.

13.5.2. Meet with departing employees to determine all storage locations for email messages and ensure that messages meeting the definition of a

Federal records are captured prior to alerting OIT to delete the user's account.

13.5.3. Notify the appropriate OIT Email Team when the account(s) of former employees can be closed, per the HRSA Account Life Cycle and Password Policy.

13.5.4. Provide Training and/or ensure that all staff is aware of the training resources that are available to them.

13.6. HRSA Personnel (Employees, Contractors, Interns, and Fellows):

13.6.1. Attend basic records management training annually and training on how to use the email system.

13.6.2. Recognize the difference between a record and non-record material and maintain email records accordingly, to the extent practicable.

13.6.3. Use the HRSA email system for all business purposes. This policy applies to all user accounts that the employee uses or monitors.

13.6.4. Notify the Agency Records Officer if you receive a large number of permanent records to determine whether your account should be re-designated as Capstone permanent.

13.6.5. Comply with the requirements of this policy including requirements related to email preservation.

13.6.6. All HRSA account holders are responsible for recognizing that the information they create while conducting HRSA business is considered Federal records. Additional information about records management responsibilities may be found in the HRSA and HHS Records Management Policies.

13.6.7. Users shall open their email on a regular basis (daily, if possible), delete non-records items, classify, and file items needed for future reference appropriately so as not to fill up their incoming mail file (Inbox).

13.7. Classify email messages to determine which records series defines how long the message should be kept.

13.8. Organize their email messages so they can be located and used.

13.9. Not retain messages longer than required. When the need no longer exists, the message should be deleted.

13.10. Protect records from loss, damage, improper destruction, and unauthorized disclosure.

13.11. Preserve all email content that falls within the scope of a litigation hold regardless of where the data resides. This includes, but is not limited to content stored in email inboxes, portable devices, and on network drives

#### **14. Applicable Laws/Guidance**

14.1. Authorities include:

- (a) 36 CFR Chapter XII, Subchapter B - Agency Records Management Responsibilities
- (b) 36 CFR Chapter XII, Subchapter C - Electronic Records Management
- (c) 44 U.S.C. Chapter 21 - National Archives and Records Administration
- (d) 44 U.S.C. Chapter 29 - Records Management by the Archivist of the United States
- (e) 44 U.S.C. Chapter 31 - Records Management by Federal Agencies
- (f) 44 U.S.C. Chapter 33 - Disposal of Records
- (g) 44 U.S.C. 3301 - Definition of Records
- (h) OMB M-12-18, Managing Government Records Directive
- (i) General Record Schedule 6.1: Email Managed under a Capstone Approach  
<http://www.archives.gov/records-mgmt/grs/grs06-1.pdf>
- (j) HRSA Records Management Policies and Procedures Manual

**15. Additional Information and Assistance**

15.1. The HRSA OIT Chief Information Officer is responsible for development and management of the Health Resources and Services Administration Policy for Electronic Mail (Email) records Management.

15.2. For additional information about this Policy, please contact the HRSA Agency Record Officer, Evelyn Reid at (301) 443-1476 or email [ereid@hrsa.gov](mailto:ereid@hrsa.gov); or Judy Wight at (301) 945-3989, [jwight@hrsa.gov](mailto:jwight@hrsa.gov)

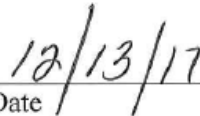
**16. Effective Date/Implementation**

The effective date of this policy is the date the policy is approved.

**Approvals**

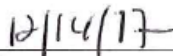
HRSA Agency Records Officer  
Evelyn Reid

  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Date

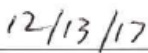
HRSA Office Chief Information Officer  
Adriane Burton

  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Date

HRSA Deputy Chief Information Officer  
Valerie Wampler

  
\_\_\_\_\_  
Signature

  
\_\_\_\_\_  
Date

### Appendix A: Key Terms

The following table provides definitions and explanations for terms and acronyms relevant to the content presented within this document.

Term	Definition
C.F.R.	Code of Federal Regulations
Email	Electronic mail
HRSA	Health Resources & Services Administration
OIT	Office of Information Technology
NARA	National Archives and Records Administration
OMB	Office of Management and Budget
U.S.C.	United States Code
CIO	Chief Information Officer
ARO	Agency Records Officer
RL	Records Liaison



## Appendix B: Glossary

**Capstone** - An approach to managing email where agencies must identify those email accounts most likely to contain records that should be preserved as permanent. Agencies will determine Capstone accounts based on their business needs. They should identify the accounts of individuals who, by virtue of their work, office, or position, are likely to create or receive permanently valuable Federal records. Capstone officials will generally be the top-level senior officials of an agency, but may also be other key decision makers at lower levels of the agency.

**Capstone Official** - Senior officials designated by account level or by email or by email addresses, whether the addresses are based on an individual's name, title, a group, or a specific program function.

**Control and Custody of Records** - HHS records/materials are the property of the Federal government, not the property of individual employees or contractors acting as an agent for the government, and may not be removed from the Agency without proper authority. All employees /contractors shall maintain records and non-record documentary materials separately from one another.

**Culling** - The act of removing or deleting material prior to disposition. This may include deleting non-record email [e.g., email blast (such as agency-wide communications), spam, and personal email (records belonging to an individual and not related to agency business)], and transitory email records (records of short-term interest or that have minimal documentary or evidentiary value).

**Electronic Mail (Email)** - All traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

**Email User** - An employee, contractor, volunteer, intern, fellow, or any other person who used HRSA email system.

**Electronic Messages** - Electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals.

**Electronic Mail (Email) System** - A computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or databases on either personal computers or mainframe computers, and word processing documents not transmitted on an email system. (36 CFR 1236.2)

**Electronic Records** - Any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record in 44 U.S.C. 330I. Electronic records

include numeric, graphic and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record.

This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks. Unless otherwise noted, these requirements apply to all electronic records systems, whether on microcomputers, minicomputers, or mainframe computers, regardless of storage media, in the network or stand-alone configurations.

**Electronic Records Keeping System** - An electronic system in which records are collected, organized and categorized to facilitate their preservation, retrieval, use, and disposition.

**Federal Records:** Includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence or the organization, functions, policies, decision, procedures, operation or other activities of the United States Government.

**Preservation In-Place** - Protects and secures electronically stored information (ESI) from accidental deletion prior to collection. (NOTE: This is usually in reference to a litigation hold).

**HRSA Policy  
for  
Implementation of Capstone Mail (Email) Approach**

December 14, 2017

U.S. Department of Health and Human Services (HHS)

Health Resources and Services Administration (HRSA)

Office of Information Technology (OIT)



**Version History**

<b>Version Number</b>	<b>Revision Date</b>	<b>Description of Change</b>	<b>Changed by</b>	<b>Approved By</b>

The Office of the Chief Information Officer (OCIO) within HRSA’s Office of Information of Technology (OIT) is responsible for development and management of the (HRSA) Policy for Implementation of Capstone procedures. Please email any recommendations and changes to email any recommendations and changes to [recordsmanagment3@hrsa.gov](mailto:recordsmanagment3@hrsa.gov).

**Table of Contents**

1. PURPOSE ..... 1

2. ROLES AND RESPONSIBILITIES ..... 1

3. ELECTRONIC MAIL (EMAIL) ..... 3

4. LITIGATION HOLDS ..... 7

5. SYSTEMS REQUIREMENTS ..... 7

6. ACCESS REQUIREMENTS ..... 7

7. DISPOSITION REQUIREMENTS ..... 8

8. EMAIL RECORDS MANAGEMENT (CAPSTONE) TRAINING ..... 8

9. APPLICABLE LAWS/GUIDANCE ..... 8

APPENDIX A: KEY TERMS ..... 11

APPENDIX B: GLOSSARY ..... 12

## 1. PURPOSE

The purpose of this document is to establish HRSA's Electronic Mail (Email) Records Management retention policy for managing emails. The policy outlines key roles and responsibilities for implementing HRSA's Capstone Approach (General Records Schedule (GRS) 6.1: Email Managed under a Capstone Approach) and describes the process of managing and identifying senior officials based on agency role/position.

### 1.1 Scope

All HRSA Bureau/Office employees, and email users, regardless of the type or duration of their employment.

### 1.2 Authority

The Office of Management and Budget (OMB) and National Archives and Records Administration (NARA) released Memorandum M-12-18, Managing Government Records Directive, on August 24, 2012. The Directive states that by December 31, 2016, Federal agencies must manage all email records in an electronic format. Email records must be retained in an appropriate electronic system that supports records management and litigation requirements (which may include preservation-in-place models), including the capability to identify, retrieve, and retain the records for as long as they are needed.

## 2. ROLES AND RESPONSIBILITIES

### 2.1 HRSA Agency Records Officer (ARO)

- 2.1.1. Collaborates with stakeholders, evaluates and assigns roles/positions as Capstone or Non-Capstone, and forwards the list to the HHS Department Records Officer (DRO).
- 2.1.2. Ensures that Capstone designations are kept current with organizational changes.
- 2.1.3. Notifies and provides a current list of all changes in Capstone senior officials to the National Institute of Health (NIH), Center of Information Technology (CIT) and HRSA's Chief of Information Officer (CIO).
- 2.1.4. Provides training to HRSA staff on Capstone records management implementation Approach.
- 2.1.5. Ensures NARA-approved schedules are in place and identify systems that contain Federal email records.
- 2.1.6. Transfers permanent email records to NARA in accordance with approved records schedules and applicable laws, regulations, and NARA transfer guidance.
- 2.1.7. Validates all emails .pst files associated with Capstone senior officials have been moved NIH domain server to HRSA's SES share drive under the current month's name.

### 2.2 HRSA Records Liaisons (RLs)

- 2.2.1. Monitor personnel changes within their offices.
- 2.2.2. Inform the Agency Record Officer of all personnel changes relevant to Capstone status designations.

### 2.3 HRSA Chief Information Officer (CIO)

2.3.1. Oversees and ensure OIT email systems retain components of email messages identified in RFC 5322 including email attachments.

2.3.2. Ensures OIT has processes in place to capture and make accessible the email records for current and departed employees throughout the record's life cycle as determined by the records schedule or legal hold, whichever is longer.

2.3.3. Ensures OIT programs are in place to search across multiple email accounts or multiple systems are available to find emails needed for agency business.

2.3.4. Ensure program and processes in place to prevent unauthorized access, modification, or destruction of email records.

### 2.4 HRSA Office Information Technology (OIT)

2.4.1. Establishes and publishes standards for email account administration and storage allocations.

2.4.2. Ensures staff is trained and informed about the use of email in the workplace.

2.4.3. Provides helpdesk support.

2.4.4. Ensures older email messages remain accessible as technology is upgraded or changed. (Each time technology upgrades and changes take place information technology staff will ask agency administrators for information about the existence and location of older messages so they can be migrated to the new technology.)

2.4.5. Provides records management support to HRSA staff.

2.4.6. Provides the Records Management branch with the assistance and resources to transfer permanent email to the National Archives.

### 2.5 Heads of HRSA Bureaus/Offices

2.5.1. Ensure that all employees with email accounts are aware of and comply with the email policy.

2.5.2. Meet with departing employees to determine storage locations for email messages and ensure that messages meeting the definition of a Federal record are captured prior to alerting OIT to delete the user's account.

2.5.3. Notify the appropriate OIT email team when the accounts of former employees can be closed, per the HRSA Account Life Cycle and Password Policy.

2.5.4. Provide training and ensure all staff are aware of the training resources that are available to them.

### 2.6 HRSA Personnel (Employees, Contractors, Interns, and Fellows)

2.6.1. Attend basic records management training annually, including training on how to use the email system.

2.6.2. Recognize the difference between record material and non-record material and maintain email records accordingly, to the extent practicable.

2.6.3. Use the HRSA email system for all business purposes. This requirement applies to all user accounts that the employee uses or monitors.

2.6.4. Notify the Agency Records Officer to determine if an account holding a large number of permanent records should be re-designated as Capstone permanent.

2.6.5. Comply with the requirements of these procedures including requirements related to email preservation.

2.6.6. Recognize that all information created while conducting HRSA business is considered a Federal record.

2.6.7. Engage in practice of opening email on a regular basis (daily, if possible), deleting non-records items, and classifying and filing items needed for future reference.

2.7 National Institutes of Health (NIH), Center of Information Technology (CIT) (HRSA's Network Service Provider)

2.7.1. Extract and move exported email of senior officials identified in the HRSA NARA-approved NA-1005 to the HRSA share drive.

### 3. ELECTRONIC MAIL (EMAIL)

Most email can be categorized as a Federal record as defined in the Federal Records Act (44 U.S.C., 3301). Federal records comprise all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

The Capstone Standard Operating Procedures apply to the Senior Officials of all HRSA Bureaus and Offices (B/Os), and to contractors conducting business for and on behalf of the Agency through contractual relationships and service level agreements. National Archives and Records Administration (NARA) has an approved NA-1005 (on file), and HRSA will adhere and comply with the NARA GRS 6.1, Email Managed under a Capstone Approach disposition authority. HHS supplemental preservation requirements that apply to HRSA records and other documentary materials potentially relevant for litigation, investigations and audit matters may be found in the HHS Policy for Records Holds and in the HRSA Records Management Policies and Procedures Manual.<sup>1</sup>

Email transmissions declared as Federal records are Government property and may not be disposed of except in accordance with approved records schedules. In accordance with HHS policy, effective December 29, 2016, the email of all Capstone Officials listed on an approved NARA Form 1005 (NA 1005) will be treated as permanent records and retained indefinitely.

---

<sup>1</sup> **NOTE:** Capstone applies only to email records, as defined in this procedures. All other records—including paper, electronic, or other media—are governed by the GRS or the HRSA-specific records schedule.



### 3.1 Implementation of the "Capstone" Approach

Under the Capstone approach, HRSA manages email records based on the role/position of the account holder rather than on the content of each email record. Capstone officials include all those positions listed on the NARA Form 1005 "Verification for Implementing GRS 6.1" approved by NARA on May 4, 2017. This includes those officials in an acting capacity for any of the positions listed on the NA 1005 longer than 60 days. The form serves as a list of permanent officials included and excluded from HRSA's Capstone implementation.

**3.1.1.** Email records captured and managed under the Capstone approach must use an existing records retention schedule or be maintained as unscheduled records until the re-approval of the NARA Form NA 1005. For example, if there is a major re-organization or changes within the structure, HRSA will not implement GRS 6.1 until NARA reviews and approves the HRSA re-submission of NARA Form 1005.

**3.1.2.** The verification process requires HRSA to implementing GRS 6.1, Email Managed under Capstone approach, to submit and updated NARA NA-1005, (This form ensures that all HRSA positions are appropriately identified and documented). The HRSA Agency Records Officer (ARO) coordinates with NARA to gain their approval prior to implementing any items on the updated GRS.

**NOTE:** The verification process for identifying Capstone officials is located in the record description of GRS 6.1. The definition of Capstone (permanent) accounts in item 010 of the GRS defines the ten categories of senior officials and acknowledges that different divisions often have different titles for similar positions. This approach is meant to assist HRSA in properly identifying senior officials within their Bureaus and Offices that correlate to each category.

### 3.2 Retaining Email Records

Email records are captured and managed according to user role using the following retention approach:

#### **3.2.1. NIH/CIT role as HRSA's Network Service Provider:**

- a) Retain email for the senior officers identified in HRSA's NARA-approved NA-1005 every Sunday for the prior 7 days.
- b) On the first Sunday of the month, run a script to create a folder for the prior month on the HRSA OIT Share Drive.
- c) Export email out of the mailbox of all users identified in the HRSA Capstone program to Outlook Personal Folders (.pst) files on a local NIH server.
- d) Move the exported .pst files from the NIH server to the HRSA share under the current month's name.

**3.2.2. Email Records of Designated Capstone Officials.** Email records (e.g., email messages and attachments, calendar appointments, and tasks captured by the electronic recordkeeping system) from designated Capstone official's email accounts are retained as permanent. These email records will be transferred to NARA according to GRS 6.1, Section 010. The HRSA Agency Records Officer maintains the official list of Capstone officials' email accounts and forwards a copy of the list to the Bureau/Office Records Liaisons annually.

**3.2.3. Email Records Captured from Email Accounts Not Designated as Capstone Officials.** Email records (e.g., email messages and attachments, appointments, and tasks captured by the HRSA electronic recordkeeping system) of all other account holders are retained as temporary according to GRS 6.1, Sections 011 or 012 and destroyed the electronic recordkeeping system. If HRSA decides not to use NARA GRS 6.1 then a records disposition schedule must be created and submitted to NARA for approval. (NOTE: Preclude records under preservation obligation, such as a litigation hold).

**3.2.4. Email Users.** Each email user (whether creator or recipient) shall take responsibility for identifying whether an email communication fits the definition of a Federal record. If deemed to be evidence of one's activities, the email shall be retained, preserved, and disposed of in accordance with the HRSA records schedule.

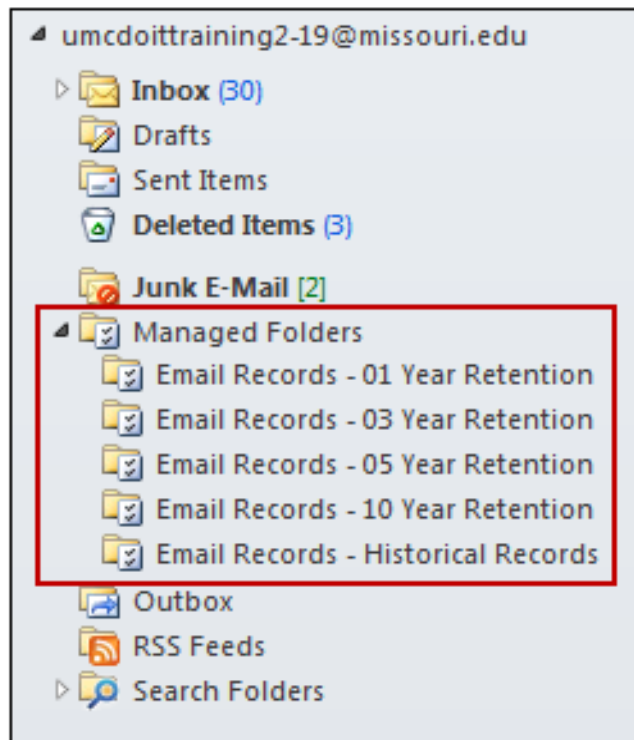
**3.2.5. Non-Record Emails.** HRSA employees may delete non-record emails that do not contain information documenting HRSA actions or activities. Non-records include items such as non-business related messages, personal messages, broadcast messages (e.g., HHS messages to all staff), and advertisements. (NOTE: This precludes records under preservation obligation, such as a litigation hold).

**3.2.6. Transitory Email Records.** Transitory records are records of short-term (180 days or less) interest which have minimal or no documentary or evidential value. Email records that are transitory may be deleted when no longer needed (precluding records under preservation obligation, such as a litigation hold).

**3.2.7. Email Containing PII.** Certain information containing sensitive or restricted data (e.g., Identifiable information) shall not be stored, transmitted, or processed using the HRSA or HHS email infrastructure unless appropriate information security mechanisms (e.g., message encryption) are used.

**3.2.8. Managing Email Records Manually.** When automated tools or features are not available within the email system to auto-categorize folders and emails, employees must manually create folders within their email inbox and manage records by record type. (NOTE: For best retention and disposition practices, a folder should be created for each record type and sub-folders created for more specific categories).

After brief periods in the Inbox, messages should be transferred to titled folders or subfolders specific to a record series. An example is provided below:



**3.2.9. Email Retained with Related Records.** When business needs require email records retained within another electronic recordkeeping system (such as part of a case file), a copy of the email should be kept with those files. Capstone does not replace existing business practices that require email messages and other related records to be retained together in established electronic recordkeeping systems.

**3.2.10. Search and Auditing of System.** System-wide email searches may be conducted by designated OIT Security personnel with the approval of the General Counsel or Chief Information Officer (CIO) as part of an internal or external investigation or in response to an access request.

**3.2.11. Unauthorized Destruction of Email Records and Reporting Loss.** If there is an instance of unauthorized destruction of email records, the user should first notify a supervisor and then contact the IT Helpdesk to attempt recovery. If recovery is not possible, the user or office must report the incident to the HRSA ARO. The ARO will subsequently report the incident to the HRSA Chief Information Officer (CIO). Per 36 CFR 1230.14, the report will describe the records, the circumstance in which the unauthorized destruction took place, and the corrective steps taken to manage the records properly in the future.

**3.2.12. Conducting Agency Business via Unauthorized External Information Systems** Transmission of HRSA "sensitive" information via personal email is prohibited. In the interest of both protecting the HRSA employee's personal privacy and increasing transparency for the public, HRSA employees assigned a HRSA-provided computer, email, and/or online storage account must use those government-provided resources for conducting any and all

official business. Under no circumstances should HRSA employees conduct official HRSA business using a personal computer, personal email, or personal online storage accounts.

#### **4. LITIGATION HOLDS**

When litigation is pending or threatened against HRSA or its employees, the Agency by law is required to preserve all data and information that pertain to the issue. Agency staff in receipt of a litigation hold directive are responsible for preserving electronically stored information (ESI), including all email communications sent, received, stored, or maintained in an Agency email account, as well as all email communications, data, and information existing on a network shared drive, local computer, and/or portable storage devices. Employees may not alter, delete, or destroy email that has been downloaded, saved, moved to a storage account or device, printed, or stored in paper form.

A litigation hold overrides the email policy, as well as any records retention schedules that may have otherwise called for the transfer, disposal, or destruction of relevant documents until the hold has been cleared by Office of General Council (OGC).

Accounts of separated employees that have been placed on legal hold status will be maintained by the departing individual's supervisor and HRSA OIT until the hold is released.

#### **5. SYSTEMS REQUIREMENTS**

The National Institutes of Health (NIH) is the HRSA email service provider, and HRSA abides by NIH's standard policies.

#### **6. ACCESS REQUIREMENTS**

##### **6.1 Retrievable**

Access supports an agency's ability to carry out its business functions. Access must address internal agency needs and accommodate responses to requests for information. As such, email records must remain usable and retrievable throughout their life cycle. All employees shall manage Federal records created in or transmitted using the HRSA e-mail system in a manner that allows each to be accessible and readable for the specific record retention period.

##### **6.2 Preservable**

Email records must be maintained in a system that (a) preserves their content, context, and structure, (b) protects against their unauthorized loss or destruction, and (c) ensures they remain discoverable, retrievable, and usable for the period of the email's life cycle. Searchable

Employees do not have privacy in anything they create, send, receive, or store on the HRSA e-mail system. This includes Instant Messaging. Messages stored in Office 365 (Outlook), in the Personal Storage Table (.pst) files residing on a shared network drive or local drive, and in portable storage devices (e.g., DVD, flash or USB drive) are subject to search for purposes of responding to disclosure requests (e.g., FOIA, litigation holds, etc.). All messages sent to or received by Government systems are subject to search.

## **7. DISPOSITION REQUIREMENTS**

### 7.1 Schedule

HRSA has a NARA-approved agency-specific schedule in place to carry out the disposition of permanent and temporary records. The schedule was last approved in September 2016.

### 7.2 Disposition

Just as HRSA has identified appropriate retention periods for email records, it has also implemented systems and policies to support the disposition of the records. These are specified in the approved GRS 6.1 records schedule.

### 7.3 Manual Deletions

Employees are encouraged to delete non-record messages on a daily basis, immediately after reading, replying, or taking other action concerning a particular message. Employees are not allow to delete record messages, unless the appropriate disposition have been met.

## **8. EMAIL RECORDS MANAGEMENT (CAPSTONE) TRAINING**

The HRSA Agency Records Officer is responsible for ensuring that appropriate staff in HRSA's Bureaus and Offices receive email records management (Capstone) training to ensure they are aware of their responsibilities to maintain and safeguard agency email records, including the obligations under this procedure and the HHS Records Holds Policy.

### 8.1 New Employees Orientation

HRSA employees whose positions have been designated as Capstone (permanent) will receive an initial briefing as part of their training on their email records management responsibilities.

### 8.2 Annual Training

HRSA personnel must complete Records Management training annually, which must include a section on email records management (Capstone Approach).

## **9. APPLICABLE LAWS/GUIDANCE**

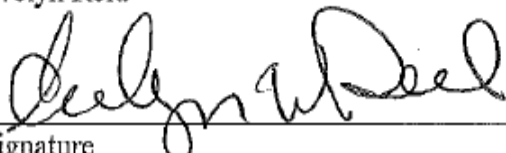
Authorities include:

- 36 CFR Chapter XII, Subchapter B - Agency Records Management Responsibilities
- 36 CFR Chapter XII, Subchapter C - Electronic Records Management
- 44 U.S.C. Chapter 21 - National Archives and Records Administration
- 44 U.S.C. Chapter 29 - Records Management by the Archivist of the United States
- 44 U.S.C. Chapter 31 - Records Management by Federal Agencies
- 44 U.S.C. Chapter 33 - Disposal of Records

- 44 U.S.C. 3301 - Definition of Records
- OMB M-12-18, Managing Government Records Directive
- General Record Schedule 6.1: Email Managed under a Capstone Approach  
<http://www.archives.gov/records-mgmt/grs/grs06-1.pdf>
- HRSA Records Management Policies and Procedures Manual

**APPROVALS**

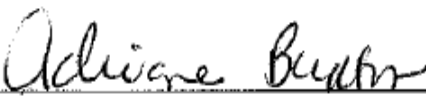
HRSA Agency Records Officer  
Evelyn Reid

  
Signature \_\_\_\_\_ Date 12/13/17

HRSA Deputy Chief Information Officer  
Valerie Wampler

  
Signature \_\_\_\_\_ Date 12/13/17

HRSA Office Chief Information Officer  
Adriane Burton

  
Signature \_\_\_\_\_ Date 12/14/2017

## APPENDIX A: KEY TERMS

The following table provides definitions and explanations for terms and acronyms relevant to the topic presented within this document.

Term	Definition
C.F.R.	Code of Federal Regulations
Email	Electronic mail
HRSA	Health Resources & Services Administration
OIT	Office of Information Technology
NARA	National Archives and Records Administration
OMB	Office of Management and Budget
U.S.C.	United States Code
CIO	Chief Information Officer
ARO	Agency Records Officer
RL	Records Liaison



## APPENDIX B: GLOSSARY

**Capstone** - An approach to managing email where agencies must identify the email accounts most likely to contain records that should be preserved as permanent. Agencies determine Capstone accounts based on their business needs. They should identify the accounts of individuals who, by virtue of work, office, or position, are likely to create or receive permanent valuable Federal records. Capstone officials will generally be the top-level senior officials of an agency, but may also be other key decision makers at lower level of the agency.

**Capstone Official** - Senior officials designated by account level or by email or by email addresses, whether the addresses are based on an individual's name, title, a group, or a specific program function. Capstone officials will generally be the top-level senior officials of an agency, but may also be other key decision makers at lower levels of the agency.

**Control and Custody of Records** - HHS records and materials are the property of the Federal government, not the property of individual employees or contractors acting as an agent for the government, and may not be removed from the Agency without proper authority. All employees and contractors shall maintain records and non-record documentary materials separately from one another.

**Culling** - The act of removing or deleting material prior to disposition. This may include deleting non-record email [e.g., email blast (such as agency-wide communications), spam, and personal email (records belonging to an individual and not related to agency business)], and transitory email records (records of short-term interest or that have minimal documentary or evidentiary value).

**Disposition:** Final operational action taken in the records life cycle. It includes the destruction of temporary records or the accession of permanent records to NARA.

**Electronic Mail (Email)** - All traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

**Email User** - An employee, contractor, volunteer, intern, or any other person who uses the HRSA email system.

**Electronic Messages** - Electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals.

**Electronic Mail (Email) System** - A computer application used to create, receive, and transmit messages and files. Excluded from this definition are file transfer utilities (software that transmits files between users, but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or databases on either personal computers or mainframe computers. (36 CFR 1236.2)

**Electronic Records** - Any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record in 44 U.S.C. 3301. Electronic records include numeric, graphic, and text information that may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record.

This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks. Unless otherwise noted, these requirements apply to all electronic records systems, whether on microcomputers, minicomputers, or mainframe computers, regardless of storage media, in the network or stand-alone configurations.

**Electronic Records Keeping System** - An electronic system in which records are collected, organized and categorized to facilitate their preservation, retrieval, use, and disposition.

**Federal Records** - All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with transaction of public business and preserved (as appropriate) by that agency or its legitimate successor as evidence of the organization, its functions, policies, decisions, procedures, operations and other activities executed to support the United States Government.

**Permanent Records** - Any federal record appraised by NARA as having sufficient historical or other value to warrant continued preservation beyond the time it is needed for administrative, legal, or fiscal purposes. Permanent records are accessioned by NARA when no longer needed by the agency.

**Preservation In Place:** A label or category that protects and secures electronically stored information (ESI) from accidental deletion prior to collection. (NOTE: This is usually in reference to a litigation hold). Bureaus/Offices must suspend disposition and retain any email, regardless of its record status, when the email becomes subject to a legal requirement to preserve or hold the email until the obligation to preservation is lifted.

**Temporary Record:** Any federal record appraised by NARA for disposal after a specified retention period.