



Town of Burlington
29 Center Street
Burlington, MA 01803

Office of the Town Clerk, Archives Division

Phone 781.270.1604/1660
Fax 781.270.1608
www.burlington.org/archives
archives@burlmass.org

Jane L. Chew, CMC, Town Clerk
Eleanor M. Gelinas, CMC, Asst. Town Clerk

Lisa A. Plato, CA
Archivist/Records Manager

Records Management Guide #3 Legal Acceptance of Records in an Electronic Environment

Excerpted from *State Government Records Management Information Series: Guidelines for the Legal Acceptance of Public Records in an Emerging Environment* (Albany, New York: University of the State of New York, State Education Department, 1994) and Donald Skupsky, *Legal Requirements for Records Management and Information Systems* (March 12, 1999 presentation in Boston, Mass.)

1. Introduction

New information technologies enable us to reduce records creation and storage costs, but they also pose issues for authenticity. In modern times, courts have admitted records into evidence when they meet specific criteria for admissibility and legal acceptance. Exceptions to the hearsay rule for public records are based on the presumption that public records reflect accurate information produced by trustworthy procedures. As we review and modernize recordkeeping practices, we must ensure that we are producing records that are reliable, complete, and accurate for legal, audit, and other purposes.

Under existing Federal rules of evidence, we can use records produced by automated information systems to meet recordkeeping requirements—provided that records are created in the normal course of business and their authenticity and reliability can be established. Establishing the authenticity and reliability of records depends on the accuracy of the process or system used to produce the record, the source of the information used to produce the record, the source of the information in the record, and the method and time of its preparation. Problems may arise if appropriate procedures are not followed in creating and maintaining records, making it difficult to lay a proper foundation for admissibility.

This guide will discuss:

- Admissibility and rules of evidence
- Evidentiary requirements for audits
- Requirements for legal acceptance of records in an electronic environment

2. Admissibility as Evidence in Legal Proceedings

Admissibility refers to a court's willingness to accept records as evidence in legal proceedings. Modern rules of evidence¹ address two principle objections to the admissibility of records into evidence. The hearsay rule prohibits the admissibility of any out-of-court statements to prove the truth of a matter. The best evidence rule precludes the admissibility of anything other than an original writing, barring an acceptable reason for the absence of the original. Neither rule is meant to preclude evidence that can be proven necessary and reliable. Federal rules of evidence provide exceptions for overcoming the hearsay and best evidence objections based on circumstantial proof of reliability and trustworthiness. These exceptions contain the specific legal requirements for admitting records into evidence.

¹ In Massachusetts, applicable laws include: Uniform Business Records Act (UBRA); Uniform Rules of Evidence (URE); and Uniform Photocopies of Business and Public Requirements as Evidence Act (UPA).

Records are generally considered trustworthy if they are created in the normal course of business. Records created to support typical business activities, e.g., the regular course of operations, are much more inherently reliable than those produced especially for litigation. Creating records in the normal course of business does not limit one to a cyclical schedule e.g., daily, weekly, or monthly. Records can be created as part of the regular program, but at irregular times e.g., special audit reports.

Under Federal rules of evidence, original and duplicate records are admissible provided that a proper foundation is laid. Reproductions of original records must be produced in the regular course of business by a process which accurately reproduces the content of the records. Newer information technologies are generally subject to greater scrutiny until experience and widespread use establish their reliability. That does not mean we cannot use them, but we must pay attention to the design and documentation process.

Before a document can be received into evidence, it must be shown that the document is what it purports to be; that is, it must be properly authenticated.

3. Evidentiary Requirements for Audits

Accurate, reliable, and trustworthy records are the cornerstones of effective programs for audit and accountability. Audits are performed periodically by expert, independent, and objective audit professionals; the process confirms that the system or process produces accurate results. Audits should be performed by persons other than those who created the records or who have an interest in their content, such as electronic data processing (EDP) auditors or outside independent auditing firms.

Although many audits address financial and program issues rather than the accuracy of information systems, almost all audits use records that originate from information systems. Because auditors must concern themselves with the relevance, validity, and sufficiency of evidentiary matters, the accuracy of records and the reliability of the systems that produced them come into question during the course of most audits. With the increasing complexity of government operations and the introduction of new technologies, the accuracy of information systems is becoming a pervasive audit concern that is no longer limited to the special area of EDP audit.

The rules of evidence contain special provisions for establishing the authenticity and reliability of records, stressing the sources of information, method, and time of preparation. The best evidence is not dependent on a specifically sanctioned technology used to create a record, but on showing that the record was the result of a process or system that accurately produced it. In establishing the authenticity of records, we must be able to demonstrate in court the trustworthiness of the system used to produce the records. The records custodian may be required to testify about the operation of the system. In some cases, the opposing parties or the court may inspect the system.

In establishing the authenticity of records, agencies should focus on the reliability and accuracy of the systems and processes that produce the records rather than on any innate characteristic of their format or medium. This is established by:

- Policies and procedures defining development, maintenance, and use of the system
- Training and support programs that ensure staff understanding of policies and procedures
- Controls that monitor the accuracy and authenticity of data, the reliability of hardware and software, and the integrity and security of the system

4. Requirements for Legal Acceptance of Records

A. General Characteristics of a System or Process

Legal acceptance of records requires proof that the process or system is reliable and hence capable of producing trustworthy records. Records will be more readily accepted as trustworthy if an agency can demonstrate that the system that produced them:

- Operated to support a business function and produced the records as part of that function
- Created accurate records
- Produced records in a timely manner, or produced records after the fact where the time lapse between an event and the creation of a record had no effect on its content.

B. Produce Written Policies and Procedures

The trustworthiness of an agency's records may be judged by the adequacy of existing procedures and how closely they are followed. Policies and procedures should define normal operations for development, maintenance, and use of information systems. Written policies and procedures for each system should:

- Describe the methods used to create, modify, duplicate, and destroy records
- Define the roles and responsibilities of the individuals involved in record creation, maintenance, and destruction
- Provide for consistent quality control, problem resolution, and other activities that might otherwise be subject to inconsistent action or misinterpretation
- Demonstrate the purpose and uses of the system
- Be kept up-to-date and readily available

Courts may scrutinize deviations from established procedures, especially if deviations are from legally-required procedures.

C. Provide Training and Support

Formal training and support programs help ensure that policies and procedures are understood and implemented by staff. Operation logs and help desk (trouble) reports document that problems were quickly identified, attended to, and resolved. If the department can demonstrate that staff knew what procedures to follow and were overseen and supported by responsible staff, it can also show a court or other outside parties that procedures were most likely followed. It is advisable to keep records of attendance at training sessions and certification of training.

D. Develop Adequate System Controls

Effective recordkeeping systems, whether manual or automated, need mechanisms and controls to ensure the quality and reliability of the records they produce. Controls monitor input and output processes, hardware and software performance, and security.

E. Develop and Implement System Audit Trails

Audit trails document who use the system, when they used it, what they did, and what were the results.

Effective audit trails can automatically detect who had access to the system, whether staff followed certain procedures, or whether fraud or unauthorized acts occurred or might be suspected in the system. Properly implemented audit trails track:

- Any changes to data in a system, including the creation, modification, or deletion of records
- Date and time of changes
- Source of any changes

There are an increasing number of tools available for maintaining system audit trails. Software is available for keystroke monitoring, time and date stamping, virus detection and other controls that can be built in the design of systems. Additional mechanisms should be established to document any changes to data, and any

changes to the software and programs used to process the data that might not be recorded by a system's online audit trail procedures e.g., batch updates and migrations.

F. Conduct Routine Tests of System Performance

Automated information systems rely on system audits and routine testing to verify the accuracy and validity of data. Tests of system performance, conducted on a routine basis, provide necessary oversight to verify the integrity of a system. The design and use of system edits and performance tests should be documented, because the reliability of records produced by the system depends on the accuracy and reliability of the programs and procedures used to create, modify, and retrieve them.

G. Test and Document the Reliability of Hardware and Software

The reliability of hardware and software affects the authenticity and admissibility of records. Because equipment which is not functioning properly can alter the content of computer records, the reliability of the equipment used to store and produce the records may be challenged. One can enhance the acceptance of computer-generated records if they:

- Routinely test hardware and software according to a plan developed with the advice of the manufacturer
- Retain all documentation related to hardware and software procurement, installation, and maintenance
- Maintain operation logs and run schedules to document the reliability of system operation and performance.

The department may also be required to provide individuals who can testify about testing and dependability of hardware and software.

H. Provide Adequate Security

- System developers should develop routines that limit access and update privileges to the appropriate staff and prevent unauthorized modification of data. Such provisions must be documented so they can be used to attest to the credibility and trustworthiness of the system.
- Security is enhanced if staff duties are divided so that individuals with an interest in the contents of records are not responsible for administering system security, quality control, audit, or other tasks where the integrity of a system can be compromised or called into question.
- Disaster preparedness plans and security backup procedures will ensure that records are protected against inadvertent or accidental loss or destruction.
- Document the use of backup procedures to restore a system or recover records, especially if backup procedures were used to generate a record.

I. Establish Controls for Accuracy and Timeliness of Input and Output

The processes used for data entry and output must produce accurate and timely records. Input can be challenged on any of the following grounds:

- Manner in which data was entered into the system initially
- Whether the data was entered in the regular course of operations
- Whether data was entered within a reasonable time after the events were recorded
- Adequacy of measures taken to ensure accuracy of the data

You can enhance the accuracy and reliability of records generated through processes that involve input and output by taking the following measures:

- Develop and follow systematic procedures for data entry
- Design, implement, and document quality control procedures
- Identify all input and output documents and procedures in the system documentation

- Attest to the accuracy and validity of records at the time they are created or updated
- Document any delays in data entry by recording the date the original source documents were created and the date the data was entered. Keep records of any unusual delays in producing output
- Retain specially written programs used for extracting data from the system
- Produce labels for media contain electronic records. Labels should identify the exact title (including the name of the system), creating department/program unit, date, purpose, source, and destination of the records.

J. Create and Maintain Comprehensive System Documentation

Documentation of a system provides verification of the processes used to produce records. Proper documentation preserves information, independent of the individuals involved, on all aspects of system design, implementation, maintenance, and oversight. It also demonstrates the existence and proper operation of system controls which ensure that records are accurate, reliable, and authentic.

Documentation:

- Should be comprehensive, covering all components of an information system and should demonstrate all steps from the beginning to the end of the process
- Should be produced during the design of the system; if a system was implemented without it, documentation should be prepared immediately
- Must be accurate
- Prepared and maintained by knowledgeable staff
- Should be clear and concise so that current and future employees can testify on its behalf
- Should be current and immediate available if needed for court proceedings or other purposes
- Should be kept for the full retention period of any records produced by the system
- Should describe how the system operated and delineate the meaning, purpose, structure, logical relationships, and origins of data

Courts may request program documentation that shows:

- How the system operates
- Training documentation demonstrating the distribution of written instructions
- Course materials, attendance of individuals at training sessions, remedial or refresher training programs, and certification of training completed
- Actual audit trail records demonstrating the activities that occurred in the system
- Evidence that procedures were followed.

In addition, individuals familiar with the operation of the system may be asked to testify.

K. Retain Sufficient Documentation

Documentation should be kept for at least the same period as the records produced by the system. When a system is modified or replaced, older versions of the documentation should be kept for as long as any records created by the system. Procedures for migration or conversion of records to a new system should be fully documented. Destruction, deletion, or other disposal of documentation must be conducted in accordance with record retention schedules.