
RECORDS MANAGEMENT DIVISION
1919 West Jefferson
Phoenix, Arizona 85009
(602) 542-3741

Managing Public Records Sent and Received Via Electronic Mail

These apply to state and local government agencies and political subdivisions in the State of Arizona

The intent of this document is to explain requirements, and to assist with the management of electronic mail (e-mail) messages that meet the criteria for public records as defined by statute (*ARS § 41-1350*).

Intent and Purpose

This document has a two-fold purpose:

- First, it is intended to assist public officials and other custodians of public records in complying with Arizona's Inspection of Public Records Law (*ARS § 39-121*) in their use of electronic mail.
- Second, it is intended to promote the effective capture, management, and retention of electronic messages that are public records.

Introduction

Electronic mail software programs, commonly called e-mail, have become the communications method of choice for many public officials and public employees in Arizona. Electronic mail messages are often used as communication substitutes for the telephone as well as to transmit substantive information or records previously committed to paper and transmitted by more traditional methods. This combination of communication, record creation, and recordkeeping has created ambiguities on the status of electronic mail messages as public records.

The management of electronic mail messages that are public records affects nearly all functions on which a government agency is dependent for recordkeeping: privacy, administration, essential records management, administrative security, auditing, access, and archives. The need to properly manage electronic mail messages that are public records is the same as for other public records. ***Agencies need to maintain these records in proper recordkeeping systems to ensure compliance with Arizona 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 electronic mail messages, like paper records, must be retained and destroyed according to established records management procedures. Agencies should institute or modify electronic

mail software programs that allow easy transfer of public record electronic mail messages to an appropriate recordkeeping environment to facilitate proper management of their public records. Procedures and system configurations will vary according to the agency's needs and the particular hardware and software in place; however, the Arizona State Library, Archives and Public Records' Records Management Division strongly encourages consistent and systematic records management procedures to assist in the preservation of electronic mail messages that are public records.

Definitions

Electronic mail software programs.

Electronic mail software programs are communication tools that transport messages from one computer user to another. Electronic mail software programs range in scope and size from a local electronic mail software program that shuffles messages to users within an agency or office over a local area network (LAN), or an enterprise-wide electronic mail software program that carries messages to various users in various physical locations over a wide area network (WAN) electronic mail software program, to an electronic mail software program that sends and receives messages around the world over the Internet. Often the same electronic mail software program serves all three functions.

Electronic mail messages

Electronic mail messages are electronic documents created and sent or received through a computer system. This definition applies equally to the contents of the communication, the information about the transmission of the message (metadata), and any attachments associated with such communication. Thus, electronic mail messages are similar to other forms of communicated messages, including, but not limited to correspondence, memoranda, and circular letters.

Legal Requirements

Arizona Revised Statutes (ARS) do not include a specific definition for electronic mail, however the characterization of a record, as defined by Arizona law (*ARS § 41-1350*) defines a “public record” or “record” in the following manner:

... "records" means all books, papers, maps, photographs or other documentary materials, regardless of physical form or characteristics, including prints or copies of such items produced or reproduced on film or electronic media pursuant to section 41-1348, made or received by any governmental agency in pursuance of law or in connection with the transaction of public business and preserved or appropriate for preservation by the agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the government, or because of the informational and historical value of data contained therein. Library or museum material made or acquired solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference and stocks of publications or documents intended for

sale or distribution to interested persons are not included within the definition of records...

An electronic mail message created or received by a government employee is a record if it documents the organization, functions, policies, decisions, procedures, operations or other activities of the political organization. Note: It is not just that the message is created or received by a public office. This is true of any communication, whether electronic or paper. Also note that if a government employee or public official sends an electronic mail message from home using a personal electronic mail account, in their official capacity as an employee or official, that electronic mail message is also a record.

All electronic mail messages that meet the criteria of the definition of a public record (*ARS § 41-1350*) must be made available to the public upon request under the Arizona Inspection of Public Records Law (*ARS § 39-121*) during the required retention period, unless the content of the message falls under one of the exceptions contained in the law or in any other statute, regulation, Executive Order, or rule of court.

Any public record, whether it is subject to access by the general public or not, must be retained according to records retention and disposition schedules approved by Arizona State Library, Archives and Public Records (*ARS § 41-1345*) unless a legal hold has been issued that halts all records destruction. Destruction of public records without legal, administrative, historical, or other value must be reported annually to Arizona State Library, Archives and Public Records (*ARS § 41-1351*).

Retention and Scheduling Requirements

Electronic mail software programs are a means of transmission of messages or information. Like paper or microfilm, electronic 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 electronic mail as a single record series. Rather, retention or disposition of electronic mail messages must be related to the information they contain or the purpose they serve. The content, the information about the transmission of the message, and any attachments associated with the message are considered records (if they meet the criteria of a public record in *ARS § 41-1350*). The content of electronic mail messages may vary considerably, and therefore, this content must be evaluated to determine the length of time the message must be retained.

Simply backing up all of the messages on an electronic mail software program to tapes or other media or purging all messages after a set amount of time is not an appropriate strategy for managing electronic mail messages that are public records. For more information on records management, contact your agency's records officer or the Records Management Division of the Arizona State Library, Archives and Public Records.

For the purposes of this document, there are non-record electronic mail messages and public records electronic mail messages.

Non-Record Electronic Mail Messages

Electronic mail messages that do not meet the criteria of the Arizona statutory definition of a public record may be deleted at any time, unless they become part of some official record as a result of special circumstances. These types of messages may include:

Personal Correspondence

Any electronic mail message that is not received or created in the course of state business may be deleted immediately, since it is not a public record. Examples of the type of messages that may be deleted are unsolicited electronic mail advertisements, commonly called “SPAM,” personal messages, or the “Let's do lunch” (not a State-business meeting over lunch) or “Can I catch a ride?” type of message.

Other Types of Correspondence and Non-Record Publications

Publications, promotional material from vendors, and similar materials that are publicly available to anyone are not public records unless specifically incorporated into other public records. For example, electronic mail discussion groups' messages, unsolicited promotional material, files copied or downloaded from Internet sites, etc. are not public records and may be deleted immediately, or they may be kept in a “Non-Record” mailbox (or folder) and deleted at a later time, just as you might trash unwanted publications or promotional flyers received in the mail. However, if you justify the purchase of a “Zip Filing System” by incorporating the reviews you received via an electronic mail discussion group in your proposal to your boss; those messages become official records and must be retained in accordance with the retention schedule for purchasing records.

Public Record Electronic Mail Messages

Electronic mail messages that meet the definition of a public record must be managed (created, maintained and used, and disposed of) as such. The retention period for electronic mail messages that are public records depends on the content of the message. For more information on retention periods, consult the proper State of Arizona Records Retention and Disposition Schedule and your agency's retention schedule.

Managing Electronic Mail: Best Practices

Record Copy Electronic Mail Messages that are Public Records

Electronic mail users should be aware that electronic 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 principle, authentic copy of the message that must be retained per the retention schedule) is vital. If the holder of the record copy is not identified or aware of his or 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, agency policy documents which are transmitted to multiple recipients via an electronic mail software program need not be maintained by each recipient beyond his or her need for this information if record copy responsibility is established so that the record is maintained by some office or agent for its established retention period. In this example,

logically, the record copy responsibility rests with the creator of the policy document. Prompt deletion of duplicate copies of electronic mail messages from an electronic mail software program makes the program as a whole much easier to manage and reduces disk space consumed by redundant information.

Generally speaking, the individual who sends an electronic mail message and the primary recipient (“To” not “CC”) should maintain the record copy of the message. A suggested consideration is whether or not the message impacted the function or caused some business activity to occur. However, the varied uses and wide distribution of electronic mail messages may result in many exceptions to this rule that will have to be dealt with internally.

Filing

Non-transitory electronic mail messages (records that require administrative action, formulate policy decisions, or are used as the basis of administrative or program actions or decisions) should be filed in a way that enhances their accessibility and that facilitates records management tasks. Agencies should set up or modify electronic mail software programs that will allow electronic mail messages that are public records to be easily shifted to an appropriate recordkeeping environment to facilitate proper management of their public records. Procedures and system configurations will vary according to the agency's needs and the particular hardware and software in place; however, the Arizona State Library, Archives and Public Records' Records Management Division strongly encourages consistent and systematic records management procedures to assist in the preservation of electronic mail messages that are public records.

After brief periods in your IN-OUT boxes, messages that are identified as public records should be shifted to an appropriate recordkeeping environment to facilitate proper management of public records. Reference copies could also be transferred to other “mailboxes” or “folders” in the electronic mail software program, based on business functions or other filing classification schemes. Provisions should be made for the deletion of the reference copies once their reference/administrative need ceases to exist. No reference copies should be maintained longer than the retention period of the record copy, unless a legal hold has been issued that halts all records destruction.

Employees should be responsible for classifying messages they send or receive according to content, the agency's folder/directory structure and established records series.

Distribution Lists

If you send electronic mail messages that are public records to a “distribution list” (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 Smith received the message. Nicknames present a similar problem.

Subject Lines

Fill in the subject line on your electronic mail messages both to help your recipient identify and file messages, and to help you file your messages that must be retained for some period. Subject lines should be as descriptive as possible. Developing standards and naming conventions will benefit users with this task.

Subject lines can also be used to aid in the retention of messages. Retention codes, records series titles, or retention period information can be added at the end of the descriptive subject line to facilitate easy routing of sent electronic mail messages into appropriate folders to manage messages. Detailed subject lines can also facilitate classification with a proper electronic recordkeeping system.

Cautionary Note about Messages with Sensitive or Confidential Information

Employees should use caution when dealing with sensitive, proprietary or confidential information. It is advisable to use other methods to transmit records containing inter-agency, intra-agency, confidential or other information that fall under exceptions to public access under the Arizona Inspection of Public Records Law. Examples of such information include:

1. Attorney-client privileged communications;
2. Trade secrets or other proprietary information; and
3. Personally identifiable information, such as social security numbers or medical information

Storing and Managing Electronic Mail Messages that are Public Records

Storage of Electronic Mail

Users should understand that they have an obligation to manage record electronic mail messages with retention in mind rather than technology. Messages only have to be retained and stored for as long as the required retention period (unless there is a foreseeable, pending or ongoing legal or fiscal investigation). Very few messages must be maintained for a long period of time or permanently. The storage method of record messages usually depends on the retention period of the record and risk associated with that record. Risk should be assessed by the agency in regards to the impact on the rights of citizens, government accountability and documenting the Arizona experience should the record no longer be available or inadvertently deleted.

For example, low risk records do not impact the rights of citizens, do not document government accountability, nor do they document the Arizona experience. Low risk messages that need to be retained for six months should be relatively easy to maintain on the current electronic mail software program and then be deleted (unless there is a foreseeable, pending or ongoing legal or fiscal investigation). Storage decisions for record messages that need to be retained permanently will require more careful consideration.

Storage strategies for record messages vary and each option has corresponding benefits and disadvantages. An agency's information technology environment will also have an impact on the storage method. Regardless of the strategy, it is important to incorporate metadata

considerations into your storage decision (In this context metadata refers to information such as sender, recipient, date, routing, subject lines, system information and manuals, etc.).

It is recommended that agencies explore three options when retaining records received from an electronic mail software program:

- Records with very short retention periods that are identified as being low-risk to the agency could be maintained in the electronic mail software program
- Electronic recordkeeping systems
- Other proper recordkeeping systems

Short-term and low-risk messages

As discussed previously, electronic mail messages that meet the definition of “public records” must be properly managed. The content of the record message determines the retention period of the record and the level of risk associated with the record should it be improperly managed determines how that record should be managed.

The majority of record messages are records of low risk, such as:

1. “Transitory materials” [which include correspondence of little or limited reference value, transmittals and informational messages];
2. “Reference materials” [which include duplicate documents, newsletters, reports and publications that are not generated by the specific organizational unit in which such messages are being received]; or
3. “Working documents” [which include notes, drafts, feeder reports that are used in the development of final or summary records].

These low risk records have short-term retention periods:

1. 3 months after created or received (Transitory materials);
2. After informational value is served (Reference materials); and
3. After completion of the final record (Working documents).

With proper attention to records retention periods and files management, users can maintain these types of records within the electronic mail software program itself, with no need to transfer them to an electronic recordkeeping system or other proper recordkeeping system. The software program maintains the full functionality of the electronic mail message, and allows users to recall the message at any time for reference or responding.

Disadvantages of this method include the potential costs and effects of storage on the performance of the electronic mail software program and the lack of access to records by anyone other than the individual who sent or received the message. This could be a significant problem in answering inspection of public records requests. The law (*ARS § 39-121*) requires that records shall be open to inspection by any person at all times during office hours. Custodians are charged with furnishing copies promptly (*ARS § 39-121.01.D.1*). Any solution to retention of record messages that includes maintaining the records within the electronic mail software program should be done only after consultation with the agency information resource manager and the agency network administrator.

Without proper attention to retention periods and files management aspects of electronic mail message management, organizations also will run the risk of reducing the retrievability of records; disposing of record messages from within the electronic mail software program; or maintaining long-term, high risk records in an inadequate environment

Long-term and high-risk messages

Record messages that have a longer retention period than six months or have a higher risk should be managed differently than those low risk records messages with short retention periods of six months or less. For these records keeping them in the electronic mail software program reduces central control and places them at risk of being deleted, therefore, it is advisable to move them out. Users should move them into an electronic recordkeeping system or another proper recordkeeping system.

Recordkeeping Systems

A recordkeeping system is a system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition. Recordkeeping systems allow record messages to be:

- grouped with related records into classifications according to operational needs;
- retrieved easily and in a timely manner;
- retained in a usable format (including the transmission and receipt data of record electronic mail messages) for the required retention period found in an approved records retention schedule; and
- accessed by individuals who have a need for the records found within the system.

Electronic Recordkeeping Systems

Electronic recordkeeping systems are usually a combination of hardware; software; and policies and procedures that allow for the storage of record electronic mail messages and other electronic records in a digital format. Capturing records into an electronic recordkeeping system allows the user to maintain a moderate amount of functionality, in that record messages can be retrieved and referenced electronically.

With the cost of electronic storage decreasing, electronic recordkeeping systems are becoming more common. The real costs associated with a system of this nature are found in the ongoing maintenance and management of both the system and the records themselves. It is important for agencies to ensure that electronic records (including those that are delivered or sent through an electronic mail software program) and their associated systems are supported over time and that the records these systems contain are accessible and usable throughout their lifecycle.

When a record message is moved from the electronic mail software program, it is important that users move not only the message, but also the metadata and attachments associated with the message into the new system. For example, a record message can be captured into an electronic document management (EDMS) or records management application (RMA) system. The record should be captured in a format that is compatible with agency operations, and classified according to practices established by the agency. It is not recommended to transfer messages

stored in an electronic mail software program to a local hard drive as this limits access of the record to only one user and backup policies and procedures for desktop computers are not adequate.

Users should maintain a classification system that is consistent with established practices. This includes classification schemes as well as the use of naming conventions. In addition, users may want to consider protecting records from alteration.

Other Proper Recordkeeping Systems

The use of other proper recordkeeping systems to manage record electronic mail messages is also a viable solution. As with electronic recordkeeping systems, this strategy requires good filing structures and naming conventions.

Proper recordkeeping systems may include an analog component where the information could be printed to paper or transferred to silver halide microfilm. Any recordkeeping system that allows for the grouping of related records into a classification system, easy and timely retrieval; the retention of the records in a usable format for the required retention period; and for ready access to all individuals requiring the records should be considered.

The clearest example of a proper recordkeeping system is to print out a record message to paper, with its relevant metadata and attachments, for filing within existing filing systems in the agency. (In this context, metadata refers to information such as sender, recipient(s), date, routing, and subject lines, etc.). Record messages may no longer be searchable or retrievable in electronic form and/or the searching and retrieving functionality may be dramatically reduced in other proper recordkeeping systems, however, this option may offer the ability to integrate the filing of record messages within existing proper recordkeeping systems in agencies. Any record messages, metadata, and attachments stored in other proper recordkeeping systems should be done in a manner consistent with agency practice.

Permanent Electronic Mail Record Messages

Record messages that have permanent retention periods will have to be removed from the electronic mail software program and stored in either an electronic recordkeeping system or another proper recordkeeping system.

Should an agency choose to store the record messages electronically, they need to be cognizant of the potential impediments to digital preservation. The agency will need to develop plans for the refreshing, migration, emulation, and/or encapsulation of these electronic records. The storage of permanent records in an electronic format must be reviewed and approved by Director of the Arizona State Library, Archives and Public Records.

If an agency decides to store the record messages in any other proper recordkeeping system, they need to be cognizant of any potential impediments to permanent preservation. It is the agency's responsibility to ensure that the records are maintained and accessible throughout the record's lifecycle.

Regardless of the long-term preservation strategy, agency records managers should regularly examine the condition, retrievability, and usability of their records.

In any of the aforementioned situations, storage of records should be in compliance with State records storage standards.

Record Electronic Mail Messages and the Rules of Evidence

Agency personnel should be familiar with both state and federal “Rules of Evidence” requirements. For records maintained electronically, 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.

At a minimum, agency personnel should ensure the following:

- Electronic mail software programs used to create, receive and maintain record electronic mail messages have full, complete, and up-to-date systems documentation;
- Electronic mail software programs follow all recommendations for system security, and complete system backups are regularly and consistently performed;
- Backup procedures should be coordinated with disposition actions so that no copies of records are maintained after the retention period for the records has expired;
- Backups do not have recordkeeping features and therefore should not be used for recordkeeping purposes;
- Electronic mail software programs retain all data and audit trails necessary to prove their reliability as part of the normal course of agency business, the record copy of a message is identified and maintained appropriately;
- Agency records officers need to plan for records maintenance and record copy responsibilities for the recordkeeping system to meet requirements for reliability and legal records disposition;
- Electronic mail software programs should allow the server administrator to prevent destruction of records for legal and/or audit purposes.

A Further Note about Backups

If backup tapes are used exclusively for disaster recovery, they do not have to be searched during discovery. If the tapes are used to recover messages outside disaster recovery - Oops! I didn't mean to delete that message, can you get it off the backup tapes?-, then the agency will have to search the tapes. The Sedona Principles address the issue of discovery and backup tapes, and judges are giving it imprimatur through their decisions in case law.¹

Access

A major challenge for agency records officers is to guarantee that records maintained electronically 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

¹ More about the Sedona Principles can be found at <http://www.thesedonaconference.org/miscFiles/SedonaPrinciples200401>

electronic mail software programs have limitations in storage space that cause operational problems when messages are stored in the program beyond a specific period (such as sixty or ninety days), procedures must be in place to transfer records from the electronic mail software program to proper recordkeeping system to meet retention requirements, when appropriate. As previously discussed, it may not be necessary to transfer short-term (retention period is six months or less), low-risk record messages.

Record messages should be maintained in a format that preserves contextual information (metadata) and that facilitates retrieval and access. The recordkeeping system should allow deletion of records once their retention periods have expired, unless a hold has been placed on destruction due to foreseeable, pending, or on-going legal or fiscal investigations.

Beyond the generic challenge of technological change, there are more mundane, but equally critical steps that must be faced in order to ensure that records created by electronic mail software programs can be located and retrieved when required. Central to this process is the creation of standard electronic mail addresses and the establishment of standardized naming conventions and classification rules.

Record messages should be indexed in an organized and consistent pattern reflecting the ways in which records are used and referenced. Records maintained electronically 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. Time spent indexing records and establishing retrieval systems is time well spent. On the other hand, excessive time expended on identifying and retrieving poorly managed electronic records is not a productive use of staff time, and is an annoyance to the public as well. Records should be stored in logical classification schemes that are searchable by multiple data (metadata) elements.

Responsibility

Roles and responsibilities of agency personnel should be clearly defined. Employees must understand and carry out their role in managing record electronic mail messages and agencies must ensure compliance with agency procedures and Arizona law. The creator and recipient(s) of record messages should make decisions regarding the classification and retention of messages per established retention schedules. Unauthorized users should not be able to access, modify, destroy or distribute records.

Agency administrators, individual agency employees, records managers, information technology (IT) managers and server administrators share responsibility for managing electronic records. Agencies should clearly identify the roles of each staff member; adopt procedures, train staff, and monitor compliance on a regular basis. The agency should take appropriate measures to preserve data integrity, confidentiality and physical security of record messages.

When an employee separates from an agency, whether it is due to resignation, retirement, or termination, knowledgeable agency administrator(s) should review the employee's electronic mail account to determine which electronic mail messages should be retained as records, where the records should be maintained, and the appropriate retention period.

5. Endnotes:

This document is based in large part upon the work done by the New Jersey Division of Archives and Records Management, New Jersey CIO's Office, Maine State Archives, Delaware State Archives, Florida Department of State, the National Archives and Records Administration and the Electronic Records Committee (ERC) for the State of Ohio

Managing Electronic Mail: Guidelines and Best Practices New Jersey Department of State. Effective date July 11, 2002
<http://www.state.nj.us/state/darm/links/circular-letter-03-10-st.html>

American Historical Association v. Peterson. United States District Court for the District of Columbia. ["PROFS Case"], 876 F. Supp. 1300 (D.D.C. 1995)

Design Criteria Standard for Electronic Records Management Software Applications, published by the Department of Defense, November 1997
<http://jitc-emh.army.mil/recmgt/>

Electronic Mail/Messaging Policy. Policy Number 99-01. Office of the Chief Information Officer (CIO), State of New Jersey, effective date January 11, 1999.

Electronic Mail and Voice Mail: A Management Guide for Maine State Government. Maine State Archives. November 17, 1998.
<http://www.state.me.us/sos/arc/general/admin/email.htm>

Policy Guidelines: Electronic Messages. Florida Department of State. January 1998.
<http://dlis.dos.state.fl.us/barm/policiesruleslaws.html>

Policy Statement and Guidelines: Electronic Mail. Delaware State Archives. March 1, 1999.
<http://www.lib.de.us/archives/recman/policy/emailpolicy.htm>

Managing Electronic Mail. Guidelines for State of Ohio Executive Agencies. State of Ohio. Electronic Records Committee (ERC), 2000.
<http://www.state.oh.us/das/dcs/opp/OhioITPolicies.htm>

NARA Bulletin 2000-02, Disposition of electronic copies; suspension of NARA Bulletin 99-04, December 27, 1999. National Archives and Records Administration, 2000.
<http://nara.gov/records/grs20/>

Public Citizen v. Carlin et al. (1997), United States District Court of Appeals for the District of Columbia, 2 F. Supp. 2d 15 (D.D.C. 1995), revd. 184 F. 3d 900 (D.C. Cir. 1999)

Wilson-Simmons v. Lake County Sheriff's Dept., Ohio Supreme Court, 693 N.E. 2d 789 (Ohio 1998).