

# A CALL TO

---

*Technology has effectively made all of us records managers. This ARMS Bulletin describes how University employees can create accurate, reliable and complete electronic records.*

---

## CONTENTS

Introduction.....	1
Record Keeping Requirements.....	2
Rules of Evidence.....	3-4
Conclusion.....	4
Appendix.....	5

## INTRODUCTION— CREATING ELECTRONIC RECORDS

### A Brief Guide to Records and Information Management Planning Issues

Increasingly, offices are being encouraged to automate existing information systems—either to make them all electronic or to design new paperless processes or procedures. Reducing or eliminating paper is an admirable goal, but this goal alone should not drive decisions about system conversions. Storage medium issues should not govern the development or modification of information systems.

Further, business information systems frequently do not meet the requirements to be good record keeping systems. This is not to suggest that business information systems are necessarily deficient or bad. Rather, attention to record keeping requirements has not been married with the application of information technology. What is now being recognized is that information systems must be capable of creating good, legally reliable records. It is preferable and less expensive to address these issues while creating information systems, not after.

There are a myriad of things to consider in undertaking the development of information system projects. This guide is designed to provide a quick listing of policy and planning issues that need to be addressed. By providing this information to program managers, technology specialists, and others, we hope that some potential problem areas can be addressed up-front. Campus information systems are increasingly sophisticated and complex, and by paying attention to these issues early on in the system development process we can:

- Reduce legal and audit risks by insuring that data is accurate and reliable,
- Eliminate or reduce the need for expensive customization to incorporate records keeping requirements after the fact,
- Insure access to needed information in a timely fashion,
- Provide for the routine disposition of data when no longer needed, and
- Insure that University interests in records are protected and maintained.

Without attention to records keeping requirements up front, there is a real danger that:

- Incomplete records will be created and maintained,
- Data redundancy will increase,
- Responding to requests for information including Open Records Requests will become problematic,
- System security and issues will not be fully address, and
- The potential for legal liability will increase.

## RECORD KEEPING REQUIREMENTS

Creating original records in electronic systems calls for considering at least two major areas:

- Record Keeping Requirements
- Rules of Evidence

### A. What do we mean by record keeping requirements?

Record keeping requirements address those issues which will make the information created and/or maintained by your system legally acceptable and insure that your information will be accessible and retrievable in the future. These requirements apply regardless of storage medium (paper, electronic, microfilm etc.).

### B. What are the major considerations in developing record keeping requirements?

Formal system documentation should record and preserve decisions and policies on:

- Formulating the objectives of the record keeping system,
- Determining legal and regulatory requirements,
- Assigning and enforcing responsibility and accountability,
- Designing records capture or data collection protocols, and
- Assuring maintenance (current and future access and retrievability, retention, disposition, and preservation).

More specifically, the documentation should address:

**Formulating Objectives.** What is the information system supposed to do? What functions is it designed to support? What will constitute the official record(s) produced by the system?

**Determining Legal / Audit Requirements.** What information is legally required? For how long? Are there any specific state or federal requirements? Are there provisions for documenting changes made to the information system—providing an audit trail?

**Approval Authority / System Access Authority.** Is there a requirement for an authorizing signature? If so, how will it be obtained and recorded? Does providing access to the system inadvertently give approval authority? Is an electronic signature sufficient? (A signature is not required to create a record, but if a signature is a requirement of a governing policy or procedure, it may need to be somehow included in the electronic system.)

**Approval authority is an important consideration.** For example, in granting access to sign-on codes for data entry you may also be granting approval authority. Student and clerical staffs often are responsible for data entry, but should they bear the

burden of approval by virtue of the fact that they are completing a data entry task?

**Assigning and Enforcing Responsibility / Accountability.** Who will have custody of the official record? Who will be responsible for verifying information in the system? For making and documenting revisions? If, for example, your office envisions a Web page to support a particular function, who will be responsible for keeping it up to date with appropriate address information, revisions of content, changes in policy etc. Who will decide whether superseded versions need to be retained? Who will be responsible for assuring that short term and long term retrieval of the information is possible? Who will respond to auditors, to open records requests, or to the court?

**Designing Records Capture and Data Collection Protocols.** Data collection is a significant area because this is where you will decide what pieces of information will be coming from which sources, how that information will be validated, and the technology tools that will be used.

What data elements are you currently collecting? How are you collecting them? What is the best data collection tool to use? If you are going to use an electronic form, will you need to be able, later, to reproduce the form exactly as seen by client? (This last question could have important legal implications.) Do you intend to merge data collected from your form with an existing database? Will your system use E-mail or have an E-mail component? If so, how will you retain and manage that E-mail information?

**Assuring Retention / Disposition / Preservation.** Wisconsin Public Records Law requires that all records be governed by approved retention schedules. Retention schedules demonstrate that you have a plan to maintain your data in accordance with accepted requirements and that you have a mechanism to fulfill your administrative, audit, and legal obligations to the data. Further, it can be legally important to demonstrate that the data has been retained, destroyed / deleted, or preserved in the normal course of business. Ideally, the provisions of the records schedule (how long, in what form, and by whom the data need to be retained) must be incorporated into the systems design.

**Cost Effectiveness.** If these considerations are not taken into account during the development phase of an information system, the costs to fix the problems later on may be significantly higher.

## RULES OF EVIDENCE

<http://www.library.wisc.edu/libraries/Archives/rm/rechome.htm>

A. Coping with evidentiary requirements is of increasing concern as the University moves to all electronic information systems. Why? If you are subpoenaed to supply documents from an electronic information system in a court action, it is likely that you will not only have to supply the particular form, report, document, etc. in question, but in addition you may be required to document or to authenticate your information system.

1. What is the basis for admitting records into evidence?

The basis for admitting records into evidence is the Uniform Rules of Evidence. In Rule 1001 of Article X of the Rules, 'original record' as it relates to computer data is defined:

(3) *Original*: If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'

This means that in fact any readable output could be considered to be an original record. Whether or not your output will actually be *acceptable* as an original will depend on your being able to demonstrate one or more of the following:

- It was prepared in the normal course of business.
- The records have an independent business purpose.
- The records are complete, accurate and reliable.
- The records or output are required by law.
- The records or output were prepared with no motive to misrepresent or commit fraud.
- The records were prepared without foreseeing litigation.
- The records contain facts not opinion.

2. What determines what is an 'original record' in an electronic system?

This is one of the most frequently asked questions about managing electronic information. First, 'original record' should not be confused with public record. Wisconsin public records law defines public records very broadly: in essence just about everything that we as employees create and maintain can be considered public records. For information about Wisconsin's Public Records Law see the records management home page at

What is an 'original record'? The answer is, "it depends!" In complex information systems, determining what is an 'original record can be difficult. The best defense is the best offense in this instance, and explicitly designating what is 'original' and who is the 'holder of the original' should be a part of the policies or rules that are outlined up front. A very important practical consideration is that designating an official 'original' saves other offices from filling up their hard disks with duplicate information.

3. Is there a legal requirement to create a paper record?

No. Records can be in any medium, and there is no specific legal requirement that records must be in one medium versus another. The important thing to remember is that you need to demonstrate that your data are complete, accurate and reliable regardless of the particular medium.

### B. Applying Rules of Evidence to Electronic Information Systems

1. What are the implications of the rules of evidence for developing electronic information systems?

As mentioned earlier, if you are called in to court or asked to supply documentation from an electronic information system, you, or someone from your information systems staff, may not only have to provide the records but also evidence to authenticate the system that produced the records.

2. Why is it necessary to authenticate a system?

The contents of electronic systems can easily and rapidly be modified and/or deleted. While paper documents can also be modified, the ease and undetectability with which it can be done electronically means that information in systems without adequate safeguards can be suspect. In other words, the trustworthiness of the data in the system can be brought into question.

3. How do you authenticate an information system?

The following list should be considered when authenticating an information system. (All of these items should be addressed in the system documentation.)

**Reliability of the equipment.** Does the system include a log of operations which documents problems and system checks? Is there a policy for retaining the log?

**Integrity of the data.** Are there procedures for checking and verifying the data? Can their use be documented?

**Methods to prevent loss.** Does the system provide for an audit trail of revisions to the data as it moves through the process supported by the information system? Is the audit trail retained?

**Reliability of the computer programs.** You may be required to demonstrate the reliability of the software program, and you may have to provide the particular version of the program that was used to create / manipulate the data.

**Time and method for preparing outputs.** Much of the data in today's information systems remains online, but outputs are only prepared as needed. So even though the report or output is not regularly prepared, you need to demonstrate that the data is adequately maintained in the system.

## CONCLUSION

It cannot be too strongly recommended that the considerations discussed in this guide be included when developing systems specifications so that:

- The data in the proposed system can be safeguarded,
- The system will serve the needs of the campus unit, and
- The information will be admissible when evidence is needed to advance or defend University interests.

The Archives and Records Management staff would be happy to participate in planning phases or to discuss the issues presented in this document in more detail.

## APPENDIX

### PRACTICAL STEPS / SUGGESTIONS TO CREATING AND MAINTAINING ELECTRONIC RECORDS

1. Understand your department's business needs in creating records. In other words, ask "WHY?" Why is a particular set of records created and / or maintained by your department? Is it required? If so, by whom? Is there an administrative rule or procedure that requires a particular record? If yes, what does the rule specifically require? A large part of making records and information manageable is collecting and maintaining only what is needed in the first place.
2. What does your department need to document? Examine the functions that your department supports. The creation of records should support those functions. Any records falling outside the supported functions should be examined to determine how necessary they are.
3. If your department is converting an existing information system to a new technology, examine how the information was previously collected and maintained. What was good about the previous system? What did not work well? What forms were used? Remember to maintain important links so that you will have 'complete' records. For example, if your department previously maintained a hard copy case file to support a particular function, you will need to make sure that the individual pieces in that case file will be linked together via an index or other means so that you will have 'an accurate, complete, and reliable record.' Create an information flow chart if necessary.
4. Know your records retention requirements. Records retention requirements apply regardless of storage media. For example, if the retention requirement was 5 years and destroy when the record was in paper form, the same retention applies to the electronic record.
5. Investigate technology alternatives carefully. What are your objectives in creating and maintaining your records electronically? Will you generate forms electronically? Will you need to have an electronic forms package? Is workflow needed to be able to share records and information? Check the campus information architecture homepage for latest standards and guidance on particular technologies.
6. Maintain a file guide / index. In the not too distant past, office maintained file guides. They provided 'a finding aid' to the office records. This type of document is taking on increased significance in the electronic environment. The file guide or index can be critical in locating information when it is needed quickly. The file guide should include: inventory of all official records maintained by your department, who has responsibility for each, and what type of software they are maintained in.
7. Communicate and coordinate your records needs with your office information technology staff. They represent key players in making sure that your information is accessible and available when you need it. They can guide you in making choices about electronic records that will meet technical capabilities of your department or indicate where deficiencies exist. Most importantly, make sure they are aware of records retention and access needs.
8. Know your office data backup routine. What is backed up when? Where are backups maintained? This can be critical in a disaster situation.
9. Remember your records users. The reason that we create and maintain records and information is to serve a purpose and so they will be used. Who uses your department records? How do they use them? What types of reports are routinely generated? Are they serving a purpose? Communicate planned changes to all users.
10. Choose a storage medium carefully. Remember the availability of hardware and software will be critical pieces to accessing records in the future. Will they be available and supportable for the life of your records?
11. Develop standards records practices for your office. This suggestion goes hand in hand with the suggestion to maintain an office information guide. For example, determine what spreadsheet package will be used. This will greatly facilitate office information sharing and ease of communication.
12. Consult with ARMS. Records and information are critical University assets. Managing them carefully protects University interests, saves money, and will assist your department in meeting its mission.

**Archives and Records Management Services**

**Main Office**

**B134 Memorial Library**

**728 State Street**

**Madison, WI 53706-1494**

**Phone: (608) 262-5629**

**Fax: (608) 265-2754**

**[Recmgmt@library.wisc.edu](mailto:Recmgmt@library.wisc.edu)**

**[www.library.wisc.edu/libraries/Archives/](http://www.library.wisc.edu/libraries/Archives/)**

©1998, Board of Regents, University of Wisconsin-Madison  
ARMS is a periodical bulletin from the University of  
Wisconsin-Madison's Archives and Records  
Management Services.