Challenges in Managing Records in the 21st Century

Prepared by the NECCC Analysis of State Records Laws Work Group

NATIONAL ELECTRONIC COMMERCE COORDINATING COUNCIL

NECCC
2401 Regency Road
Suite 302
Lexington, KY 40503
(859) 276-1147
www.ec3.org

Made in the United States of America.

NECCC is a national think tank of public and private sector leaders working to identify and develop best practices for e-government.

Alliance partners are:

National Association of State Auditors, Comptrollers and Treasurers
National Association of Secretaries of State
National Institute of Governmental Purchasing

NECCC also works in partnership with these affiliate organizations:

Association of Government Accountants
Information Technology Association of America
National Automated Clearing House Association
National Association of Government Archives and Records Administrators
National Association of State Treasurers

Table of Contents

Introduction

In the course of doing business, records are created through a variety of government activities such as vehicle registration, professional licensing, procurement contract transactions, general correspondence, and other external and internal business processes within state and local government offices (note: state government generally has oversight for local records rules and regulations). Governmental records may be created and transmitted in a variety of ways:

- Handwritten.
- Typewritten.
- Audio/video recording.
- Computer generated (including e-mail and databases).

These records support, document, and provide evidence of a variety of governmental activities including:

- Business processes.
- Program evaluation.
- Information policy making processes.
- Accountability ensurance.
- Facilities planning.

The records of governmental agencies capture information used to protect the rights and interests of governments, businesses and citizens and to preserve history and culture by documenting information about noteworthy people, issues, places, and events.

Most of these records are useful for a relatively short period of time and can then be destroyed. Some of the records will represent the agency's business record and need to be maintained for stewardship and public accountability purposes. Some records need to be preserved for many years, and a few should be preserved permanently to maintain the historical record. The challenge for public officials is to manage each of these types of records, making sure that those records with important information are preserved, while records that are no longer valuable are disposed of in an appropriate and legal manner.

This paper addresses the real world dilemmas of what a government record is and the task of its lifecycle management by proposing a working definition of a record, discussing the challenges of managing records, and identifying a set of best practice recommendations.

This page left blank intentionally.

The Scope of Records Management

All states have records laws that establish the need for effective records management, provide for the authority to dispose of records, and establish a structure for records management in the state. While these state laws are not entirely consistent, they generally encompass all information materials, regardless of format, created or received in the course of business. The retention of these records are codified in records retention schedules, which are established by analyzing statutory and administrative needs in combination with the content of the record, not the material on which it was created (i.e. hardcopy vs. electronic).

Government records may include but are not limited to:

- General correspondence.
- Transactional records.
- Vital statistics.
- Working papers, including drafts, versions, and copies databases (including the underlying tables, as well as routine reports).
- Web sites (including Web pages, images, documents, and audio/video files).
- Electronic backup media (including tapes, disks, and other storage devices).
- Electronic messages (including e-mail, instant messaging, and voice mail and including copies thereof on PDAs or home e-mail/instant messaging/voice mail systems).
- Metadata associated with records.

Most states also have open records, right to know, or freedom of information laws[1] that give the public the explicit right to access government records. The types of government records the public has access to vary significantly from state to state, however, that access is not unlimited. The federal government and each state identify information that is deemed confidential and therefore not accessible by the general public. The information may be a whole document or a portion thereof. In some states work documents are restricted from public access to ensure that state employees can have a free exchange of ideas, and most states have laws to protect individuals' privacy (e.g. phone numbers or social security numbers).

Unfortunately, the phrase *public record* can mean both *all government records* and *only those government records open to the public*. The definition of what is "open" may change over time and, given enough elapsed time, most records may become open. Regardless of whether the records are open or

[1] The United States federal government's law is the Freedom of Information Act. It pertains to records created and maintained by the federal government and should not be confused with individual state laws. Open records laws are also known as sunshine laws or good government laws.

not, they are all subject to records management laws and good records management practices. In this paper, the term *records* includes all the materials that an agency creates or receives in the course of business and the phrases *open records* and *confidential records* refer to that subset of records without or with restrictions on access, respectively.

Although not all records are equally important, they are all records that must be faithfully managed in accordance with state law. The principal task of records management and records managers is to help employees manage the records in their desks, cabinets, and computers. That includes helping employees to know how to organize materials so that those who need them – not just the employees – can find them; to know which records are vital and valuable; to know how to preserve records; and to know how and when to dispose of records or to identify non-records that can be disposed of immediately.

A Working Definition of Record

Records, as previously defined in most laws, were historically characterized in large part by format, for example:

- **<u>Georgia</u>:** "'Records means all documents, papers, letters, maps, books (except books in formally organized libraries), microfilm, magnetic tape, or other material…made or received pursuant to law or ordinance or in performance of functions by any agency" (Georgia Statutes 50-18-91[5]).
- **<u>Kentucky</u>:** "Public record or record" means all books, papers, maps, photographs, cards, tapes, disks, diskettes, recordings, and other documentary materials, regardless of physical form or characteristics, which are prepared, owned, used, in the possession of or retained by a public agency.
- **<u>New Jersey</u>**: "For the purpose of recording… loose leaf record books may be used…" (New Jersey Statutes 47:1-3).

In today's environment, records are now understood more in terms of function, content, context, and structure. This shift in understanding has resulted in large part from the rise of electronic records, in which records may be stored as bits and bytes dispersed non-sequentially across a storage device or media and assembled into a complete record only when viewed.

In the context of state laws, a more contemporary definition of record might read:

> *Data or information created or received in the course of agency business; that has been fixed on some medium; that has content, context, and structure; and that is maintained as evidence of that activity.*

Fixed Record

Fixity is the quality of content being stable and resisting change. To preserve memory effectively, a record's content must be consistent over time. Records made on mutable media, such as electronic records, must be managed so that it is possible to demonstrate that the content has not mutated or been altered. A record may be fixed without being static. For example a computer program may allow a user to analyze and view fixed data in many different ways. A database itself may be considered a record if the underlying data is fixed and the same analysis and resulting view remain the same over time.

Record Content

Content is the text, data, metadata, symbols, numerals, images, and sound that make up the substance of the record. A record's ability to fix information so that it can be repeated, recited, or recalled at a later date functions as an extension of memory and is at the heart of the concept of record. A record may be created specifically to preserve information over time or to prevent future misinterpretation of that information, although a record cannot be presumed to be reliable without authentication. However, any item – no matter how ephemeral it was intended to be – may serve as a record if it is later used as evidence of the thing to which it refers.

Record Structure

Structure refers to a record's physical characteristics and internal organization of the contents. A record's structure is the form that makes the content tangible and intelligible. Physical characteristics include components and methods of assembly, such as paper, ink, seals, and font families, or character sets, encoding, and formats. Structure also includes the intellectual organization of a document. A record's structure may be very simple, such as plain text on a page; it may be organized into an outline or sections with headings; or it may be highly complex, including a preamble, the body, and the signatures of witnesses.

A document's structure is contained within boundaries, which define the record as a unit and give it identity by distinguishing it from other information and may be identified/outlined in the records metadata. A record may consist of many physically or logically discrete parts that function together as unit, such as several pages or data values from many tables. However, those parts must be bound together in some fashion.

Record Context

Context is the organizational, functional, and operational circumstances surrounding a record's creation, receipt, storage, or use. Context includes a record's date and place of creation, compilation, or issue, and its relationship to other records. Context explains the "why" of the record and may be contained within the record's metadata. A single record derives its trustworthiness and usefulness from its association with other records that collectively tell the story of an event or activity. A letter from a constituent, for example, may be filed with the letter of response so that anyone viewing the response in the future can see it in the context of the request. Without the request, the response may be taken out of context and misconstrued. Record context is very important for agency accountability as it establishes the chain of events, business activities, information gathered, etc. that led to a business decisions or outcome.

Lifecycle Management of Information

As will be discussed throughout this paper, the true challenge to managing records in the 21st century office begins with system design and implementation. To accomplish this goal, a different approach to traditional records management is required – one which encompasses all stages in the lifecycle of information. The process map in Figure 1 proposes a framework for the lifecycle management of information. This framework is implemented through a combination of legislative, programmatic, and policy initiatives to achieve the creation and maintenance of electronic records meeting all the challenges of authentication, integrity, security, and usability. Each module of the process map is discussed below.

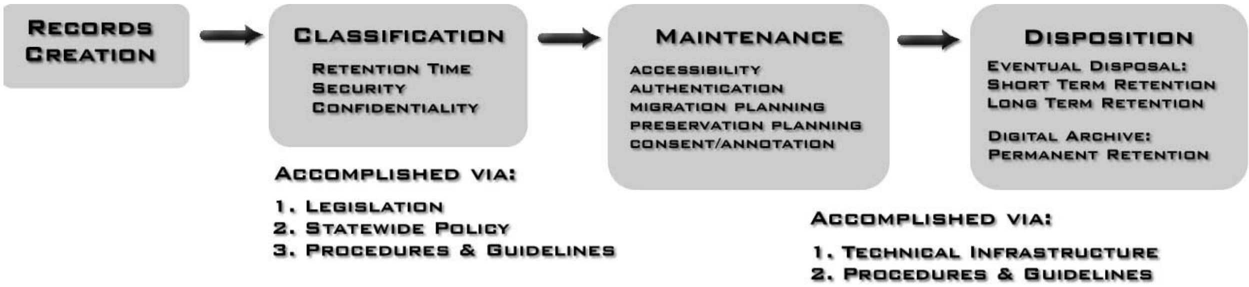

FIGURE 1. LIFE CYCLE MANAGEMENT OF INFORMATION

Classification

Classification refers to the designation of data as open or restricted, as an official record with an assigned retention period or as a copy or duplicate that will be disposed of after a short reference period. Classification of data occurs immediately following its creation and becomes the first step in managing the data through its useful life.

Throughout state statutes there are references to information and records that are restricted from public access and exempted from the provisions of state open records and freedom of information laws. What results in most states is a mass of laws that when combined with those federal regulations also applicable to state records, leaves local and state officials confused yet scrambling to answer an information request. In such an environment, some restricted information may be missed (not redacted) and released to the requester. The development and use of electronic applications provides agency officials with an opportunity to identify confidential data at its creation and provide protection for that data throughout its lifecycle through the application of security controls. Part of the protection of data includes knowledge of what to keep and for how long. Retention periods should be established with the assistance of the state's records management authority and the official copy of the record identified so that the retention can be implemented in a routine and systematic manner meeting all legal requirements for the record.

Maintenance

The maintenance of data is the second module in the lifecycle model. This module is key to the use and usefulness of data in that controls are applied to the data to ensure its authenticity and reliability over time. Strict controls are applied to annotation of the data and migration planning lays out how software upgrades and changes might impact the trustworthiness of the information. The successful implementation of e-government applications relies on the secure transmission of data between the agency and the citizen, between two or more agencies, and between the citizen and the agency. Much of this data consists of personally identifiable data that if released or intercepted by a third party could result in loss or adverse impact to the citizen and the agency. Yet, few governments have policies that clearly define the procedures and protocols that prescribe the handling of restricted data.

Strategies for the long-term maintenance and preservation of data, according to established retention periods, must be put into place at this stage. Such strategies would include migration and conversion of data and the creation of backups as part of the disaster preparedness program.

Disposition

The transformation of the modern government office from a largely paper environment to an electronic environment presents a variety of problems and concerns for records management. Where once business was conducted via paper, today e-mail, Web portals, databases, and other electronic applications are the means by which government transacts business. Electronic information cannot be set aside and ignored in the same fashion as paper. Such information is only eye-readable through the interface of software and hardware. With each upgrade or change in software environment, we risk the loss of vital government information, much of it historical. Adding to the problem, by not managing the information through the use of retention schedules, we are increasing the volume of information clogging our networks, slowing retrieval times and increasing both the fiscal and legal liability of the agency.

The need for policies, procedures, and guidance for agencies in the disposition of electronic records is critical to ensure the creation of legally-admissible data; the preservation of the integrity of this data for time periods sufficient to cover an audit or statutes of limitations; and the authenticity of the party conducting the transaction as well as the authenticity of the transaction once conducted. Technology alone cannot address all these areas of concern. Neither can a records management program alone address these concerns. The two in harmony with state law, agency policy, and technical infrastructure must work together to provide a framework for the management of information from cradle to grave.

The Challenge of Managing Records

Employees need guidelines to manage all the information resources on their desktops, in their files, and in the computer systems with which they interact. Further, they need to determine which of those information resources are records and how much of that information is subject to open records laws.

Although mandated by government, records management has been unevenly implemented with few agencies devoting a full-time position to the task. Even then, the job of records management has been driven by the need to destroy vast amounts of paper rather than to systematically control, manage, and use information and knowledge of the agency. As budgets have tightened and governments have turned to technology to "do more with less," e-mail, Web portals, databases, and other electronic applications have been typically implemented without regard for managing the information or for ensuring the creation and preservation of records.

Traditionally, paper records were managed long after creation, once they were physically filed into agency filing systems and began to take up valuable office space. This management typically consisted of transferring the records offsite to a records center facility or warehouse dumping ground where they were forgotten. With electronic records, management must be included in system planning and implementation and must take place immediately upon creation as the agency classifies the information for further use. This classification is vital for the application of corresponding electronic controls to ensure the effective maintenance and disposition of the record.

The following is a discussion of the challenges that the face every governmental employee who participates in the creation and use of records.

Ambiguity of What A Record Is

People often think of "record" in very narrow terms, as limited to formal documents documenting a significant event and often bearing official signatures and seals. State records laws generally define the term record much more broadly, creating some confusion as to what records management encompasses.

Records may be formal or casual. Memos and scribbled notes, e-mail, voice mail, and sketches on paper placemats may all be records. Records are not limited to "official" documents signed by senior management. Records are created throughout an agency.

Records can be in any format. They are more than text on paper, and include maps, photographs, audio and video recordings, and publications. Records include the electronic equivalents of those formats, including word processing files, spreadsheets, databases, graphics (jpg, gifs, and tiffs), and video and sound recordings (wav, mp3).

Records include drafts and final versions. Although drafts may not have the same value or retention period as the final version, drafts may capture important information showing how the final document evolved. For example, drafts may show shifts in thinking or indicate when a certain decision leading up to the final version was made and who made it.

Records may be of limited or permanent value. Many records have only ephemeral value and need to be kept for only a short period of time. Most have limited value and must be kept for a limited period of time, ranging from a few weeks to years. Only a few records have permanent value and will be transferred to an archive to be kept indefinitely.

In short, a record can be anything that contains information that has been created or received in the course of business that can be used to provide information about some action.

This ambiguity in what constitutes a record is especially complicated by electronic communications and computer-based workflows, and their consequent production of digital records. The government "paper trail" is now just as likely to be made up of electrons on a disk as ink on paper. Hard disks, magnetic tape and memory cards are replacing paper and file cabinets.

The electronic office poses unique challenges to recordkeeping. As noted in a previous section of this paper, the most essential qualities of a record are that it is authentic and that its content is fixed over time. In other words, people must have confidence that a record is what it says it is. Electronic records, unfortunately, do not intrinsically inspire this confidence in the same way that paper records do. The ease with which electronic documents can be created, altered, accessed, duplicated, and shared jeopardizes their value as records. Ironically, the most appealing aspects of creating electronic documents are what weaken our confidence in electronic records.

There are six fundamental challenges in maintaining confidence and trustworthiness in electronic records. Organizations should adopt practices and policies to address all of these challenges:

- **Classification:** Develop and adopt data classification standards to protect information from unauthorized or accidental disclosure, modification, or loss. Data classification categories may be as simple as "Open" or "Confidential," or the classification categories may be more elaborate. Classification standards should be based on applicable laws, legal, and regulatory requirements, not individual desires.

- **Authenticity:** Provide assurances that every record truly originates from its attributed author.
- **Integrity:** Detect and track unintentional or malicious record alteration.
- **Non-Repudiation:** Prevent authors from refuting any record that they created.
- **Security Persistence:** Maintain a document's security throughout its lifecycle, from first draft to archived record, per the classification assigned.
- **Usability:** Finally, the practices and policies to address the five preceding challenges should be easy to understand and easy to use so that everyone in an organization who creates and accesses electronic documents protects document confidentiality, authenticity, integrity, etc.

For a record to remain reliable, authentic, with its integrity maintained, and useable for as long as the record is needed, it is necessary to preserve its content, context, and sometimes its structure. A trustworthy record preserves the actual content of the record itself and information about the record that relates to the context in which it was created and used. Specific contextual information will vary depending upon the business, legal, and regulatory requirements of the business activity (e.g., issuing land use permits). It also may be necessary to preserve the structure or arrangement of its parts. Failure to preserve the structure of the record will impair its structural integrity. That, in turn, may undermine the record's reliability and authenticity[2].

Maintaining the Authenticity and Trustworthiness of Electronic Records

The records profession defines authentic records as being what they purport to be – reliable records that over time have not been altered, changed, or otherwise corrupted. Historically, protecting paper records from alteration or change was made possible through locked file cabinets, use of records vaults, and transfer of the records from the custody of their creators to an independent organization or individual whose mission was to protect this material from change or alteration. This protection involves an appropriate storage environment, care and handling of the records, and controlled access to the records.

Electronic records require the same care and handling in order to protect them from the same alteration or change. However, it is difficult to provide this protect in a production or operation environment where most of these records reside. Information technology professionals will often claim that the use of authentication technologies will ensure the protection of the records. Authentication technologies are used to verify the identity of the user – making sure that users are who they claim to be. As Internet usage continues to grow and more agencies make more services available online, this issue will become increasingly important to the creation of a reliable record. When services are provided via traditional, non-electronic processes, various authentication methods are used. Customers are required to sign forms or letters, present identification numbers or case numbers, or show a driver's license or birth

[2] New Jersey Circular Letter 01-01-ST UETA Guidance: Records Management Guidance for Agencies Implementing Electronic Signature Technologies, http://www.njarchives.org/links/circular-letter-01-01-st.html#4-2.

certificate. Most of these methods will not work online. A sample of online authentication methods includes passwords; personal identification numbers (PINs); user identification (USER IDs); cookies; biometrics; encryption; public key cryptography (digital certificates); and Secure Sockets Layer (SSL) and Transport Layer Security (TLS). While the use of authentication technologies is critical to the creation of reliable data, it is only part of the answer.

So long as the electronic records remain in the custody and control of their creator or recipient, they are perceived (by the courts) as being subject to change or alteration. Transferring the records from the custody of the creator into the custody of a “trusted third party” is the first line of protection for the trustworthiness of electronic records. Unlike paper records, electronic records are susceptible to alteration and corruption from the environment, so maintaining a stable storage environment is essential to protecting the records. In addition, the physical storage media (CDs, magnetic tapes, optical disks, etc.) are vulnerable to corruption and degradation from age, requiring their periodic replacement. To top everything off, the records themselves may be altered without leaving any physical evidence. Thus, the technology that makes it so easy to create, use, store, and retrieve records also has the potential for making it possible to alter, change, or corrupt the record of events in an agency.

There are four technology solutions that provide the level of protection needed to guard against alteration of the record over time.

- **Secure Client-Server Architecture:** This technique uses the structure of the agency’s information systems to permit read-only access to documents. In a client-server architecture, a user addresses queries to a database or retrieval requests for specific electronic documents from the desktop; queries are then transmitted to a server, which passes the request to the storage repository. The system then retrieves and processes the instructions and sends the data back to the user. In a secure client-server architecture, the original electronic record is never directly accessible to the user, and the reliability of the record remains intact.

- **Cyclical Redundancy Checksum:** Used by the telecommunications profession to ensure error-free transmissions, this technique uses the number of bits in a packet (a frame check sequence) divided by a pre-defined 16-bit or 32 bit polynomial as a comparable computation (a cyclical redundancy checksum) that proves the lack of errors (or alterations) in an electronic record or file. The original computation (the cyclical redundancy checksum) can be compared at any point in time (such as during or after a conversion or migration) with a second computation using the same values – number of bits in the packet divided by a polynomial – to verify the reliability and authenticity of the data. These values can be appended to the record so that this reliability extends over time and through multiple migrations.

- **One-Way Hash Digest:** A one-way hash involves the use of an algorithm to compress a record into a fixed length, reducing its size. It is called one-way because the hash digest itself is irreversible. No matter how many times this hash is repeated, the same fixed length results, showing that no change has occurred to the record. This method, however, presents one problem – conversion or migration of the data changes the underlying bit stream (it alters the size of the record so the original hash digest will not match) and necessitates the creation of a new hash digest.

- **Hash Digest With Digital Time Stamp:** This technique combines the use of the above-described one-way hash digest with the use of a third-party certificate service that time-registers the digest. Multiple hash digests of a record are stored and date-time stamped to form a root superhash. An authentication certificate is then generated and stored with each record or in a database, documenting the authenticity of records. When the need arises to authenticate a record, a new hash digest can be generated and compared to the authentication certificate.

The piece to the puzzle of maintaining authenticity over time is a non-technology component – policy and procedure. Approved policies and procedures are needed to guide agency staff in making the appropriate decisions on when to create a record, how to name it and file it, and how to protect passwords and other security measures taken to protect records. The selection of a technology solution, such as use of hash digests, should also be documented as part of the agency's IT procedures.

The Organization of Records

Responsibility of Agency Staff: Government agencies have an obligation to make employees aware that the records they generate must be retained and destroyed according to established records management procedures as set forth by their respected state record laws. If agency records are mishandled, electronic and paper records can easily be lost or misplaced, and information may be difficult to retrieve. The results are costly delays, lost business opportunities, frustrated office personnel and managers, businesses, and citizens being forced to make decisions based on inadequate information. Currently, most electronic information systems used to create, receive, and store these records do not provide full records management functionality. Agencies need to adopt electronic information systems that provide proper controls over the creation of records, maintenance of records, and disposal according to approved processes for managing records according to their predetermined classification, category and approved retention schedule.

Agency roles and responsibilities pertaining to records management should be clearly defined. Employees must understand and carry out their roles in records management and agencies must ensure compliance with agency procedures, state and federal record laws. 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 agency records. Agencies should clearly identify the roles of each, adopt procedures, train staff and monitor compliance on a regular basis. The creator or recipient of a record should make decisions regarding its status for retention and storage. The agency should take appropriate measures to preserve data integrity, confidentiality and physically secure all types of records.

Records Retention: Most of the 50 states have record retention schedules which inventories the records located within state and local agencies and establishes the period of time in which those inventoried records be retained. The retention schedule serves to ensure that records are kept for their reasonable time period, after which the retention period expires, the records should be destroyed. Record retention schedules help prevent regulator problems and court cases. To assist in complying with state retention schedules, agencies need to implement record retention education opportunities for its staff. Agency staff needs to be aware of their own responsibility for record keeping and the penalty for not complying with the record management policy or plan. An effective records management system/policy will ensure that only records that are required by law or for business continuity and value will be retained.

Record Category: A record category is a group of related or identical records, which are used and filed together, have a common purpose, and are governed often by the same retention period. A records category system can assist organizations in effectively managing their records. Establishing a series of record categories according the business functions can help staff file their records into a common file system. Examples of records organized into typical business categories include:

- Administrative.
- Fiscal.
- Legal.
- Personnel.

The filing of the record into one of the categories applies its official or originating version. All other versions may be destroyed when the agency deems appropriate.

Traditional Record Practices: Many agencies have been following the same records management processes for their paper records for years. However, the majority of state agencies have not extended these record management policies to include electronic records, including e-mail. E-mail messages that are records must be identified, scheduled and retained just like records in other formats. In determining the proper length of retention for messages and attachments sent or received electronically, consideration should be just as if the message was conveyed on paper. All e-mail messages should never be considered to have equal retention value. Each e-mail should be managed individually according to its informational content and retained accordingly.

The Exponential Growth of Information and the Challenge of Rapidly Multiplying/Spreading Copies

In today's world, we are experiencing an information explosion. A recent study by the School of Information Management and Systems at the University of California-Berkeley[3] finds that the amount of

[3] Lyman, Peter and Hal R. Varian, "How Much Information", 2003. Retrieved from http://www.sims.berkeley.edu/research/projects/how-much-info-2003/, on August 23, 2004.

new information has roughly doubled in the last three years. Roughly 93 percent of that information was born digital and is stored electronically as well.

Personal computers, electronic mail systems, Instant Messaging, the World Wide Web, PDAs, and digital cameras have all contributed to this information explosion. They have impacted the way we communicate and live. More specifically, the information explosion has impacted the way business is conducted in government today.

The tremendous growth in technology has placed more sophisticated tools in the hands of office workers. Much of the electronic information being created by governmental agencies, political subdivisions, and contractors resides in stand-alone personal computers and in networked computer environments. Most information is under the direct control of the individual at that particular desktop, or the information technology staff administering the network. This has impacted the authenticity and reliability of government records. There are inadequate controls over the creation and maintenance of electronic records. Everyone can create and delete records, but few are managing them. Management comprises of controlling the creation, maintenance and use, and disposition of the records. Illustrations of the mismanagement of records follow.

Records are becoming more informal, as they are being made by individuals who have not been educated in proper recordkeeping practices. The records are often not complete, accurate or comprehensive to document government activities. For example:

- Individuals may send out a complete record (perhaps a signed letter on letterhead, or an annual report complete with graphs as amendments all bound together) to someone. The record retained by that individual may be the unfinished copy (the unsigned word processed document, not on letterhead, with a date stamp that changes everyday to that day's date; or the different documents that comprised the annual report which sometimes are modified later as they include spreadsheets that are still useful for current statistics) resident on their personal computer or shared networked space.

- A Webmaster posts inaccurate information on an agency's web site that greatly impacts citizens. The information later is revised and the Webmaster does not capture the record prior to or after changing the Web site. Impacted citizens sue for compensation.

- A prominent university professor has a collaborative government grant with another prominent professor at a different state university in a different state. They share their information via the Internet. Records are created by joining their data together and neither one is capturing the record.

Records are becoming more difficult to manage. For example, there may be several drafts and the final (incomplete, as described above in one of our examples) record stored in the same place. Other copies may reside on computer backups, e-mail messages back and forth with revised drafts attached, floppy disks or rewriteable CDs (since the individual took the work home to complete), on their home computer, laptops (because they may have been on official travel while they were completing the work), PDA or BlackBerry® (so they could continue working on it while they waited for their plane at the airport), etc.

These drafts and copies have strange names that no one but the end user will be able to recognize. The end-user does not take the time to clean up the copies and drafts before they go on to their next project. In most cases, some time later the records are requested in an open records request, or subpoenaed; the end user leaves that position and either cleans house or boxes up the floppy disks and CDs (obviously not labeled) or the person coming in after them cleans house; the IT department requests people to delete things for better performance of the technology; or information is lost in some other way.

The above examples are meant to illustrate the importance of building recordkeeping processes into new systems design as well as the need for records managers to be included in the decision making processes that impact records. Records are important resources that must be managed efficiently and effectively, no matter what form the records take. Some information may never exist in hardcopy form. Information in all media must be readily available, understandable and useable to support decision-making, programs, and accountability to the government and the public.

Properly managing electronic records will become more and more important as records proliferate. Greater use of technology means that records managers must become more involved in the lifecycle of electronically created records. With the rise of distributed computing by users, records managers and information technologists have found it to be a challenge to retain influence and control of the lifecycle of information being created in end-user environments.

There is perhaps no other information technology in recent memory that has grown as fast as electronic mail. A recent study by the School of Information Management and Systems at the University of California-Berkeley[4] finds that approximately 31 billion messages are sent daily via e-mail. The study notes that this figure will double by 2006.

Electronic mail software programs, commonly called e-mail, have become 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 transmit substantive information or records previously committed to paper and transmitted by more traditional methods. This combination of communication, record creation, and record keeping has created ambiguities on the status of e-mail messages as public records.

[4] Ibid.

E-mail proliferates at an astounding rate. For illustration purposes, let's look at a hypothetical example[5]. A small agency may have 100 employees who each receive or send out 20-30 messages a day. This agency will have 500,000 - 756,000 messages by the end of one year (250 working days per year). The IT staff at this agency backs up the e-mail system daily, weekly and monthly. Monthly backups are retained while the daily and weekly ones are rotated. The agency now has 6,000,000 – 9,072,000 messages in its holdings for the year.

The management of e-mail messages that are public records affects nearly all functions on which a government agency is dependent for recordkeeping: privacy, administration, vital records management, administrative security, auditing, access, and archives. The need to properly manage e-mail messages that are public records is the same as for other public records.

Knowing What to Keep

Due to the ease at which records can be created, copied, and destroyed, agencies need to have policies in place, and train their employees to control the amount of copies that are created from any given record. "Official" or "record copies" need to be identified as early as possible in the life of the record. These official copies should be described in a records retention schedule, and are the version of the record to which the retention period is applied. All other copies are then considered "duplicate copies," and the employees can and should be encouraged to destroy them as soon as they are no longer needed.

Official electronic records should be housed in a central file repository, ideally on a networked file server, or on a centrally located computer in a non-networked agency, that is secured and backed up on a regular basis. It is important to remember to institute a version control/change control methodology for electronic records. This is similar to the central files that agencies are used to keeping their paper records in. Employees should be trained to not store official records on their local hard-drives as these drives are not routinely backed up and may not be totally secured. Also, the more copies of records that are scattered about the agency, the more legal risk the agency is exposing itself too.

Disposing of Records Properly

Disposition is the final stage in any record's lifecycle, and proper disposition is an important part of any records management program. All of the records an agency creates should be described on a records retention schedule as noted above. The schedule establishes the length of time the records should be retained by the agency. For records with enduring value, usually identified as permanent in records retention schedules, disposition may involve transfer to an archival facility. Agencies need to contact their archival institution for proper transfer instructions. Most of the records an agency produces will be

[5] This example was adapted from an example by Kenneth J. Withers, Federal Judicial Center, in his PowerPoint presentation "Electronic Discovery National Workshop for United States Magistrate Judges, June 12, 2002" retrieved from http://www.fjc.gov/newweb/jnetweb.nsf/pages/196 on August 27, 2004.

destroyed, or deleted in the case of electronic records, at the end of their lifecycle. Agencies need to make sure that they have written policies in place that outline the procedures to properly dispose of their records, and they must make records destruction part of the normal course of business. In other words records destruction must occur on a regular basis following the records retention schedules, not randomly or on an ad hoc basis. The best times to dispose of records are at the end of fiscal or calendar years; the end of an audit (following the release of the final report); or, in the case of government agencies, at the change of administrations, but only if the retention of the records has expired and appropriate legal permission has been granted for the destruction. Records destruction should always be suspended in the wake of legal or administrative action against the records involved, even if the retention period has expired.

Most states have statutes prohibiting tampering with a public record. For example, Arkansas makes it a crime to destroy a public record; "a person commits the offense of tampering with a public record if with the purpose of impairing the legibility of a public record he knowingly makes a false entry in or alters a public record or erases, removes, destroys or conceals a public record." If a person destroys a record that fits under a specific retention law and the destruction of it prevents if from being available, the law has been violated.

One of the biggest differences between paper and electronic records is the methods of destruction. Electronic records are, on the one, hand extremely fragile. They can be corrupted or rendered unreadable with the stroke of a key. On the other hand, electronic records can be very durable in that they can be hard to destroy. Disposal, in an electronic environment, is the ability to identify, gain authorization, and completely purge a record from a computer system. Hitting the "delete" key does not actually delete the record. Hitting the "delete" key simply removes all markers to the record and tells the system the record is no longer needed and may be overwritten. If the system does not need the space, then all or part of the record may still exist on the disk. There are several ways to remove records from electronic systems. These include:

- DoD 5220.22-M Data Destruction Standard.
- Commercial software programs that will destroy records from electronic systems by overwriting the medium.
- Media can be factory reformatted or degaussed to remove records.
- The media can be removed from the system and physically destroyed through manual means.

The sensitivity or confidentiality of the information contained in the record will dictate the appropriate method of destruction. For example, if the record contains no sensitive information and would simply be thrown out in paper form, then overwriting or reformatting the media would probably be sufficient to delete the electronic record. However, if the record contains highly sensitive or confidential information and is the type of record that would be shredded in paper form, then physically destroying the media may be necessary.

The destruction of electronic records is further complicated by the backup procedures that are so important to the overall reliability of the system. The proliferation of duplicate records located on the daily, weekly, monthly and other backups created for disaster recovery and business continuity process necessitates extra care in the destruction of electronic records. Procedures must exist for the media and frequency of both individual record (such as databases) and system backups. In addition, procedures for the physical destruction of the official records must include the destruction of the backup and should be detailed enough to specify the number of overwrites that should occur to a backup tape or the method of physical destruction of the media in order to ensure the total destruction of the records.

In some rare cases, an agency may be order by the courts or other legal authority to expunge the record. Expungement is the removal and destruction of an individual document, image, or data element from the overall agency record. This procedure often requires (rulings vary between courts and between individual states) that no record or identification of the documentation ordered expunged remain in existence. The phrase “expunged from the record” literally may mean that no documentation of the act remains in existence.

Knowing What Is Confidential and How to Comply With Open Records Requests Without Violating Confidentiality

Agencies should be aware that some records are restricted from public access, or may contain specific data that is restricted from public disclosure and should be redacted before releasing the records to the public. Such data includes Social Security Numbers, specific health information, and other personal identifying information (drivers license numbers, credit card numbers, etc.). Many states have statutes that identify the type of records and data that is restricted or exempt from disclosure, usually referred to as Open Records Laws or Freedom of Information Laws. A public agency has no obligation to make these records available to the public and cannot be forced to make them available except by entry of a court order. Records custodians need to be aware of other state and federal laws regarding privacy and confidentiality, for example the Health Insurance Portability and Accountability Act (HIPPA) and the Federal Education Rights and Privacy Act (FERPA). For a more detailed discussion of the impact of these laws on how an agencies protect privacy and confidentiality, please refer to your state statutes and *INFORMATION PRIVACY: A Spotlight on Key Issues (February 2004,Version 1.0)*, produced by the National Association of State Chief Information Officers.[6]

[6] The National Association of State Chief Information Officers (NASCIO) has released *Information Privacy: A Spotlight on Key Issues* to serve as a resource for states developing privacy policies that protect citizen information and are compliant with federal and state legal requirements. This publication highlights key areas of privacy such as children's information, drivers' information, health information, financial information, educational information, social security numbers, homeland security related information, website privacy policies and government data matching activities and agreements. In addition, the publication includes state

In cases where a database containing confidential and open data is requested, the agency must redact such confidential data while making the non-exempt data available to the requestor. This redacting of confidential data from an otherwise open record is often the responsibility of the agency. When databases are being designed, any confidential data should be contained in separate fields so that they can be easily identified and filtered out of a response to an Open Records request. [7] This formatting can be easily done on any new databases in the design stage. The agency may also need to evaluate existing databases to see if it would be in their best interests to redesign those databases.

The Need for Records Managers and Records Management Principles at the Table During Systems Design

No consistent guidance is provided to agencies regarding needed policies and procedures to guide records creation. System documentation focuses more on how the application was installed rather than on the ways information is collected, shared, and stored. Each state must issue policy (and if needed, legislation) to guide agencies in the classification and maintenance of information as records. State chief archivists and chief technology officers must work together to develop statewide electronic record archival standards to insure consistent enterprise-wide long-term data storage formats and information retrieval expectations.

It is important to build good recordkeeping into new systems. The involvement of the records manager in the design of new systems is essential. This will help to ensure that records are identified and methods are used to capture fixed records to provide evidence of an activity. The records manager can help articulate what systems and rules are needed to ensure those records are captured and maintained, how long the records should be kept to meet business and other requirements, how they should be stored, and who should have access to them.

Business rules that dictate what a record is, how and when records will be created or captured, how they will be maintained and used, and for how long need to be built into new systems as they are being designed. Too often systems have been designed with no recordkeeping requirements and valuable records that protect the rights of citizens, provide evidence of government accountability and document specific and significant government historical events have been lost. Sometimes this lack of incorporating recordkeeping requirements has caused records that need to be destroyed to be kept longer than

examples for many of these areas of information privacy. The document is available for purchase to non-NASCIO members at https://www.nascio.org/publications/index.cfm.

[7] When creating databases with redacted layers, the file produced for distribution should be a combination of the original file and the redacted layer(s), so that they are one image with one layer. Once the new file is saved, it should not be possible to lift the redaction from the confidential fields.

required. The cost of managing and storing these records places an unnecessary financial burden on valuable and scarce public funds.

Here are some recordkeeping requirements to consider when developing a new system:

- What records need to be created or kept that document the functions/activities in this new system?
  - What is it necessary to capture?
  - Who will rely on the information?
  - Will it be necessary to provide a fixed record of what was relied on to make decisions by the organization?
  - Will it be necessary to provide a fixed record of what was relied on to make decisions by the organization's stakeholders or the general public?
  - How will the information be verified for authenticity, completeness, and accuracy before it is captured into a fixed record?
  - Is an outside contractor being used [e.g., to receive inputs from stakeholders that are then converted to be ingested into the new system], if so:
    - Will inputs need to be captured as received from the stakeholders?
    - How will the information be verified for authenticity, completeness, and accuracy before it is captured into a fixed record?
    - How long will records being received and created by the contractor need to be maintained and accessible?
    - All recordkeeping requirements should be documented in the contract with the contractor.
- What will be required to supply appropriate content, context and structure of the records before the records are captured in a fixed method?
  - Are there automated tools that can be integrated to provide date of creation/receipt; owner; classification information as the type of record (draft, version number, final official record, duplicate copy), records series (to be able to link the records to their retention periods and to other salient records related to the same business activity), and access restrictions (including the ability to redact restricted information from the records when required by an open records request); and other metadata that will enhance the retrievability of the records (such as appropriate and approved keywords found in the organization's official thesaurus)?
  - What will be necessary to ensure a smooth transition when the records are migrated to another new system?
- How will these records be captured so they are fixed?
- If retention periods for the records change, how will the new retention period be transitioned into the system?
- How will records be maintained through the retention period?
  - How will the records be protected from unauthorized access?
  - How will the records be protected from unauthorized destruction?
  - If there are plans to move records near-line or off-line, what protocols will be built in to ensure that the media is refreshed and the bit error rate is corrected on a regular basis?
  - What indexing systems will be used to ensure the records are accessible?
  - What migration strategies will be in place to regularly replace the media and to refresh the data?

  - What migration strategies will be used to convert the records without loss or corruption to the next version or another system?
  - What will be the backup strategy used for the new system?

    - How will the strategy provide business continuity/vital records protection?
    - How will the strategy provide for the reliability and integrity of the records should a server crash or if a security violation occurs?
    - How will the strategy provide for times when the system is down – how will the records be available, how will the new records be captured, and how will captured records be put into the system after it is back up and running?
    - How will the strategy provide for the deletion of records once their retention period has lapsed, even on backup media?

  - What records will need to be created for audit purposes within the new system:

    - Will the system need to record who captured, retrieved or deleted records and when?

- How will any downloads of data be managed so that renegade standalones systems are not created without the proper recordkeeping requirements attached to them?

- How will records be deleted from the system when their retention period has lapsed?

- Will the organization want to delete all associated metadata when the records are deleted, if not, what will need to be retained and for how long?

- How will records be protected from deletion when there is a hold on destruction?

- How will the records with permanent retention be preserved and accessible over time?

- What system documentation will need to be created to document recordkeeping processes?

- What training will be provided to users to ensure they are aware of their recordkeeping responsibilities?

(Caveat: this list of considerations may not be all-inclusive, but should generate contemplation when designing, implementing, and/or managing an electronic records/information management system.)

Policies and Procedures

To effectively manage records and information, governmental agencies should develop, implement, and maintain a codified set of records management policies and procedures. This is especially important in the current milieu where agency personnel must no longer manage just paper-based records, but the proliferation of records in electronic form in conjunction with paper, microform, and other formats.

Quality policies and procedures should include the following:

- Records retention schedules.
- Organizational charts.
- Business process flowcharts.
- Classification procedures.
- Records storage procedures.
- Backup procedures.
- System documentation.

- Disaster prevention and recovery procedures.
- Disposition procedures.

Polices and procedures should not be static; they should be distributed to all personnel and the agency personnel should been trained in their usage. Further, policies and procedures should be reviewed on a routine basis, yearly at a minimum, to make certain that they are effective;

Training in Records Management

In the past, the responsibilities of records management have fallen upon a professional records management unit, a central files unit, and/or administrative/secretarial staff of a government agency. Gone are the days when an administrative support staff would type, file, and eventually transfer records to some form of longer-term storage or destroy the record through appropriate means. Now the vast majority of government agency personnel have computers on their desktop where they are creating, receiving, and storing records on a daily basis, from documents that need to be printed out and signed to e-mails.

It is problematic enough working in a hybrid world where records are "born" electronically and converted to hardcopy for distribution and retention. Now governmental agencies are in the process of deploying electronic records management systems where the records creator will be intimately involved in the in the records management process from the start. Without the appropriate training, these electronic records management systems will suffer from the "garbage in-garbage out" syndrome.

Agency personnel will need to be trained not only in the basics of records management, but also in the ability to categorize documents. Further, they will need to be trained in what not to do, such as printing out and distributing five copies of a memo that can be viewed on line; that in the "electronic records world" only one copy needs to be maintained. Most importantly, they will need to be trained to understand that it is the content of the document, not its format nor the medium on which it is created, received, or viewed that dictates its retention.

This page left blank intentionally.

CONCLUSIONS

In the course of doing business, records are created, received, and maintained through a variety of government activities, and in a variety of forms. Although computers were once thought to be ushering in the age of the "paperless office," we are experiencing exponential growth and replication of records. Moreover, the management of the records no longer falls strictly to a record management unit or an administrative support staffer. Therefore, it is essential for governmental agencies to develop sound records management programs that are grounded in thoughtful and effective polices and procedures that inform agency personnel: as to nature of what is a record; which records are open to the public and which are confidential; how to classify, organize, and maintain records; and how to dispose of records properly. Lastly, it is imperative that the design and implementation of records and information management systems include project teams that are multidisciplinary, with a spot reserved for records management personnel. By taking these recommendations into consideration, governmental agencies should be prepared for the challenges of managing records in the 21st century.

This page left blank intentionally.

Contributors

NECCC Board Liaisons

Dan Combs, President, Global Identity Solutions
David Lewis, Consultant
Amelia Winstead, State and Local Government Services Manager, Georgia Office of the Secretary of State

Work Group Co-Chairs

Michael Engelhardt and Diane Helander, Adobe Systems
Steve Walker, Idaho State Archivist

Other Active Work Group Members

Martha Combs, Microsoft
Richard Dymalski, Maricopa County, Arizona
Bruce Garner, North Carolina Office of the Secretary of State
Gordon Richardson, Iowa State Archives
Sigi Konieczny, Georgia Archives
Drew Mashburn, Arkansas Office of the Chief Information Officer
Glen McAninch, Kentucky Department of Libraries and Archives
Richard Pearce-Moses, Arizona State Library
Mark Myers, Kentucky Department of Libraries and Archives
Dan Noonan, New Jersey Division of Archives and Records Management
Laurie Sletten, Arizona State Library
Albin Wagner, New Jersey Bureau of Records Management