University of Wisconsin-Madison

RECORDS MANAGEMENT

Archives and Records Management Services (ARMS)

Records Management Publications Series

Records Disposition & Destruction

Guidelines for University departments concerning best practices for the disposal and destruction of records

THE UNIVERSITY of WISCONSIN MADISON

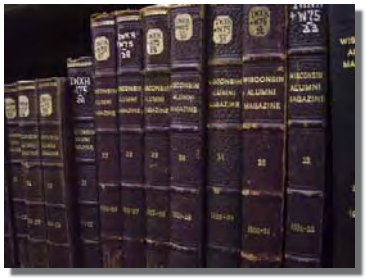
ARMS
Archives and Records Management Services

Created by UW-Madison Archives and Records Management Services (ARMS)
Published: January 2007

Records Disposition & Destruction

Guidelines for University departments concerning best practices for the disposal and destruction of records

CONTENTS



Records at the UW Archives

INTRODUCTION

Privacy and the need to protect records and information throughout their life cycle have placed increased significance upon the disposition and disposal process. Legislation such as Wisconsin's Dumpster Diving Law, HIPAA, and recently proposed federal legislation enhancing the protection of Social Security Numbers (SSNs) emphasizes that need. Records disposition normally occurs at the end of the records life cycle. Two things prevent this: either numerous duplicate copies of records are made or they exist in multiple formats that do not need to be maintained until the end of the life cycle and can be destroyed. University offices need to follow appropriate policies and procedures pertaining to records disposal so that inadvertent disclosure of sensitive information is avoided and also to ensure compliance with state and federal laws.

Breaches in data security can also occur if proper destruction procedures are not followed. The inadvertent exposure of student record data, patient data, personal financial information, or other sensitive information can have significant consequences for the University. In such situations, an organization can be required to notify all affected parties (all persons whose information was accessed without their consent) as well as pay costs associated with such notification and other penalties. It is critical that proper destruction of data be completed before the disposal of hard drives, cell phones, laptops, and other electronic devices that have been used to store large quantities of personally identifiable or confidential information.

The methodologies for destroying records are changing as different types of technologies are used to record and store records and information. While paper continues to be the dominant storage medium, it is often not the only storage medium in which a particular record may be recorded and stored. University offices need to be aware that merely destroying the paper record will not necessarily fulfill a requirement to destroy records.

This publication discusses requirements, procedures, and processes that will ensure that records and information are appropriately protected during the disposition and destruction process. It also contains a checklist for determining appropriate disposition of University records. For the UW-Madison guidelines on records destruction, please consult the appendix of this document.

Authority for Records Destruction

University records, including recorded information assets, are retained and destroyed in accordance with approved records retention policies (see the UW-Madison Records Destruction Guidelines in the appendix of this publication). These policies (in the form of records retention schedules) are developed and approved according to Wisconsin's Public Records Law. The retention schedules identify relevant State and Federal requirements that may apply to the particular set of records. They indicate whether the records are confidential or contain sensitive information that may require special handling at the time of records destruction.

Prior to implementing the recommended disposition (normally either destroying the records or transferring them to the University Archives), the University department should also be certain:

a. No open audit or audit exception exists.
b. No pending litigation involving the records exists.
c. No open records requests exist.
d. Appropriate notifications have been given, if required.

Legal Issues and Requirements

What are some of the legal ramifications for failure to conduct proper disposal of records?

- When a system of recordkeeping is such that it in effect conceals or makes it difficult to locate records, this situation can be considered the functional equivalent of records destruction or spoliation.
- As previously noted, the destruction of records that are needed for litigation, an audit, or an open records request can lead to legal action.
- Failure to have a procedure to halt the destruction of records can also have legal implications, particularly as they apply to electronic records. The management of computer tapes needs to include hold procedures for data subject to legal action.
- The unauthorized destruction / deletion of email can be problematic. While email is not always admitted as evidence, the fact that it has been destroyed can always be used against you.
- New laws and regulations relating to personal privacy have monetary and other penalties associated with them.

Changes to the Federal Rules of Civil Procedure (effective December 2006), will in effect mandate many of the items noted above.

Perhaps more than the legal ramifications of unauthorized destruction is the appearance of poor recordkeeping practices. The negative public image created can linger and be of greater impact than the legal implications of destroyed records.

Records Management and Records Destruction

DESTRUCTION is defined as a disposal process that results in the obliteration of records.

Records Destruction Principles for University Records

The following principles should guide the destruction of University Records:

1. Authorized—*If necessary, has a records retention/disposition authorization (RDA) been prepared or other appropriate clearance been given for records disposal?*
2. Appropriate—*based upon the value of the records and the storage technology used. The level of concern for appropriate destruction resides not in the media but in the information recorded thereon.*
3. Secure and confidential.
4. Timely.
5. Documented as necessary or required.

Confidential Records

Numerous State and Federal laws describe records or types of information that must be considered private or that is confidential in nature. Some of these laws prescribe particular disposition procedures or processes.

One example of Wisconsin legislation on this topic is the ***Wisconsin Joint Legislative Council Information Memorandum 00-1*** (*http://www.legis.state.wi.us/lc/jlc00/im00_1.pdf*). This memorandum provides a listing of Wisconsin Statutes and constitutional provisions (in table format) relating to personal privacy and confidentiality. The table is organized by agency.

Generally, there are two broad categories of confidential or private information within the University community:

- Student records and information
- Medical records and information

Personal identifying information must also be treated as confidential and handled appropriately in the disposition process. This information includes: name, address, phone number, driver's license number, SSN, employer or place of employment, employee identification number, mother's maiden name, financial account numbers, and taxpayer identification numbers. Other personal identifying information includes: deoxyribonucleic acid profile, code, or number that used alone or with access devices can obtain information; unique biometric information (fingerprint, retina image); any unique information that is assigned to an individual or can be used to access services, funds, etc.; and any other information that can be associated with a particular individual through one or more identifiers or other information or circumstances.

University departments or units cannot determine the confidentiality status of their records. Generally, in Wisconsin State Government, records are considered to be open (that is, accessible by the general public) unless there is a specific State or Federal law or administrative rule that states the records are confidential. The confidentiality status of the particular type or record or set of data should be noted on its governing RDA. This information will be located in the access requirements section of an RDA.

Electronic Records

The disposal of electronic records poses special problems. Some people have advocated for simply removing index pointers as sufficient for "destroying" electronic records. Technically records are not destroyed until they are physically destroyed. Modifying either an index, shipping records to a commercial destruction center, or other like acts may make it difficult to find a specific record; however, from a legal perspective, they are not destroyed. Below are two specific media formats of electronic records.

- **Magnetic media:** Records on magnetic media can be "bulk erased" by subjecting them to a strong magnetic field, referred to as degaussing. For secure destruction, magnetic media can be reformatted. Back-up copies also need to be destroyed. Simply deleting the files does not remove the data from the magnetic media and therefore is not sufficient for records destruction. Reformatting, degaussing, or pulverizing are also appropriate methods for destruction of records stored on computer diskettes.

- **Optical media:** Records held on optical media can be destroyed by cutting, crushing, or other physical means of destruction. Rewritable optical disks should also be reformatted before being disposed of or re-used. Other physical means of destruction, such as microwaving, can be used; these are often only useful for very small quantities. Care should be taken with microwaving due to fumes produced and possible harm to the microwave oven if item is "over-cooked."

Outdated Electronic Systems

Encryption is generally not an accepted disposal methodology for electronic records. The ability of hackers to de-crypt is increasing and therefore, the ability of outside parties to access confidential or sensitive electronic data not be guaranteed over time (see the NIST *Guidelines for Media Sanitation*, 2006).

If information technology systems are going to be replaced, a process of de-commissioning the old system is recommended. De-commissioning involves several steps to insure that records and data are properly managed in moving from an existing technology to a new one.

Do not just delete files from electronic storage media such as floppy disks, rewritable optical disks, and hard disks. The information on these media formats can still be recovered.

Methods of Destruction

Destruction involves a variety of methods listed below:

- **Clearing:** This is a form of media sanitation that would render the information unrecoverable by data, disk, or file recovery utilities. One method of clearing is overwriting both the addressable locations and the logical storage locations with random data. There is software that will accomplish overwriting.

- **Purging/Degaussing:** Degaussing exposes the media to strong magnetic field in order to disrupt the recorded magnetic domain.

- **Recycling:** For most paper records without any personally identifiable or confidential information contained in them, recycling is a perfectly acceptable method of destruction.

- **Shredding:** Shredding is also acceptable for records disposal. Frequently, it can be time consuming, noisy, and environmentally unfriendly to use shredding. For small volumes of records, it can be an acceptable in-office method to destroy records.

- **Physical destruction:** With some devices, the only way to ensure that confidential or sensitive information has been destroyed is to physically destroy the item itself.

CAUTION:
Some devices such as cell phones, BlackBerries, and the like have batteries or other materials harmful to the environment. Care should be taken to remove the batteries prior to disposal/ destruction.

Please Note:
Sending devices to Surplus With A Purpose (SWAP) is not a disposition plan. SWAP is not responsible for records disposal/destruction. Destruction of records must occur prior to disposition of the device.

Compact Storage at the State Records Center

Contracting With Vendors

A number of commercial records storage facilities as well as recycling firms will conduct records disposal. It is always important to verify that services are as advertised. An onsite visit is recommended before signing any type of contractual agreement. Please refer to the ***ARMS Off-Site Records Storage publication*** and the ***UW-Madison Health Information Privacy Manual*** (*http://www.provost.wisc.edu/hipaa/privacymanual/*).

Similarly, if the records involved contain protected health information (PHI) and a vendor is contracted for disposal/destruction services, the contract needs to meet the following conditions:

1. Specify the method of disposal/destruction.

2. Specify the time that will elapse between acquisition and disposal destruction of the data/media.

3. Establish safeguards against breaches in confidentiality.

4. Provide proof of disposal/destruction..

Records at the SRC

Use of the State Records Center

The State Records Center (SRC) has a contract for confidential disposal with the University. In fact, all records on deposit at the SRC that are eligible for disposal are confidentially destroyed. The SRC does charge a fee for records disposal, but depending upon the volume of records to be destroyed, it can be a very economical way to destroy records. The SRC will also issue a certificate of destruction documenting that the identified records were destroyed along with the date of destruction. Information about using the State Records Center is available by contacting ARMS.

The SRC can also arrange for the destruction of microfilm or microfiche.

Definitions

Degaussing
The process of removing information from magnetic media by neutralizing the magnetic signal that encodes the information.

Destruction
A disposal process that results in the obliteration of records.

Expungement
The legal process leading to the destruction of a criminal record.

Media Sanitation
Term used by information technology industry to mean the process of destroying information from the digital media using approved equipment, techniques, and procedures.

Spoliation
The destruction of records by a willful or negligent act and usually carries with it some presumption of guilt.

Records Disposition
The last stage of a record's life cycle. In terms of Wisconsin's public records law, disposition means either physical disposal or transfer to an official state archival repository.

Records Retention Disposition/Authorization (RDA)
The form used to secure approval for the disposition of all public records. It outlines how long records are to be maintained and their disposition after a retention period has ended. After 10 years, the RDA sunsets (expires), and a new one must be resubmitted for Public Records Board approval.

Records Retention Schedule
The timetable and description of a records series' lifecycle, including instructions for disposition. In Wisconsin State government, the retention schedule takes the form of the Records Retention/Disposition Authorization (RDA).

Checklist

Use this checklist to help determine how to dispose and/or destroy records from your department. Please contact Records Management with any questions.

1. Consult the Records Destruction Guidelines (see the appendix of this publication).

2. Are the records covered by an approved Records Retention/Disposition Authorization (RDA)?

3. Is a secure destruction methodology required? If the approved RDA indicates that the records are confi dential or contain sensitive personal health information (PHI) records or information, then the records and information must be disposed/destroyed using a secure methodology.

4. In what type of storage media are the records contained?
   - Paper
   - Microfilm
   - Magnetic tape
   - Hard drive
   - CD
   - DVD
   - Other

5. Determine the type of destruction process based upon the content of the records (see the RDA) and the type of storage media used.

6. Have all copies been destroyed? How about the back-up tapes?

7. Do you need a certificate of destruction to document that the records have been destroyed? If the records contain PHI, a certificate of destruction may be required.

8. When retiring used computers, have the hard drives been scrubbed of data, reformatted, degaussed, or other destruction method to ensure that no records can be retrieved?

9. If contracting with a commercial vendor for records destruction, are they:
   - Equipped to handle the type of storage media that contain the records?
   - Bonded or otherwise insured?
   - A Business Associate or completed a Business Associate agreement? *(required if they are handling PHI)*
   - Have you specified a type of destruction method to be used?
   - If a high-level of security is required, does the vendor have locked bins or other in-house provisions for the temporary storage of the records while awaiting disposal?

10. If you are repurposing the device (i.e., surplus the device to SWAP, transferring to a charitable entity, etc.), make surethat ALL University records contained on the device have been properly disposed before the transfer. It is NOT the job of SWAP or other agencies to dispose of your records. If a complete disposal of the records cannot be accomplished, then the device should be physically destroyed.

11. Be aware that the following are insufficient for records destruction:
    - Removing the partition information from the media, such as using FDisk.
    - Reinstalling the operating system, without first completing a full media overwrite.
    - Removing the media and disposing of it in any way that does not render it difficult to recover.
    - Using a magnetic degaussing tool is not reliable for every form of media (e.g., modern hard disks may not be completely erased with most degaussing tools).

Sources for Further Information

Digital Media Storage - Facilities and Procedures. Electronic Records Management Guidelines. South Carolina. Department of Archives & History. (*http://www.state.sc.us/scdah/erg/ermDMSFP.pdf*)

Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-88. February 2006.

IM 06-03. New Wisconsin Identity Theft Statutes (2005 Acts 138, 139, and 140)Wisconsin Legislative Council Information Memorandum.
(*http://www.legis.state.wi.us/lc/2_PUBLICATIONS/Other%20Publications/Reports%20By%20Subject/Privacy%20and%20Information%20Technology/IM06_03.pdf*)

Purdue University Information Security Program.
www.itap.purdue.edu/security/policies/GLBPurdue1.doc

Wisconsin Legislator Briefing Book 2005-06.
http://www.legis.state.wi.us/lc/2_PUBLICATIONS/Publications.htm

APPENDIX: University of Wisconsin–Madison Records Destruction Guidelines

Purpose

The University of Wisconsin–Madison recognizes the need for appropriate management of its records and information resources from their creation through disposition/destruction. It also recognizes that many institutional records and information resources contain confidential or sensitive information that must be safeguarded and appropriately disposed of in order to protect individual privacy. These guidelines describe the authority and requirements for records disposal within the University of Wisconsin–Madison.

Guidelines:

1. The authority for the retention and disposition, including physical destruction/deletion, of University records and information is the records retention schedule. For a listing of approved campus-wide retention schedules (usually called General Records Schedules), visit *http://archives.library.wisc.edu/RM/GENSKED/gensched.html*. If you need to prepare a records schedule, contact the Campus Records Officer.

2. University employees have a responsibility for the management, including appropriate disposition, of records they create and maintain as part of their job duties. It is further recognized that University employees handle and must have access to client (student, staff, and other) information in order to fulfill their job responsibilities.

3. Generally, paper records that do not contain personal or sensitive information can be recycled. Most routine administrative and financial paper records can be recycled. Recycling containers are available throughout the campus.
   For the purposes of this guideline, personal information generally includes medical information, account or credit information, tax information, and any individual information that may be accessed by the association of one or more personal identifiers.

4. Paper records containing private or confidential information (e.g., personal identifiers, credit card numbers, social security numbers, student academic information, personal financial information) must be confidentially destroyed. The State Records Center provides a confidential disposal service. Some private commercial vendors also provide this service, but it is up to the University department to ensure that the vendor meets the requirements of this guideline and also the ARMS publication on off-site storage.

5. It is advisable to render undiscoverable certain types of personal information prior to disposal. This can be accomplished by:
   - Shredding. Cross-cut shredding or shredding that results in materials being less than 1/8 of an inch wide.
   - Erasing the personal information in the records.
   - Modifying or otherwise making the personal information unreadable.
   - Taking actions that will reasonably result in no unauthorized individual access to the personal information contained in the records.

6. Encryption can be used to secure confidential or sensitive data; however, it is not a disposal mechanism. University employees are reminded that if encryption is used for official institutional records, care must be taken to ensure the readability of these records throughout their retention life.

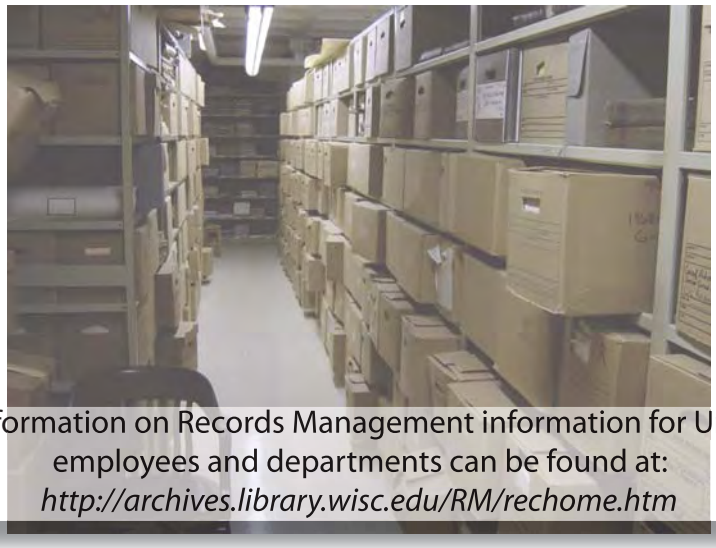
APPENDIX: University of Wisconsin–Madison Records Destruction Guidelines (contd.)

Guidelines: (contd.)

7. The Health Information and Portability and Accountability Act (HIPAA) contains specific requirements regarding the disposal of protected health information (PHI). See Chapter 8 of the ***University Health Information Privacy Manual*** at *http://www.provost.wisc.edu/hipaa/privacy manual/index.html*.

8. The requirement to destroy records also applies to records and information in electronic formats. The sale, donation, scrapping, or internal transfer of University computer equipment requires that all information on the device be deleted in accordance with accepted procedures prior to such sale, donation, or transfer. University records and information contained on storage media (such as floppy disks, CDs, DVDs, videotapes, audiotapes, etc.) must also be appropriately deleted and/or the media destroyed. These forms of storage media cannot be simply put in the trash or sent to Surplus With A Purpose (SWAP) without first being appropriately erased or otherwise evaluated for the deletion or rendering of the information undiscoverable.

9. University employees must have appropriate guidance and training about the appropriate management



More information on Records Management information for University employees and departments can be found at:
http://archives.library.wisc.edu/RM/rechome.htm

University Archives and
Records Management Services (ARMS)
B134 Memorial Library
728 State Street
Madison, WI 53706-1494
Phone: 608.262.5629
Fax: 608.265.2754
Email: recmgmt@library.wisc.edu
URL: http://archives.library.wisc.edu/