



## RUTGERS POLICY

**Section:** 50.3.10

**Section Title:** Legal Matters

**Policy Name:** Records Management

**Formerly Book:** N/A

**Approval Authority:** Executive Vice President for Academic Affairs and Senior Vice President for Administration

**Responsible Executive:** Executive Vice President for Academic Affairs and Senior Vice President for Administration

**Responsible Office:** Division of Administration & Public Safety

**Originally Issued:** June 11, 2007

**Revisions:** 9/19/2012; 7/1/2013; 10/10/2013 (Updated title)

**Errors or changes?** Contact: [apspolicies@aps.rutgers.edu](mailto:apspolicies@aps.rutgers.edu)

1. **Policy Statement**

The university recognizes that the efficient management of its records, regardless of their form or medium, is essential to support its core functions, to comply with its legal and regulatory obligations, and to contribute to the effective overall management of the institution. The university further recognizes that proper methods of records disposal and the determination of what records should be stored in the University Archives for permanent preservation is an important responsibility. This document provides the policy framework through which to meet this responsibility.

2. **Reason for This Policy**

- To promote efficient administration and management of the records of Rutgers, The State University of New Jersey.
- To provide guidance on the maintenance, retention, storage and disposition of official records based on their fiscal, legal, administrative, and historical value to the university.
- To reduce and/or prevent unnecessary legal and fiscal responsibility caused by retaining university records longer than the retention schedules authorizes or by premature disposal of university records.

3. **Who Should Read This Policy**

All members of the Rutgers University community.

4. **Related Documents and Links**

- Rutgers Records Management Program (includes Records Retention Schedules: <http://recordsmanagement.rutgers.edu>)
- University Archives: <http://www.libraries.rutgers.edu/rul/libs/scua/scua.shtml>
- Identity Theft Compliance Policy 50.3.9 in the University Policy Library at: <http://policies.rutgers.edu>

- Draft Information Security Classification Policy: <http://rusecure.rutgers.edu/content/draft-information-security-classification-policy>
- Minimum Security Standards for Networked Devices: <https://rusecure.rutgers.edu/content/minimum-security-standards-electronic-devices>
- NIST Special Publication 800-88, Guidelines for Media Sanitization: [http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_with-errata.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf)

## 5. **Contacts**

Rutgers Records Management Program

- recordsmanagement@aps.rutgers.edu
- <http://recordsmanagement.rutgers.edu/>

## 6. **The Policy**

### 50.3.10 RECORDS MANAGEMENT

#### I. **INTRODUCTION**

Records management is the systematic control of recorded information from creation or receipt, through processing and use, until final disposition. Final disposition will be through destruction or transfer into the University Archives. Proper records management satisfies compliance with laws and regulations, and ensures that historically significant records are properly preserved.

This policy provides direction on records management to ensure that the university complies with federal, state, and other regulatory guidelines. Therefore, university faculty and staff shall:

- Retain records according to established Records Retention Schedules
- Maintain active and inactive records in appropriate storage equipment and locations
- Preserve records of historical significance
- Protect sensitive information using secure methods of recordkeeping and disposal
- Identify and protect vital records
- Discard (in an approved manner) records that are no longer required

No employee has, by virtue of his/her position, any personal or property right to official records even though he/she may have helped develop or compile them. The unlawful destruction, removal from files, and personal use of official university records is strictly prohibited.

#### II. **DEFINITIONS**

##### A. **Definition of a Record**

University records are defined as any and all data or information in a fixed form and in any format that is created or received in the course of institutional activity and retained as evidence of that activity for future reference. Records include all textual or printed materials including, but not limited to, papers, manuscripts, correspondence, books, maps, drawings, plans; microfilm, photographs, sound and moving image recordings, electronic data and/or machine readable data on all mediums or other documentary materials regardless of physical form and characteristics.

##### B. **Vital Records**

Some university records are “essential” meaning that their loss would jeopardize the rights and privileges of the university. Vital records include records whose legal status and informational value to the university is so great, and the consequences of loss are so severe, that special protection is justified in order to reduce the risk of loss. The following records are considered to be essential:

- Records containing information required to re-establish or continue the university in the event of a disaster

- Records containing unique and irreplaceable information necessary to recreate the university's legal and financial position
- Records that preserve the rights of the organization and its employees, students, and other constituent groups.

C. **Electronic Records**

Electronic records consist of information captured through electronic means, and which may or may not have a paper record to back them up. Electronic records are data or information that has been captured and fixed for storage and manipulation in an automated system and requires the use of the system to render it intelligible by a person. "Electronic records" can encompass both analog and digital information formats and most often refers to records created in electronic format (born digital) but is sometimes used to describe scans of records from other formats. Examples of electronic records include, but are not limited to, email, text messages, pdfs, word processing documents, digital photographs, sound recordings, moving images, formatted data, spreadsheets, databases, and records existing in a university computing cloud such as emails, instant message conversations, calendars, videos, blogs, etc.

D. **Archival Records**

Archival records are defined as any and all data or information in a fixed form and in any format that is created or received in the course of institutional activity and are permanently retained because of their enduring informational, evidential, and historical value.

E. **Active Record**

An active record is a university record that is currently being used during the ordinary course of university business.

F. **Inactive Record**

An inactive record is a university record that is no longer being used in the ordinary course of university business, but must still be retained until the end of its Records Retention Schedule.

G. **Expired Record**

An expired record is a university record that is no longer being used in the ordinary course of university business when such record has fulfilled its retention requirement in accordance with the Records Retention Schedule and does not need to be permanently retained. A record cannot be considered "expired" if it is currently subject to a "Litigation Hold Notice."

H. **Office of Record**

The Office of Record is the designated division, department, unit or individual, as identified in the Records Retention Schedule, responsible for both the retention and timely destruction of university records in accordance with this policy.

I. **Retention Schedule**

The Records Retention Schedule provides a list of official records for each major administrative department in the university and prescribes the periods of authorized retention. The schedule may be revised periodically to include a newly created record series, to change retention periods, or to address records that are no longer useful or that are obsolete. A university record, regardless of the format in which it is created, must be retained for designated periods of time and may only be disposed of in accordance with approved retention and disposition schedules. Once a university record has satisfied its retention period, the retention schedule will dictate the document's ultimate disposition (i.e., authorized destruction, retention extension or transfer to the University Archives).

**J. Protected Health Information (PHI):**

Protected health information means individually identifiable health information that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual and identifies or could reasonably be used to identify the individual.

- Except as provided paragraph two (2) of this definition that is: a) transmitted by electronic media; b) maintained in electronic media; or c) transmitted or maintained in any other form or medium
- Protected health information excludes individually identifiable health information in: a) education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g; b) records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and c) Employment records held by a covered entity in its role as an employer.

**III. LOCAL UNIT'S RESPONSIBILITIES**

It is the responsibility of each local unit (department, division, area, etc.) to identify a records management liaison who shall be responsible for ensuring the storage of active records in an appropriate manner which is consistent with this policy. Responsibilities of the local unit include, but are not limited to the following:

1. University records, both paper and electronic, must be properly maintained during their retention period. In-house maintenance of records should ensure proper accessibility, security, and protection.
2. Identify an authorized location for storing university records within the unit's custody. Questions regarding proper storage and identifying authorized locations should be directed to the Records Management Program.
3. All university employees must ensure that information in confidential or privacy-protected records is protected from unauthorized disclosure through the ultimate disposition of these records. As a normal matter of conducting business, destruction of confidential or privacy-protected records will be done by shredding or pulping. "Deletion" of confidential or privacy-protected information in computer files or other electronic storage media is not acceptable. Electronic records must be "wiped" clean or the storage media physically destroyed. These methods of destruction are specified in the retention schedules so that records may not be viewed or used by unauthorized persons after they are disposed.
4. Many records can be legally destroyed at the end of their active lives if there are no audit, legal, fiscal, regulatory or historical reasons for the preservation of the records. Those university records designated for destruction (after fulfilling their retention requirement) must be disposed of in an appropriate method. Records containing confidential information should be destroyed by pulping, shredding, or incineration. In accordance with HIPAA regulations, the destruction/disposal of all PHI will be accomplished by shredding, incineration or another comparable fashion that ensures that the PHI cannot be recovered or reconstructed.
5. In the case of electronic records, complete and proper deleting and purging should be performed.
6. Email messages and other electronic business records are considered university records and are subject to the same retention requirements as that which govern the management of paper records.

For assistance in determining how to dispose of university records and/or to identify appropriate storage locations, local units should contact the Records Management Program.

#### **IV. RECORDS MANAGEMENT OFFICE RESPONSIBILITIES**

The university's Records Management Office, provides resources and information on the creation, management, transfer and/or disposition of all official Rutgers records. As a continuing management function, the university's Records Management Coordinator shall provide for the retention of university records through the period of their value or legal requirement and for their systematic disposition.

Inactive records may be stored in the University Records Management Center, which offers departments a centralized storage facility where inactive records may be stored, retrieved, and disposed of once the Records Retention Schedule has expired. Exceptions may be granted with the written approval of either the Executive Vice President for Academic Affairs or Senior Vice President for Administration. Records in the Records Management Center remain under the authority of the depositing department, and may be retrieved by that department upon request. Records stored in the Records Management Center may not be used for research except by the depositing department, or with the written permission of the depositing department, or as otherwise determined by an authorized official. Records may also be retrieved in accordance with all relevant legal or fiscal requirements of the university.

The services of the Records Management Office are available to all university units. The Records Management Office will:

1. Develop Records Retention Schedules in conjunction with departmental staff and monitor the maintenance of and compliance with those schedules.
2. Assist with inventorying departmental active records and analyzing active departmental record-keeping systems.
3. Manage and operate the Records Management Center, retrieving records upon the request of the depositing department or authorized personnel.
4. Arrange for the appropriate disposal of records stored in the Records Management Center, according to the Records Retention schedules.
5. Assist in the preparation for and protection of university records in the event of a disaster.
6. Provide departmental consultations and campus-wide workshops to better educate the university community in proper records management principals.

#### **V. AUDIT**

Adherence to proper records storage and to the appropriate Records Retention Schedules is subject to audit by the Internal Audit Department.