Back to Table of Contents

LEGAL ASPECTS OF ELECTRONIC RECORDS

Legal standards, for the acceptability of records other than paper records as evidence, have been slow to evolve. State and federal historical legislation, which allowed for the admissibility of microfilm as evidence, had to gradually develop. Paper copies of microfilmed records are admissible if microfilm is created with proper certification and standardized procedures.

Additionally, precedent has shown that if a government agency, in the regular course of business, has recorded, copied, or reproduced by any photographic or other process which accurately reproduces the original, the original may be destroyed in the regular course of business. The reproduction, when satisfactorily identified, is as admissible in evidence as the original itself in any judicial or administrative proceeding whether the original is in existence or not. (See also "Legal Guidance" earlier in this Handbook.)

ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES

Electronic records satisfy requirements for written materials so that the enforceability of a record or signature cannot be denied simply because it is electronic form. Electronic records must still satisfy any other formal requirements, such as notices, disclosures or completeness of terms. For example, if the parties' e-mails show agreement on the sale of widgets, these electronic records would still need a quantity term to create a valid contract. Electronic records and signatures simply satisfy requirements under existing law, such as the statute of frauds that require documents be in signed writing. An electronic signature is defined as:

"Electronic signature means an electric sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record."

One specific type of electronic signature is called a digital signature. The term "digital signature" is often used to denote the use of encryption technology to enable a computer user to transmit secure communication over the internet or through any other open or closed network with a signature that has the same legal force and effect as a traditional handwritten signature on paper. The security features of a digital signature allow networked communications to be authenticated, confidential, and nonrepudiable.

The Electronic Signature in Global and National Commerce Act and the Uniform Electronic Transaction Act

Electronic signatures have been incorporated as part of the Federal law as the “Electronic Signature in Global and National Commerce Act (ESGNCA);" and “The Uniform Electronic Transaction Act (UETA); the California Public Records Act, Section 6250; and Section 1633 of the California Civil Code.

The Electronic Signature in Global and National Commerce Act (ESGNCA)

On June 30, 2000, the President of the United States signed the "Electronic Signatures in Global and National Commerce Act" establishing the validity of electronic signatures for interstate and international commerce. After signing the bill with pen and ink (still required for legislation), the President also signed it electronically.

The Act is an important piece of legislation. It is cautious and conservative in that it lets the market make the important decisions about electronic signatures and about the infrastructure required to use and trust them. The focus on the market rather than legislation as the primary force to shape the use of electronic signatures has important implications for managers of businesses that might use such signatures.

Rather than simply understanding the law, business managers also need to understand the risks and benefits associated with electronic signatures. They need to be able to identify the key capabilities that they need to put in place in order to prevent fraud and to reduce the potentially significant liabilities associated with uninformed use of electronic signatures. Most important, they need to be able to make judgments about when the use of electronic signatures makes business sense.

Uniform Electronic Transaction Act (UETA)

The State of California enacted the UETA on September 16, 1999 under the 1999 California Senate Bill 820**.** California's version differs from the National Conference of Commissioners on Uniform State Law's (NCCUSL) UETA by adding provisions under the "use of electronic records and electronic signatures" section, the "notarization and acknowledgment" section, as well as the "time and place of sending and receipt" section. Additionally, California's version of UETA eliminates sections 16-20 of the NCCUSL version that relate to transferable records and the use of electronic records by governmental agencies.

With the provisions of the UETA becoming effective January 1, 2000, the UETA is substantially the same form as the ESGNCA that became effective October 1, 2000. The

UETA's limited objective is to place electronic documents and the use of electronic signatures on a par with traditional paper-based transactions and the use of manual signatures. It is intended to eliminate any doubt about the enforceability of electronic transactions, and thereby remove barriers to their use in the business, public, and government sectors.

UETA recognizes and authorizes the conduct of business, public and governmental affairs using electronic means. The UETA applies to "electronic records and electronic signatures relating to transactions." It defines electronic record as *"a record created, generated, sent, communicated, received, or stored by electronic means."*

The UETA applies to all the electronic records and signatures related to a transaction, and would cover e-mails, reports, memoranda, accounting records, or other electronic documents prepared in connection with a transaction.

Some of the more significant provisions of the UETA are:

- A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

- A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

- If a law requires a record to be in writing, an electronic record satisfies the law.

- If a law requires a signature, an electronic signature satisfies the law.

In summary, the UETA applies to transactions that the parties have agreed to conduct electronically. Under most circumstances, electronic records and electronic signatures may now be used in place of traditional paper-based and handwritten methods. In the area of records retention, electronic records may replace other methods so long as there is assurance the electronic records will provide the accuracy, integrity, and accessibility of traditional methods of retention. For more information on the UETA, please see Appendix 10, Overview of the Uniform Electronic Transaction Act.

Electronic Records as Evidence

Electronic records as a group involves a much newer medium than paper or microfilm. Precedent has also shown some courts, admitted records with a variety of contents and forms. Each judge is free to dismiss evidence on the basis of the court's independent evaluation of the authenticity of a given document.

The court must believe that records admitted before it, are "trustworthy" that is, they must clearly and accurately relate the facts as originally presented in summary form.

In contrast to traditional paper records, electronic records have systemic vulnerabilities and additional efforts must be taken to assure the court of their trustworthiness. Hence, an electronic recordskeeping system incorporates the functionality to assure the court of the reliability of the recordskeeping integrity. For the mini and mainframe environments, attention to the following items will enhance record trustworthiness:

- Equipment and software reliability.
- Preparing printouts in the regular course of business.
- Records retention schedule.

Equipment and Software Reliability

Since the content of a record may change if the equipment is not working properly, an organization may be required to present evidence that its equipment was operating reliably on the day the computer record was prepared.

A computer operations log indicating the absence of any malfunctions is generally adequate. Errors in computer records can also result from errors in computer programs. An organization may be required to present evidence related to the development and testing of programs. An expert witness to determine its accuracy or reliability often examines programs. An organization may be required to present the specific version of the computer program used to process the data or manage the electronic document being entered into evidence.

A different version of the program may be considered if it is the only one available, but the absence of the exact version may raise serious questions on the trustworthiness of the computer records.

Preparing Printouts

Computer printouts prepared in the ordinary course of business activity are perceived to have higher trustworthiness than similar computer printouts prepared for trial. However,

if the organization can show an adequate audit trail leading to data creation and merely a time lag before printing, the acceptability of the printouts is improved.

Records Retention Schedule

An approved records retention schedule can have a profound impact on court proceedings because the schedule establishes a retention period and specified disposition time.

Although an approved retention schedule for a record requested does not guarantee the court's acceptance of it, the fact that a record is scheduled definitely helps meet the requirement of a record being created as a "regular practice" of the agency. Courts also accept the defense that records have been disposed of under an approved records retention schedule.

Electronic recordskeeping systems incorporate the ability to associate a specific electronic document (as part of a specific record) with a specific electronic retention schedule providing further assurance of the link between the retention policy and the disposition of the specific record in question.

Courts have imposed penalties on entities that failed to have current records retention schedules or failed to follow established procedures to manage and safeguard records properly. Dismissal of cases, fines and sanctions has been imposed for failure to produce required records. If records are willfully withheld or the entity cannot demonstrate a good faith effort to find them, in some extreme cases criminal sanctions have been imposed.

ELECTRONIC MAIL

Electronic mail systems, commonly called e-mail, are becoming the communications method of choice for many public officials and public employees. E-mail messages are often used as communication substitutes for the telephone as well as to communicate substantive information previously committed to paper and transmitted by more traditional methods. This combination of communication and record creation/keeping has created ambiguities on the status of e-mail messages as records.

The management of e-mail systems touches nearly all functions for which a government agency is dependent on recordskeeping: privacy, administration, vital records management, administrative security, auditing, access, and archives. The need to manage e-mail messages and systems properly is the same as for other records keeping systems--to ensure compliance with California laws concerning the creation of, retention of, and access to public records.

Government agencies that use electronic mail have an obligation to make employees aware that e-mail messages must be retained and destroyed according to established records management procedures. Agencies should set up or modify e-mail systems to facilitate electronic records management. Procedures and system configurations will vary according to the agency's needs and the particular hardware and software in place.

Definitions

E-mail **systems** are store-and-deliver software systems that transport messages from one computer user to another. E-mail systems range in scope and size from a local area network e-mail system that shuffles messages to users within an agency or office; to a wide area network e-mail system that carries messages to users in various physical locations; to Internet e-mail that allows users to send and receive messages from other Internet users around the world.

E-mail **messages** are electronic documents created and sent or received by a computer system. This definition applies to the contents of the communication, the transactional information, and any attachments associated with such communication. Thus, e-mail messages are similar to other forms of communicated messages, such as correspondence, memoranda, and circular letters.

Record Management Concerns

Government Code Section 14741 provides the following:

"Record(s)" means all paper, maps, exhibits, magnetic or paper tapes, photographic films and prints, and other documents produced, received, owned or used by an agency, regardless of media, physical form or characteristics."

An e-mail message is a document produced, received, owned or used by an agency. Whether the e-mail serves to document the organization, functions, policies, decisions, procedures, operations or other activities is the deciding factor as to its status as a record. This is true of any communication, whether electronic or paper.

E-mail messages that meet the criteria of the definition of a record must be scheduled and retained for the appropriate time period before disposition. E-mail messages that meet the criteria of the definition of a record may be considered public records and must be available to the public

As with any format, an e-mail message is considered a public record unless it falls under one or more exclusions such as individual rights to privacy. These records must be maintained and made accessible to the public upon request through the appropriate requesting process, i.e., Public Records Act.

Retention and Scheduling Requirements

E-mail itself is not considered a record series or category. It is a means of transmission of messages or information. Like paper (mail) or microfilm, e-mail is the medium by which this type of record is transmitted. Just as an agency cannot schedule all paper or microfilm records together under a single retention period, an agency cannot simply schedule e-mail as a record series.

Retention or disposition of e-mail messages must be related to the information they contain or the purpose they serve. The content, transactional information, and any attachments associated with the message are considered a record (if they meet the agency's record management plan criteria). The content of e-mail messages may vary considerably, and therefore, this content must be evaluated to determine the length of time the message must be retained.

One of the difficulties with e-mail is arbitrary size limits on e-mail user "mail boxes" which require users to purge or archive files or be restricted in their use of the system until the mail boxes are kept below the size limit. This may contribute to improper deletion of e-mails that are records. Education of Information Technology professionals on the records implications and proper training of personnel can ensure good records management procedures are followed. Use of an electronic recordskeeping system also helps to manage this increasing source of records.

NOTE: Simply backing up the e-mail system onto tapes or other media or purging all messages after a set amount of time are not appropriate strategies for managing e-mail.

For more information on records management, contact your agency's records management analyst/manager or the DGS Records Management Program.

Guidelines and Best Practices for Managing E-Mail

Record Copy E-mail

E-mail users should be aware that e-mail messages are often widely distributed to a number of various recipients. Determining which individual maintains the record copy of the message, i.e., the original message that must be retained per the retention schedule, is vital to e-mail management. If the holder of the record copy is not identified and aware of his/her responsibility, the agency may find that no one retains the message or that everyone retains the message. Neither of these scenarios is appropriate.

For example, in the absence of an electronic recordskeeping system, agency policy documents which are transmitted to multiple recipients via an e-mail system, need not be maintained by each recipient beyond his or her need for this information, if the record copy responsibility is established so that the record is maintained by some office or agent for its established retention period. In this example, a logical record copy responsibility rests with the creator of the policy document. Prompt deletion of duplicate copies of e-mail messages from an e-mail system makes the system as a whole much easier to manage and reduces disk space consumed by redundant information. Another technique to avoid proliferation of duplicate copies is to use e-mail to notify readers of a document that is then accessed by the user going to a shared drive or other source, or by providing a link to the document. The document can then can be managed in one location.

This example, however, becomes increasingly difficult to manage as the electronic records grow in volume and diversity. An electronic recordskeeping system keeps track of the originator, disposition, and relationships to other documents within the record.

NOTE: *Generally speaking, the individual who sends an e-mail message should only maintain the record copy of the message under the control of the electronic recordskeeping system.*

Filing

E-mail messages should be filed in a way that enhances their accessibility and that facilitates records management tasks. Agencies should set up or modify e-mail systems to facilitate records management and appropriate filing systems. Procedures and systems configurations will vary according to the agency's needs and the particular hardware and

software in use, but electronic recordskeeping systems must conform to the DGS "Specifications for Electronic Record Management Software."

NOTE: Employees should be responsible for classifying messages they send or receive according to content, the agency's file classification scheme and established records series.

Distribution Lists

If you send to a "distribution list" (not a listserve, but a specified list of individuals), you must also keep a copy of the members of that list for as long as you are required to keep the message itself. It is of little value to know that the "Security Alert!" notice went to "Swat Team 7," without knowing whether Arnold S. or Judy F. received the message. Nicknames present a similar problem.

Subject Lines

Fill in the subject line on your e-mail both to help your recipient identify and file messages, and to help you file your SENT ITEMS box messages that must be retained for some period. Subject lines should be as descriptive as possible.

Following are some examples of poor and good subject lines for the same message:

Poor or confusing subject lines	Better, descriptive subject lines
"Helpful Info"	"Contact Info"
"Report"	"Quarterly Financial Report"
"Minutes"	"January 2001 Board Minutes"
"Important"	"Revised Admin. Procedures"
"News"	"New Agency Head Appointed"
“Contract Status”	“PO 12345 Delivery Status”

Storage of E-mail

We recommend that agencies explore retaining records from an e-mail system in a central repository managed by an electronic recordskeeping system within on-line storage.

E-mail Messages and the Rules of Evidence

Agency personnel should be familiar with both state and federal "rules of evidence" requirements. For records maintained in electronic information systems, including e-mail systems, courts concentrate on assurances that records, and the systems in which the records are created and maintained, are reliable. The reliability of the process or system used to produce records, not the type of media or technology used, determines the admissibility of records in evidence. Moreover, the federal rules of evidence place the burden for the identification of relevant records on the record creator, and within a reasonable time period.

At a minimum, agency personnel should ensure the following:

- E-mail systems used to create, receive and maintain e-mail messages have full, complete, and up-to-date systems documentation
- E-mail systems follow all recommendations for system security
- Complete systems backups are regularly and consistently performed
- E-mail system should retain all data and audit trails necessary to prove its reliability as part of the normal course of agency business
- The record copy of a message is identified and maintained appropriately
- Backup procedures should be coordinated with disposition actions (within the established methodology) so that no copies of records are maintained after the retention period for the records has expired

Again, agency records managers need to plan for records maintenance and record copy responsibilities for the records system to meet requirements for reliability and legal records disposition. Close coordination with information technology professionals is needed.

NOTE: The e-mail system should allow the server administrator to prevent destruction of records for legal and/or audit purposes.

Access

A major challenge for agency records managers is to guarantee that records maintained in electronic information systems are accessible and usable for the entire length of the retention period. Rapid changes and enhancements to both hardware and software compound this challenge. As many e-mail systems have limitations in storage space that cause operational problems when messages are stored in the system beyond a specific period (such as sixty or ninety days), procedures must be in place to transfer records from the e-mail system to another electronic recordskeeping system to meet retention requirements.

NOTE: Messages should be maintained in a format that preserves contextual information (metadata) and that facilitates retrieval and access. The system should allow deletion of messages once their retention periods expire.

Beyond this generic challenge of technology change, there are more mundane, but equally critical steps that must be in place to ensure that records created by e-mail systems can be located and retrieved when required. A central step is a system of standardized naming conventions and filing rules within the e-mail systems.

E-mail messages should be indexed in an organized and consistent pattern reflecting the ways in which records are used and referenced. Records maintained electronically, including e-mail messages, have an advantage over conventional "hard copy" document filing systems in that indexing for multiple access points is relatively simple and inexpensive, provided an effective indexing framework is in place.

Planning records indexing and retrieval points is time well spent. Unnecessary time needed to retrieve electronic records is not productive staff time, and is an annoyance to the public as well.

Messages should be stored in a logical filing system that is searchable by multiple data elements.

Responsibility

Roles and responsibilities of agency personnel should be clearly defined. Employees must understand and carry out their role in records management and agencies must ensure compliance with agency procedures and California law. Unauthorized users should not be able to access, modify, destroy or distribute records.

Agency administrators, individual agency employees, records managers, information technology managers and server administrators have different responsibilities in managing electronic records. Agencies should clearly identify the roles of each; adopt procedures, train staff and monitor compliance on a regular basis. The creator or recipient should make decisions regarding messages. The agency should take appropriate measures to preserve data integrity, confidentiality and physical security of e-mail records.

FINAL DISPOSITION OF RECORDS

Final disposition is the last stage in the life cycle of records, when they no longer serve a useful purpose for agency business. At this point, identified records may be destroyed or transferred to the California State Archives for permanent preservation.

Records Destruction and Services

The objective of records destruction is to remove the record permanently from possible use after it has become obsolete and to ensure that sensitive or confidential information does not become public. Because destroyed records cannot be recalled, extra care should be taken before records destruction. All statutory requirements must be satisfied.

Final disposition of state records must be according to an approved STD Form 73, Records Retention Schedule, and a properly prepared STD Form 71, Records Transfer List. See the Records Retention Handbook for general procedures for the destruction of records. All destruction procedures described apply to the record (official) copy. Convenience or reference copies should be disposed of as soon as they are no longer needed. In some instances, convenience copies could be confidential and must be destroyed in accordance with the prescribing directives.

Within the State Records Center, the Document Destruction Center operation facilitates the destruction of confidential microfilm, microfiche, computer cassettes, computer tapes as well as the traditional paper. An on-sight shredding process is provided and overseen by authorized state personnel. Appointments can be scheduled for "witness" destruction, if so required, at no extra cost.

Archival Preservation and Processing Requirements

The California State Archives "flags" developed records retention schedules as part of California's State Records Management Program approval process that their staff wishes to review. The "flag" identifies potential archival, historical, research, or uniquely significant electronic records that are important to the State of California. The final disposition of these electronic records must be coordinated with, and transferred to the California State Archives. State agencies are responsible for coordinating and ensuring the proper transfer of these electronic records.

Because of the variety of formats of electronic records, issues of proprietary software and specialized hardware, decisions must be made in consultation with California State Archives, as to whether to transfer the records or maintain them in the agency of origin. If a transfer decision is made, the method, frequency, and format of the transfer must be determined cooperatively by the agency and California State Archives.

Timing of the actual physical transfer of electronic records should be determined through the records retention schedule process. California State Archives must be involved early in the process to ensure the archival requirements are met. Special preservation measures are often required to preserve electronic records.

Electronic records may require conversion to a medium and format suitable to ensure long-term access and readability. All appropriate system documentation must accompany the transfer of electronic records. A computer database without minimum documentation is useless because the contents cannot be read or interpreted.

Electronic records containing information will, like other records containing confidential information be under the same restrictions in the State Archives as they are in the agency of origin. Transfer to California State Archives does not affect the statutory restrictions on access to confidential information.

Also, the courts have determined that e-mail in its native format may be a record and must be managed appropriately. Electronic records are stored on a variety of media, such as magnetic tapes, disks, video files and optical disks. Remember, it is not the medium that is the primary factor for determining potential archival preservation--it is the "records series" itself.

Procedures for Purging Files

Written procedures should be developed for the purging and disposition of electronic records after the retention period is complete. Depending on the volume of records and the staffing situation of the agency, purging of files can be performed on a monthly, quarterly, semi-annual, or annual basis. For electronic records, procedures for purging of records should be performed within the electronic recordskeeping system.

The Records Management Program recommends that the agency maintain a disposition log. This log reflects the records series titles, dates covered, volume, and date of final

disposition. The electronic recordskeeping system software will provide an audit disposition log.

Responsibility for Approving Disposition

Written procedures or designated authorization should verify who has responsibility and authority for approving final disposition of records.

- If the agency has a current STD Forms 72, Records Retention Schedule Approval Request, which is signed by both the program manager (or person authorized to sign for the program manager) directly responsible for the records listed on the STD Form 73, Records Retention Schedule, and the Records Management Analyst and/or Manager and the Department of General Services, the disposition of all the records series as listed is authorized.

- If a records series is not listed on the approved STD Form 73, the agency must amend the STD Form 73 appropriately to dispose of that records series. A records series can also be added to the schedule for approval by amending again the STD Form 73. The details of the process to develop and update the agency records retention schedule are discussed in the Records Retention Handbook.

- If there is not an approved records retention schedule, the agency must submit both the STD Forms 72 and 73 and have them approved before final disposition is authorized. Steps for processing the STD Forms 72 and 73 are again listed in the Records Retention Handbook.

Disposition of Magnetic Media

Electronic records are usually stored on erasable, reusable, fragile and relatively inexpensive media. The data on this media are easy to revise and update. For these reasons, the disposition of electronic records should be determined as early as possible when they are no longer needed for state business.

Diskettes that contain sensitive or confidential electronic records should not be discarded in regular waste containers. They should be cleared by degaussing (a method of electromagnetic erasure) and reused, or use a software utility that conforms to the Department of Defense's requirements (DoD 5220.22-M), which is to overwrite all addressable locations with a character, or rendered useless by shredding. Data scrambling programs are also available as a means of making the file's data permanently unavailable. The same methods apply to hard drives except if not degaussed or reformatted by the use of above mentioned software utility, they should be rendered useless by complete destruction.

These specific precautions are required for confidential information because many computer operating systems do not actually erase the entire file when files are "deleted." They simply remove the file's name from the system directory. This allows the space occupied by the file to be declared available for a new file. The electronic records remain unchanged until that portion of the disk is reused. Consequently, "deleted" electronic records files may be recovered by using commercially available utility programs.

NOTE: For active or current records within an electronic recordskeeping system it is acceptable for authorized personnel to "delete" files, consistent with security, and then simply reuse the space on the magnetic media for new information. The recordskeeping system will preserve an audit trail regarding record disposition.

SUMMARY - WHY ELECTRONIC RECORDSKEEPING?

When properly employed, electronic recordskeeping is an efficient tool for managing the entire record, across many media, because of the unique characteristics (i.e., volatility, metadata, etc.) of electronic records and the complexity of their use. An even more thoughtful application of sound records management principles needs to be given electronic record creation, maintenance, and final disposition.

To have an effective electronic records management program, the agency Records Management Analyst and/or Manager--in cooperation with administrative, professional, technical, and administrative support staff must:

- Establish the necessary program elements to manage all records using electronic recordskeeping.
- Use the electronic recordskeeping systems to provide an up-to-date records inventory.
- Make the decisions necessary for developing the agency records retention schedule.
- Organize electronic files to maximize their usefulness.
- Implement security measures to protect electronic information.
- Cooperate with the California State Archives to preserve the State's historical heritage.
- Apply the approved retention schedule and agency procedures to dispose of obsolete electronic records.

A FINAL COMMENT

Agencies are encouraged to contact staff at CalRIM, State Records Program, Department of General Services with any concerns regarding the management of electronic records. We trust that this Handbook will prove helpful in developing and improving effective electronic records management in all state agencies. As standards for electronic recordskeeping systems and procedures for their management continue to develop, the State of California Records Management Program will provide further information and guidelines to state agencies.

Back to Table of Contents