



NIH E-Mail Message Backup Policy

**Chief Information Officer
National Institutes of Health
Department of Health and Human Services**

Version 2.1

August 16, 2011

This page was left blank intentionally.

Table of Contents

1. Purpose.....	5
2. Background.....	5
3. Scope.....	5
4. Policy	6
5. Roles and Responsibilities	6
5.1 NIH Chief Information Officer (CIO)	6
5.2 NIH Chief Information Security Officer (CISO)	6
5.3 IC Chief Information Officer (IC CIO)	6
5.4 IC Information Systems Security Officer (ISSO)	6
5.5 NIH Records Management Officer	7
5.6 NIH IC and OD Office Directors	7
5.7 IC Records Management Officers	7
5.8 Management Officials	7
5.9 System Owners	7
6. Compliance and Oversight.....	8
7. Applicable Laws and Guidance	8
8. Information and Assistance.....	8
9. Effective Date/Implementation.....	8
10. Approved.....	8
Glossary	9
Appendix A: Links Referenced.....	10

This page was left blank intentionally.

Record of Changes

Version Number	Release Date	Summary of Changes	Section Number/Paragraph Number	Changes Approved by and Date
1.0	October 6, 1997	Original Version.	All	OCIO/ISAO
2.0	September 23, 2004	Changed the back-up retention period for e-mail records.	All	OCIO/ISAO
2.1	August 16, 2011	Annual review and updated format.	All	OCIO/ISAO

This page was left blank intentionally.

1. Purpose

This document presents the National Institutes of Health (NIH) policy on e-mail message backup. This policy applies to all emails that are created or received by NIH employees or by contract personnel. Retention and disposition guidance can be found in the NARA approved Manual Chapter 1743, Keeping and Destroying Records. The General Records Schedule may be utilized for Electronic Records or Information Technology Operations and Management Records.

2. Background

E-mail messages created or received on NIH computer systems or transmitted over NIH networks are NIH property. E-mail messages that document activities of the agency or have informational value are considered federal records and must be maintained appropriately. Official NIH records are created by or for NIH or received by NIH in the course of doing business. The essential points about these records are that: (1) they contain information about the organization, functions, policies, procedures, decisions, or other activities of NIH or any of its components; or (2), they contain information such as biomedical data, which is useful to NIH in carrying out its mission. See <http://oma.od.nih.gov/ms/records/rtypes.html#rt> for a definition of a federal record.

Necessary and useful records must be retained in the files of NIH offices and laboratories for as long as required and reasonable. It must be possible to retrieve information efficiently from these files, therefore unnecessary records must be weeded out so that valuable space is not taken up by records not needed for current business and that records with lasting historical, legal, or scientific value are preserved.

All NIH e-mail messages, including backup copies, are subject to official inquiries such as Freedom of Information Act requests, requests from Congressional committees and subcommittees, Office of Inspector General audits and investigations, and requests involving litigation and other official investigations. NIH's ability to comply with these inquiries efficiently depends on the time required to search the large volume of e-mails that are stored on individual systems and backup files.

More information on NIH official records policy, including definitions and retention schedules, can be obtained from: <http://oma.od.nih.gov/manualchapters/management/1743/>.

3. Scope

This policy applies to all NIH e-mail services, including all NIH information systems operated by a contractor on behalf of the government.

4. Policy

System administrators who have responsibility for creating backup copies of NIH e-mail records must maintain the backup copies for seven working days. This provides for efficient management of information contained in e-mail messages and attachments while ensuring that there is adequate backup to restore e-mail records that have been deleted from NIH computers due to equipment failure or user error.

In accordance with current NIH Records Management Guidelines, e-mail messages that are considered to be official NIH records will be copied, along with the transmission data, distribution list, and attachment(s), if applicable, to a separate recordkeeping system and then deleted from the user's e-mail system. This recordkeeping system can be either hard copy or electronic.

To facilitate NIH's ability to comply with requests for official records, users will be advised to delete all non-official e-mail records and those official records existing past the required retention period from their computers in compliance with records management requirements.

5. Roles and Responsibilities

The primary individuals listed below may assign a designee to carry out these responsibilities.

5.1 NIH Chief Information Officer (CIO)

The NIH CIO establishes and ensures the implementation of this policy at NIH consistent with all other Federal, Department of Health and Human Services (HHS), and NIH rules and regulations.

5.2 NIH Chief Information Security Officer (CISO)

The NIH CISO implements this policy within NIH, ensures compliance, reviews exception requests specific to this policy and renders decisions.

5.3 IC Chief Information Officer (IC CIO)

The IC CIO provides the resources necessary for this policy implementation; training of IC employees, as appropriate; implementing security controls required; and reporting this policy implementation status to the CISO. The IC CIO is also responsible for ensuring that IC specific policies, guidance, and standards are written and implemented, as applicable.

5.4 IC Information Systems Security Officer (ISSO)

The IC ISSO coordinates the implementation of this policy within his or her IC, ensures compliance, and submits exception request to the NIH CISO.

5.5 NIH Records Management Officer

The NIH Records Management Officer of the Office of Management Assessment (OMA), Division of Management (DMS) develops, maintains and revises the NIH Records Control Schedule. They are also responsible for:

- Assisting and advising NIH offices on interpreting or applying the records control schedule within NIH;
- Providing liaison with HHS and higher authorities regarding all aspects of records keeping and disposal.

5.6 NIH IC and OD Office Directors

The NIH IC Directors are OD Office Directors designate an Institute and Center (IC)/Office of the Director (OD) Office Records Management Official, known as the Records Liaison.

They are also responsible for:

- Integrating the NIH records management program into IC/OD Office operations and ensuring compliance;
- Applying the recordkeeping and disposal instructions from the NIH Records Control Schedule to IC/OD Office files; and
- Ensuring that adequate records management training is provided to all staff.

5.7 IC Records Management Officers

The IC Records Management Officers, known as Records Liaisons, implements the records management policies and procedures. They are also responsible for:

- Ensuring that the records control schedule is implemented within each IC;
- Assisting and advising IC personnel on interpretation of the schedules;
- Ensuring that all employees know the difference between personal and agency records;
- Assisting IC personnel in retiring inactive records to the Washington National Records Center; and
- Reviewing and transmitting reference requests to the Washington National Records Center for withdrawing records.

5.8 Management Officials

Management officials, in their supervisory role, ensures that employees, contractors, interns, etc., review this policy in a timely manner, as appropriate; and informing users (employees, contractors, interns, etc.) of their rights and responsibilities, including the dissemination of the information in this policy.

5.9 System Owners

System Owners ensure that systems under their control adhere to this policy or that a current policy waiver is in place.

6. Compliance and Oversight

Where deviations from this policy are necessary, requests for policy exceptions will be evaluated by the NIH CIO and the NIH CISO. A waiver request must include a business case that specifies how the enforcement of this policy would restrict the mission of NIH and the specific compensating controls that will be implemented. IC ISSOs are responsible for submitting exception requests to the NIH CIO and the NIH CISO using the NIH Policy Waiver form. The NIH CIO and NIH CISO will determine what additional documentation may be needed from the IC ISSO submitting the request.

7. Applicable Laws and Guidance

HHS-OCIO Policy for Information Systems Security and Privacy, September 2010

NIH Manual Chapter 1743, *Keeping and Destroying Records*

NIH Enterprise Information Security Plan

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* (as amended)

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

8. Information and Assistance

Comments, questions, suggestions, or requests for further information should be directed to the NIH/OCIO/ISAO.

9. Effective Date/Implementation

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

10. Approved

_____/s/_____
Daniel A. Sands
NIH Chief Information Security Officer

8/16/2011
Date

Glossary

For additional information or terms, please visit the [NIH Glossary of IT Security Terms](#).

Appendix A: Links Referenced

NIH Definition of Official Records

<http://oma.od.nih.gov/ms/records/rtypes.html#rt>

NIH Official Records Policy

<http://oma.od.nih.gov/manualchapters/management/1743/>