The Daily Management of Records and Information

By David O. Stephens, CRM, FAI

IIMC Records Management Technical Bulletin Series • 2012

Records Management Technical Bulletins

This publication, one of sixteen bulletins in the *2012 Local Government Records Management Technical Publication Series*, is a joint effort of the Municipal Clerks Education Foundation (MCEF), the International Institute of Municipal Clerks (IIMC), and the National Association of Government Archives and Records Administrators (NAGARA). Funding for this project was made available, in part, by a grant from the National Historical Publications and Records Commission.

The Municipal Clerks Education Foundation (MCEF), established in 1984, is a tax-exempt, nonprofit foundation under Section 501 (C)(3) created to raise funds for its partner, the International Institute of Municipal Clerks. IIMC uses these funds to promote, train and educate Municipal Clerks, making them proficient in the services they provide for the citizens of their community. MCEF is a diverse team of volunteers who are passionately committed to helping IIMC pursue its educational objectives.

The International Institute of Municipal Clerks (IIMC) is devoted to advancing the professionalization of the Office of Municipal Clerk and improving the efficiency of municipal government. The IIMC provides its members with educational, conference, reference, research, and informational services designed to keep them informed of changes in the professional community.

The National Association of Government Archives and Records Administrators (NAGARA) is a professional association dedicated to the improvement of federal, state, and local government records and information management programs and the professional development of government records administrators and archivists.

The National Historical Publications and Records Commission (NHPRC), a statutory body affiliated with the National Archives and Records Administration (NARA), supports a wide range of activities to preserve, publish, and encourage the use of documentary sources, created in every medium ranging from quill pen to computer, relating to the history of the United States.

Preface

Like every organization, local governments create and maintain large quantities of records. Many of these records not only are of great value to the local government, but also are of concern and essential to the citizens of the community. Federal and state-mandated program requirements, changes in growth and development patterns, expanded service needs, the use of computers and other technologies for creating and using information, and the proliferation of copies in various formats, have all contributed to this enormous accumulation of records. Each publication is intended to make available to local governments the basic principles, policies, and guidelines that should be followed in establishing a sound records management program and in carrying out sound records management practices.

The series is intended for local officials, with limited resources, who lack formal records management or archival training but who have custodial responsibility for records. These local governments include townships, villages, cities, counties, school districts, and other local political subdivisions and special-purpose districts. Each of the following publications in the series includes a bibliography that refers to other reading for more detailed information and guidance.

Overview:

Starting a Records Management Program, The Daily Management of Records and Information, Making Your Records Management Program Successful, Managing Records on Limited Resources, Funding Your Records Management Project

Creation, Collection and Storage:

Identifying and Locating Your Records, Establishing Records Retention, The Selection and Development of Local Government Records Storage Facilities, Developing a Records Storage System

Preservation, Promotion, Use and Access:

Archives for Local Governments, Protecting Records, Using and Storing Microfilm

Care, Management, and Preservation of Electronic Records:

E-Mail Management, Selecting and Using Document Imaging Systems, Managing Electronic Records, Preparing for E-Discovery

Copies of these bulletins are available on the IIMC and NAGARA websites.
IIMC at www.iimc.com • www.nagara.org

Acknowledgements

Meet the Author: David O. Stephens, CRM, FAI

David Stephens is senior vice president for records management consulting at Zasio Enterprises, Inc., a leading records management company. His most recent book is Records Management: Making the Transition from Paper to Electronic (ARMA International, 2007). He has spoken to thousands of records managers throughout the United States and in some twenty countries in Europe, Asia, Latin America and the South Pacific. Mr. Stephens is a Certified Records Manager, and in 1989-1990 served as President and CEO of ARMA International. He was inducted into the Company of Fellows of ARMA international in 1992.

Editor: Dr. Julian L. Mims III, CRM, CA

Julian Mims is a career archivist, records manager and educator. He directed the local records program at the South Carolina Archives from its inception. He was in charge of the Long Island office of the New York State Archives and Records Administration (NYSARA). As a Vice President and Award of Merit winner of ARMA International, he helped to found a record ten ARMA chapters. Dr. Mims is the author of the International City/County Managers Association (ICMA) best-seller, *Records Management: A Practical Guide for Counties and Cities*, and was editor of ICMA's *Electronic Records Management*. Earning a doctorate from the University of South Carolina in 2001, he has taught at six colleges and universities.

Special thanks to the support team:

Dale Barstow Project Co-Director and MCEF President, Municipal Code Corp., *Tallahassee, FL*

Paul R. Bergeron, MMC, CA Project Co-Director and NAGARA Liaison, Office of the City Clerk, *Nashua, NH*

Marian Karr, MMC MCEF Treasurer, Office of the City Clerk, *Iowa City, IA*

Chris Shalby IIMC Executive Director and IIMC Liaison, *Rancho Cucamonga, CA*

Citation example: Author Last Name, Author First Name. "Title of Bulletin." Local Government Records Management Technical Publication Series. Ed. Julian L. Mims III. Rancho Cucamonga, CA: MCEF, IIMC and NAGARA, 2012. Print (or Web. Date of Access).

Table of Contents

Introduction

Most Technical Bulletins concern large-scale initiatives that local governments should implement to improve recordkeeping. Another aspect of recordkeeping is equally important – the *daily management* of records and information. Each employee should take these actions every day to improve the quality of jurisdictional recordkeeping.

This bulletin provides guidelines for departmental employees. This guidance is also for those with overall responsibility for the jurisdiction's records so that these daily tasks can be effectively planned and managed – every year.

The primary goal is to describe practices in clear and practical terms, so that all employees may daily create records in a professional manner. This will meet standards of best professional practice.

Why are daily recordkeeping tasks so important? Because records management runs local government. A most eloquent statement of the need for professional local records management was made by Dr. H. G. Jones, former head of the North Carolina State Archives. Dr. Jones wrote:

"Public records are public property, owned by the people in the same sense that the citizens own their courthouse or town hall, sidewalks and streets, funds in the treasury. They are held in trust for the citizens . . . As public property, public records may no more be altered, defaced, mutilated, or removed from custody than public funds may be embezzled or misappropriated. Indeed, because [public] records document the conduct of the public's business – including the protection of rights, privileges, and property of individual citizens – they constitute a species of public property of a higher value than buildings, equipment, and even money, all of which usually can be replaced by the simple resort to additional taxes. *It is the unique and irreplaceable nature of records that give them a sanctity uncharacteristic of other kinds of property and that account for the emergence of common-law principles governing their protection.*"

In today's electronic era, Dr. Jones' message applies with equal weight and force.

The Changing Nature of Public Recordkeeping

Local government is experiencing the biggest "paradigm shift" in recordkeeping history. The all-digital office is no longer a question of if, but when. Still, local governments must manage dual or even multiple media types in parallel, side-by-side, on a daily basis. This technical bulletin, and the others in this series, help do this.

Media Independence of Policies and Procedures

Paper-to-electronic brought changes in policies/procedures. Today most records that can be considered as "official" now may exist only in electronic format. Perhaps ninety percent of *all* organizational records are now "born digital"; they may never print to paper, except for storage and retention. Technical Bulletins address the new realities of government record keeping.

Translating Policies and Procedures into Daily Practice

What, then, should local government employees do, daily, to manage records professionally?

- Exercise due care in creating all governmental records.
- Create full, complete documentation evidencing government business.
- Organize / identify records for ready retrieval to support efficient government operations.
- Retain / store records only in managed repositories according to and in accordance with sound records management principles and practices.
- Organize / manage recordkeeping systems so approved retention rules / policies are effectively implemented.
- Retain / discard duplicates/drafts /working papers in a manner reflecting their use / value.
- Retain email as records, in accordance with sound records management principles / practices.
- Conduct all document imaging operations so integrity of scanned records is assured.

- Protect / safeguard all vital records against loss / destruction.

Recommended practice for each of the above comprises the remainder of this Technical Bulletin.

Disclaimer: existing state / policies are the operative requirements for your jurisdiction.

Chapter 1

Records Creation, Collection and Storage

Local government records are created / collected each business day. Thus, daily records management activities must be done properly – by all employees who create and / or maintain jurisdictional records. Following are recommended practices toward this goal:

Records Creation

Public business results in records, as evidence. It is important that records be complete, true and accurate, and reflective of professional business practices.

Writing a paper letter forced thoughtful, contemplative, and careful wording/ construction. Moreover, business letters / office memoranda frequently involved sign-off approval. The result was often highly formal / meticulously constructed documents, with equally formal replies. Most e-mail / electronic messages, however, lack the formal attributes of former paper. Such messages may be "on the fly"; they tend to be casual, spontaneous, and informal. There is risk: ill-considered or intemperate remarks reduced to writing can cause trouble!

In daily creation of records, no information should be construed as false or misleading. All business documents should be thoughtfully, appropriately, and accurately worded to reflect concern for proper and ethical business practices. No language should be construed as misleading, inaccurate, fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, abusive, libelous, defamatory, or in violation of laws or regulations. Writing should reflect positively on you as an individual or the government for which you work. Rule: write only as you would for the front page of the newspaper!

Completeness of Documentation

Documentation related to business should be complete; no holes or gaps should appear in the record. Make sure that all:

1. Business matters are written to a formal record for the files.
2. Documentation reaches the proper filing destination for retention.

Departments should conduct periodic self-assessments to ensure rigid daily adherence to these rules. Annual assessments – more often, if needed – are warranted. Holes or gaps in records must be closed immediately.

Organizing and Identifying Records

Records, once created, must be organized for ready retrieval in an efficient operation. Created daily, records should be earmarked for safe storage.

"Unstructured" records are created in electronic form using desktop software applications - - word processing documents, spreadsheets, reports, presentations, for example. Focus on them, since they are a significant retrieval challenge for local government.

Good Daily Filing Requires a Good File Plan

Create a file plan – a single most important step. A one-time, rather than a daily, task, it is nonetheless extremely important. Why? Without a file plan, every act to organize and identify documents for filing is based on an arbitrary decision. Resulting files may become fragmented and difficult to retrieve. File plan guidelines follow.

A file plan (a "document classification scheme" or "taxonomy") is a written plan for organizing records and information. It applies a logical scheme of major and subordinate subjects or topical categories, arranged in hierarchical fashion from general, to specific. A file plan has predefined subject or category terms that encourage document storage / retrieval by department employees. Such categories impose logic / order upon organizational files so they may be found quickly.

Category hierarchy shows major / subordinate functions of local government business. Standard categories reflect information organized in a multi-tier "grandparent-parent-child" arrangement:

- First level – Primary: Major business functions / processes
- Second level – Secondary: Subordinate business functions / processes
- Third level – Tertiary: Individual document types

When selecting the subject / topical categories that comprise the file plan, follow these guidelines:

- Categories should serve departmental employees. Fully customize them to reflect the document retrieval requirements of each business process and workgroup.
- Base categories on comprehensive identification of set records order by logical groupings. Certain records "belong" with other records; thus, meaning / context can be compromised or destroyed if their relationships are not mirrored by the hierarchy of categories in the file plan.
- Select primary / subordinate categories to channel how information will be segmented / used. Categories must not be too broad or specific. If they overlap or fail to cover a subject / functional area, users may experience retrieval difficulties.
- Categories must encompass all subcategories. For example, everything below "eye diseases" must be an eye disease.
- Documents place higher in the hierarchy; more specific documents, place lower. Ideally, a document can be filed only one place. The goal is mutually exclusive categories for content.

Finally, file plans should be *media independent*; representing the record's intellectual content, regardless of storage media. Thus, filing guidance is equally applicable to paper-based or electronic environments.

Naming Files When They Are Saved

File plans provide "umbrella" categories under which records are classified. Nonetheless, files must be assigned names when they are saved. Within the file plan schema, departmental discretion best earmarks individual documents for effective retrieval. Importantly, *filenames must capture the essence of the document*. Further, names should facilitate future retrieval – even by persons who did not select the file name. Finally, when choosing filenames, err on the side of brevity – twenty-five characters maximum.

Creating and Capturing Other Metadata

For paper records, a good filename is the only type of "metadata" that is needed for retrieval. Physically placing the record in a logical sequence in a drawer or on a shelf ensures that the record can be found when needed. With electronic records, however, the situation is different; other metadata is needed. "Metadata" simply means "data about data;" other indexing attributes may be needed to retrieve / manage the stored records over time.

Metadata may describe how, *when and by whom the record was collected, created accessed or modified, what the record is about, and how it is formatted.* Document indexing attributes are best captured by the document creator / author. The best time to capture them is at document creation. If metadata is not captured then, chances are it never will be. Specific metadata attributes are captured from application to application (and system to system) A list of common metadata attributes includes:

- Unique record identifier
- Date and time of record capture
- Record creation date
- Record title or description, to include its subject content
- Name of record creator
- Name(s) of related party or parties
- Record format
- Record handling, usage or processing requirements
- Record retention / disposition requirements

Identify required metadata for every system of records in your department. All persons who create, process and save records into the system or storage repository must capture such data daily, every time a new or changed record is filed and saved.

[See the Technical Bulletin on *Identifying and Locating Your Records*.]

Storing Records in Managed Repositories

Having chosen good filenames and other indexing metadata for records, consider the characteristics of the repositories into which they are saved and stored. First, focus on what not to do. Consider the analogy of your closets at home. While some are better managed than others, often the contents of these facilities consist of items placed there arbitrarily, with little regard for how long, or even whether, such storage is appropriate. Organization of the items is similarly random and there is no index to the contents; retrieval is, therefore, "hit or miss".

This is essentially unmanaged repository storage. Managed storage is the opposite. Every local government records storage repository should store only content that is designated for such storage. Think (1) organize and (2) how long?

Per strict policy and practice as part of their daily work, local government employees should file / store electronic records they create to an approved, formally managed recordkeeping system. These basic records management principles are common sense. Why do most records storage repositories appear unmanaged?

Following are types of local government storage repositories that are frequently unmanaged, or at least under-managed. Better management practices will help these repositories, particularly with content retention. Email systems, "will default" repositories for many local government communications, are under-managed. This problem – and recommended solutions – is addressed in the next chapter.

SharePoint Sites

SharePoint, a software application of Microsoft Corporation, is heavily used by many local governments. These systems provide advanced functionality for workgroup collaboration, and are often used by project teams for storage of project related records. Frequently, electronic records created by common office applications, such as MS Word documents, Excel spreadsheets, and PowerPoint presentations are stored in these environments. SharePoint is often used for Internet, intranet, and extranet sites.

Frequently, however, SharePoint sites and their contents are not administered as "managed resources" in accordance with sound records management principles. Common problems with SharePoint sites include:

- Active / inactive sites co-mingle on the same servers.
- Unclear responsibility for site ownership and administration. Retention polices / practices on site content are absent; in practice, both site and content are retained indefinitely.
- Nearly always, site content does not comply with approved retention rules / policies.
- SharePoint may lead to automatic identity/clean up of unused sites. Yet this capability is often misunderstood or improperly used.
- Blogs, wikis, or other information not covered by retention schedules.

If SharePoint site(s) exhibit such problems, contact site administration, the Records Manager, or the IT department to resolve them. The site administrator should perceive official copies of records that must be kept per retention schedule. This is generally no easy task. Most sites contain a wide variety of record types with differing retention periods, and an item-by-item application of these retention periods will not be feasible. Thus, a simpler strategy is required. Recommended:

- Retain SharePoint sites for the predetermined uniform period after project termination (or related activities to which the sites relate, or after the site is declared inactive).

- A uniform retention period of seven years after a site is declared inactive should be adequate for most of the site's content.
- The site's owner should identify records that must be kept longer than this retention period. Sites may be designated for permanent preservation, in cases where the records are of historical significance.
- Inactive sites need not be retained online; they can be archived onto magnetic tapes, optical disks, or other removable media for offline retention.

Fileshares

Fileshare management problems, and recommended solutions, are similar to SharePoint sites. "Fileshares" refers to electronic records with defined access privileges that are stored on local government network drives. Local governments heavily use fileshares. They may have many electronic records residing in these types of repositories, often being retained "indefinitely." Records include word processing documents, spreadsheet files, presentations, PDF files, CAD files, digital images, and video / audio clips.

As with SharePoint sites, a uniform retention period of predetermined duration (with a strategy for retaining content of longer retention value) is often the only workable solution for the content residing in existing fileshares. Adopt a reasonable policy that gets the jurisdiction away from indefinite retention.

Records Management Software Applications

A records management software application (RMA) system indexes, tracks and monitors the location / retention status of records – both paper and electronic – throughout their life cycle, and facilitates proper disposition under retention rules / policies. RMA's primary functions are categorizing / locating records, and earmarking records for disposition per retention schedules.

These software applications are inherently "managed repositories." They permit management of saved content in accordance with sound records management principles and disposition of content as authorized by approved retention rules. As such, they are generally recommended for use by local governments.

RMAs manage the lifecycle of unstructured electronic records. Software creates and maintains a searchable repository for these records, including those saved as fileshares, housed in SharePoint sites, or stored in other locations. The repository maintains these records per their retention schedule.

Retention periods can combine elapsed time and specified events - - such as termination/completion of a contract / project, plus a specified number of years. Electronic records saved to these repositories are "locked down" – that is, they cannot be edited, deleted or replaced until their designated retention periods elapse.

In 1997, the U.S. government issued the first standard prescribing functionality requirements for electronic records in records management software applications. The standard is DoD 5015.2 – Design Criteria for Electronic Records Management Software Applications. It has been revised several times.

The DoD 5015.2 standard is implemented via a certification program: software developers who market RMA products have their programs tested / certified as compliant with the standard's mandatory and optional requirements. If your local government contemplates RMA implementation, determine whether the products under consideration have been certified under this standard.

Many people feel that computer software – including RMA solutions – is "magic"; once installed on servers, all recordkeeping problems will miraculously vanish from the organizational landscape.

No. RMA software seldom delivers immediate results. Organizations do not control documents / data sources well enough to identify quickly / consistently what should be managed as a record, and what should be discarded. Best-path to successful RMA deployment is a phased implementation, beginning with pilot installations at the workgroup or departmental level. Moreover, most local govern-

ments should anticipate a minimally invasive solution wherein users integrate technologies and tools that are already in place.

[For further information, see the Technical Bulletins on *Developing a Records Storage System and Managing Electronic Records*.]

Chapter 2

Records Retention and Disposition

We discussed how records, once created, should be organized / stored for effective retrieval / use in managed repositories. This retrieval and usage occurs mainly during the active life of the records. Most local government records – generally between two and ten years – transition from active to inactive in their lifecycle. They should be discarded if they have no further value. If records have continuing value, they should be retired until their value expires entirely. Finally, a small percentage of local government records never lose their value and must be retained permanently for operational or historical reasons. Managing these aspects of the lifecycle of local government records is the subject of this chapter. In records management practice, this is "records retention and disposition."

"Rules" of records retention for local governments are normally established by state mandate. Less frequently, local governments have created their own customized rules for records retention, based on the state mandates. A local government records retention schedule, and any related narrative policies, should be regarded as the official, approved source for policy guidance in records retention. The challenge is to implement retention schedules effectively. This chapter provides guidelines for doing this.

Our primary goal is to provide a set of recommendations which, if successfully implemented, will enable the government to get as close to "perfect" in records retention as possible. This means as close as possible to "full compliance" with the jurisdiction's approved records retention rules. This, in turn, means that the government is retaining only those records prescribed by the retention policy rules for as long as the rules specify that they must be retained. All other records will have been discarded, systematically and lawfully, when the records have aged to the times specified by the retention periods in the records schedule.

Where the jurisdiction has paid little attention to these matters, its degree of compliance is likely to be very low, since the behavioral tendency of many employees to retain records "indefinitely" is very strong. This is bad because indefinite retention of records constitutes a liability for the government. Excessive retention of records results in additional storage costs, plus increased requests of the public (such as freedom of information), and legal discovery requests of attorneys and courts. Finally, for electronic records, excessive retention can sometimes result in retrieval delays and other system performance issues, greater data backup costs, or other negative consequences.

Each department should make systematic records retention a continuing priority and assign appropriate resources to it. The department head should designate a departmental records coordinator who will have operational responsibility for records related matters, to include compliance with state and local policy mandates.

Beyond these measures what, then, is required for the government to get as close to perfect as possible in records retention? To achieve success in records retention, rules contained in the retention schedule, and accompanying policies, must be applied to the jurisdiction's six major recordkeeping environments. These are:

1. Paper records of official character retained in departmental filing systems
2. Duplicates, drafts and other personal working papers, whether in paper or electronic form, retained in office areas and cubicles
3. Electronic records created daily by individual employees, utilizing common office software applications, and retained on local hard drives, SharePoint sites or network servers

4. Email messages received / created daily by individual employees and retained on dedicated email servers
5. Structured data retained in rows / columns of database applications, typically managed by IT departments
6. Boxed / stored paper records that are retained in records centers or, less formally, in attics, basements, closets or other storage facilities

Retention rules applied to each of these recordkeeping environments constitutes the balance of this chapter. Close examination of these six environments will reveal that the first four contain records that are under the direct custody and control of individual departmental employees. Therefore, effective strategies for complying with retention rules must be applied at this level. For paper / electronic records, a combination of daily and annual retention implementation strategies are required. These are described below.

Annual Retention Days

In order to be successful in records retention, individual employees should be required, by jurisdictional mandate, to review their records annually and apply retention rules – fully, faithfully and diligently. If every employee who creates and maintains records devotes at least one day per year to retention tasks, most records eligible for destruction will have been eliminated – properly and lawfully under approved retention rules. Thus, annual Records Retention Days are recommended as best practice. From experience, these dedicated days are essential in order to provide a systematic and comprehensive approach to the application of retention rules to the jurisdiction's various recordkeeping environments. There simply is no better alternative means to achieve success in records retention.

During these dedicated days, departmental employees should be individually responsible for reviewing the paper records housed in filing cabinets, on open shelves and in other equipment, comparing their dates to the retention periods in the approved / current schedule, and discarding those which have aged beyond their authorized period of retention. This chapter provides guidance on records disposal to ensure that integrity of sensitive information in the records is not compromised.

Semi-active records require continuing retention in an offsite storage repository. They should be properly boxed, without disturbing their proper arrangement / sequencing, and described in sufficient detail to permit effective retrieval, even by persons who did not create them. Different record types having varying retention periods should never co-mingle in the same storage cartons. Only official record material should be transferred to storage – never duplicate records or personal working papers.

During annual records retention days, electronic records created by individual employees, utilizing common office software applications, should also be reviewed and deleted if their retention periods have lapsed, regardless of whether they reside on local hard drives or on network servers. These retention actions should be executed, even if the retention actions described in the previous chapter for SharePoint sites and network fileshares are performed.

Electronic records stored on removable media, such as USB drives or portable hard drives, should be similarly reviewed and eligible items deleted. For electronic records residing in records management software applications (RMAs), no such actions should be required since software should have the requisite functionality to execute approved retention rules. Departmental employees should confirm with the system administrator that retention rules are properly applied.

Duplicates, Drafts and Working Papers

Annual retention days bring effective compliance with retention rules, yet departmental employees exercise retention actions *daily:*

- **Duplicate records** – Designate one copy as the official copy, to satisfy retention mandates. A routine stipulation, for each record identified within the jurisdiction's retention schedule, will do this. All copies other than the official copy

will then be considered duplicate records. A duplicate record replicates the full content and functionality of the official copy. It may be in the same, or different, format or medium as the official copy. According to local government policy, duplicate records should be discarded when no longer needed for their created purpose. Employees should be required to carry out these disposal actions every working day. Per policy, duplicate records should not be retained longer than official copies that contain the same information.

- **Drafts** – A draft is a preliminary version of a record; it will be supplanted by a subsequent, final version. For retention purposes, the final version is considered the official copy. As provided by jurisdictional policy, drafts should be discarded when no longer needed for the purpose for which they were created. Employees should be required to dispose of drafts daily.
- **Working papers** – Short-term, transitory working papers, generally have no business value beyond their immediate usefulness. These records, too, should be discarded daily. This practice should apply to working papers in all formats, including word processing files, spreadsheets, and other computer files.

Email

A significant percentage of local government work – and resulting records– are created and retained in email. Unfortunately, good records management practices – and retention rules – often are not implemented in these environments. For many local governments, email remains the worst managed form of records. Many e-mail users retain hundreds, even thousands, of e-mails, in the messaging environment. This is not best but worst practice!

The single most important principle: use e-mail for current communications only. A top local government priority: ensure that the messaging system is not unwittingly morphed from an "e-post office" into an unmanaged digital archive.

These systems should not be used as repositories for retained, official records. In many email environments, however, indefinite retention is the prevailing practice, without regard to the content value of the messages, their status as official records, or their retention requirements. In other situations, messages may be deleted and purged, arbitrarily and at the discretion of employees, again without regard to rules or policies. In other words, often there are no safeguards against the deletion of email messages before their retention value expires. Conversely, often there is no mechanism for ensuring the deletion of messages which have no further retention value. In short, e-mail - - commonly - - is not managed, and the resulting price of mismanagement could be exorbitant.

What is needed is an email system which provides reasonable assurance that messages will be available when needed for decision-making, project management, transaction processing, and other governmental purposes. To be legally acceptable, an email archiving / retention system and its governing rules should consider state-imposed mandates for records retention. It must demonstrate reasonableness and good faith. Finally, it must be practical to implement, and must operate with a minimum of decision-making and judgment by users.

Good news. Each of these goals can be achieved by implementing an email archiving software system governed by good retention rules. These aspects of recommended email management and retention are discussed below.

Email Archiving Software: Common Functionality

Your jurisdiction must consider an email archiving system. Most email archiving solutions combine the following features:

- Automatic or user-initiated transfer of messages and their associated metadata from mailboxes or external files to the archiving repository.
- Integration with email client software for transparent access to archived messages by mailbox owners and other authorized persons.
- Full-text indexing of messages for advanced content retrieval.

- Cross-mailbox searching by authorized persons subject to restrictions determined by policy.
- Ability to delete messages and attachments by age or file type based on predefined retention rules.
- Litigation or audit holds for specific mailboxes or messages.
- Single-instance storage (de-duplication) of messages and attachments received by multiple employees, including messages that originate internally or are received from external organizations.
- Compression of messages and attachments to conserve storage space and to prevent unauthorized access by persons external to the organization.
- Replication of folder and subfolder structures from user mailboxes.
- Ability to separate message and attachments for storage external to the centralized repository.
- Ability to generate reports and graphs about email patterns and traffic in aggregate or for individual users.

Your local government should consider an email archiving solution and proceed to acquire one, via competitive procurement, if the need for it is adequately justified.

Email Retention Rules

With a good email archiving software solution in place, it is critical that message retention be governed by effective retention rules. Consider:

- **Email of transitory value** – Email not required to support local government business. Further, such messages are not required to ensure complete documentation of any records in the local government retention schedule. This may be 20 to 40 percent of the total email messages. Employees should be required by policy mandate to delete such messages each workday. This may require ten to fifteen minutes per day. By policy, maximum retention for such messages should be ninety days.
- **Email of routine business value** – The standard retention period for this email should be established by jurisdictional policy. Volume may be 50 to 60 percent of the total. Three to seven year retention is recommended. However, the state retention period for "correspondence" prevails. The email archiving system automatically transfers, without user involvement or decision-making, all e-mail remaining in employees' mailboxes when messages have aged for a certain number of days (90 days is commonly adopted) to the archival repository. There they remain for the duration of the approved retention period. Then messages will be purged, without user intervention or decision-making. To implement this retention strategy, an email archiving software solution must be installed.
- **Email of long-term retention value** – must be retained longer than the "routine business value" rule above, as specified by the jurisdiction's retention schedule. These messages should be saved in a separate repository that can satisfy their retention period. They can be printed and filed in paper format; alternatively, they can be saved to another software application. RMAs and Enterprise Content Management (ECM) solutions are ideal for this purpose. Employees should take such actions to ensure that this occurs on a daily basis. Usually such email encompasses no more than ten percent of the total. Depending on their job responsibilities, many employees have no email of this type.

Recap: an email archiving system plus the above retention rules equals minimal employee decision-making. Each day employees should delete transitory email. If certain messages require retention beyond "routine," staff must save them to a proper repository where these retention requirements can be satisfied. All other retention actions are handled automatically by the email archiving solution. With combined technology / employee practice, local government control of email can rise to the level of best professional practice.

[For further information, see the Technical Bulletin on E-mail Management.]

Database Applications

True, advances in data storage technology are epochal. Yet, to say that indefinite retention of data residing in local government database applications "doesn't matter" is like saying costs don't count. Yes, media costs have declined significantly (reducing cost-per-megabyte). However, this does not justify needless or indefinite retention. Nor do these factors invalidate the business case for records retention. In most organizations the total quantity of electronic records is *doubling* every two to three years or even faster. Moreover, in nearly all governmental jurisdictions the total cost of data ownership continues to increase, not decline.

Cost alone dictates that approved retention rules encompass electronic records residing in the jurisdiction's database applications. The major problem, however, is that some applications lack the requisite functionality to execute retention rules. Simply stated, software running the applications must have the capability to recognize and "tag" expired data as per the retention rules, and then to carry out purge routines to discard the data. The information technology department should determine whether the application can be modified through custom programming. Do so at the earliest practical opportunity, especially when each application is upgraded to a new hardware or software environment.

If modification of existing applications is not feasible, earmark data for indefinite retention, and reconsider the application's retention status later. Technology upgrade cycles average 5 years. Most applications can then be made "retention-capable / compliant." Of course, policy must require new applications to incorporate retention functionality at the time of initial design / deployment.

Boxed and Stored Paper Records

Local government often has paper records housed casually in under-managed facilities (e.g. basements, attics, closets, or warehouses). Retention policy should apply to such cartons. Cartons containing lapsed-retention-period records should be discarded. Those requiring continuing retention should be indexed and described on a software application (RMAs are specifically designed for this purpose), and returned to a managed and secure storage repository for the duration of their retention life.

Where many unmanaged records exist, the jurisdiction should appoint a project team, consisting of designated representatives from each department, to review the records and execute the proper retention actions. One day a month should be devoted to the task until it is done. At conclusion of this update, all boxed / stored records should properly be stored in an environmentally controlled and secure facility; labeled / computer-indexed as to their contents, retention status and future disposal dates.

Manner of Records Disposal

As a matter of policy, destroy jurisdictional records in a manner that is safe and appropriate to the content of the records and to the media on which the records have been recorded. By media type, the following guidelines are recommended:

- Paper records – Shredding, incineration, and chemical disintegration.
- Microfilm / photographic media – Pulverization and chemical disintegration work for microfilm, photographic negatives, motion picture films, or other photographic media.
- Magnetic media –Degaussing (bulk erasure), erasure by sanitization software, or reformatting, followed by physical destruction of the media may be appropriate for magnetic tapes, floppy disks, magneto-optical disks, or other removable magnetic media.
- Optical media – Cutting, crushing, pulverizing, chemical disintegration, or other physical destruction of the media is effective for optical disks, including Compact Disks and DVDs.

In systematic execution of retention actions, good practice creates or obtains attestations or certifications that the actions have, in fact, been accomplished pursuant to approved policy, and that no sensitive or confidential information has been compromised.

Compliance Monitoring and Documentation

Local government should conduct regular, periodic departmental audits to determine compliance with state and locally mandated retention rules / policies. Each year, all department managers should be required to certify compliance with retention rules. They should attest full compliance, or if the department is not in full compliance, they should be permitted to request exceptions. All such exceptions, however, should be justified by valid legal or business needs and be properly documented.

In cases where departmental employees do not fulfill their obligations to comply with retention rules, appropriate penalties should be imposed. These should be invoked at the discretion of the supervisor. However, against willful, flagrant and repeated non-compliance, jurisdictions should invoke stringent penalties, including dismissal.

Suspension of Retention Actions

Under jurisdictional policies, daily or other destruction of records with elapsed retention periods should be immediately suspended where records have been or may be requested for use in pending / ongoing investigations or lawsuits. This prohibition should be effected immediately – at the time litigation or an investigation can be reasonably anticipated – not just when records have been requested by subpoena or other official production order issued by legal authorities.

A Sustained, Multi-year Commitment

Full compliance with jurisdictional retention rules usually requires sustained, multi-year commitment. The four content types of records that are under the personal custody and control of individual employees, can achieve full retention compliance in a year or two via an aggressive management initiative. However, to clean out large records centers or storage warehouses and make all the jurisdiction's database applications retention-capable / compliant may require several years of dedicated effort. With the right allocation of resources – people and technology – success in records retention is within reach of every local government!

[For further information, see the Technical Bulletin on Establishing Records Retention.]

Chapter 3

Converting Records from Paper to Electronic Format

Local government digital documents are created by word processing programs, e-mail systems, presentation software, spreadsheet programs, computer-aided design software, or other computer applications. They are described as "born digital." Perhaps 90 percent of all documents are born digital.

Still, most jurisdictions continue to receive paper records from external sources. They are digitally born at the source of creation, but not where they come to rest in local government. Thus, in order to capture this content digitally, these records must be scanned for storage and retrieval as digital images. Alternatively, they can be digitally captured by conversion to character-coded form by key-entry or optical character recognition.

Document scanning operations often occur daily in the routine course of departmental work, they are relevant to daily actions of this bulletin. The important principle: all document imaging / scanning operations must assure integrity of scanned records. As discussed below, scanned records must be complete, true and accurate, accessible, legible and otherwise fully usable for any business or legal purpose.

Imaging and Scanning

Document scanners are computer peripheral devices that convert paper source documents to electronic images suitable for computer processing and storage. Source documents may be typed, printed, handwritten, or hand drawn. They may contain textual or graphic information in black and white, gray tones, or color. The scanning process is properly termed "document digitization." Document scanners are usually the following types:

- Desktop scanners for low-to-medium-volume departmental applications
- High-speed floor-standing models for production-intensive installations
- Duplex scanners for applications that involve two-sided pages
- Flat-bed scanners for bound volumes, and large-format scanners for engineering drawings.

Because the scanned / digitized images are not stored as character-coded documents, they cannot be "full-text searched" using text retrieval search engines. Thus, their retrieval depends wholly on manual indexing processes. Other technologies for content capture include optical and intelligent character recognition (OCR and ICR, respectively). [These are beyond the scope of this Technical Bulletin. See the Technical Bulletin on Selecting and Using Document Imaging Systems.]

Software provided with most document scanners can record digital images in an operator-selected file format. The Tagged Image File (TIF) format or the Portable Document Format (PDF) are recommended for digital images that will be retained as official records, particularly in cases where they must be retained for ten years or longer.

Integrity of Scanned Documents

The digital capture process can be complicated, time-consuming, and costly. The most important principle is that digital images must be faithful reproductions or "true copies" of the pages from which they are produced. A true copy is one that preserves all significant information from source documents as determined by the legible reproduction of all words, numbers or other markings that can be read in the source documents. To ensure this, all scanned images should be inspected – daily, at the time of digitization – for clarity, legibility, and correctness so that the local government can demonstrate the integrity of its scanned records against legal scrutiny or challenge.

Chapter 4

Protecting Vital Records

Vital records are must-have records, essential to local government business operations. If such records are lost, damaged, destroyed, or otherwise rendered unavailable / unusable, the jurisdiction's mission-critical operations will be curtailed, discontinued, or severely disrupted, with resulting financial loss or other adverse business consequences.

Despite data backup routines by Information Technology, most local governments lack adequate protection for essential records. Do yourself a favor: correct this immediately.

In daily recordkeeping, the most important vital records rule is: Never store any vital records of the government in a manner that does not provide for adequate security and backup against the risk of loss. This means two things:

1. If vital paper records have no backup, scan the paper and store the resulting images on routinely backed up servers. Alternatively, where records quantity is small, storage in fire-resistant filing cabinets will provide lesser protection.
2. Never store vital electronic records to local hard drives without backup. All such records should be saved to network fileshares or to other software applications for which backup is routine.

Measures to assure the security of the jurisdiction's vital records should occur daily in every department where such records exist. Each department manager and all employees involved with such records should be individually responsible for these actions.

[For further guidance, see the Technical Bulletin *Protecting Records*.]

To Have Great Records, Here's What You Must Do *Every* Workday

This is a convenient reminder of daily records actions that you must do every day so that you and your department will maintain records in a professional manner. Please distribute to all employees. For additional information, see this and other Technical Bulletins in this series.

Have you each day . . .

- Documented, fully and completely, all official transactions of government business accomplished for your department, and done so in a manner that reflects professionalism for the government and for yourself?
- Saved all records / files / information in accordance with a formal, approved file plan, developed in a manner that is fully customized to the needs of your department and / or the jurisdiction?
- Assigned all filenames to saved records / documents / information using terms designed to facilitate their future retrieval, including by persons other than you?
- Saved all records / documents / information solely to storage repositories that are managed in accordance with approved records management policies / rules of the jurisdiction?
- Selected and assigned metadata fields / attributes that are needed to manage / retrieve saved electronic records for the duration of their approved retention periods?
- Discarded duplicates, drafts / working papers daily, as soon as they are no longer useful in accomplishing departmental or jurisdictional business?
- Deleted email of transitory value?
- Saved email of routine or long-term business value to managed repositories in which their retention requirements can be satisfied?
- At the first sign of trouble, halted the disposal of any records related to litigation / audit / investigation, even if approved retention periods have lapsed and they are not (yet) under subpoena?
- Disposed of all jurisdictional records for which you are responsible in a manner appropriate to the level of confidentiality of their content?
- Daily scanned (or otherwise converted from paper) to digital format local government records, for which you are responsible, in a manner to ensure that they are complete, true and accurate, accessible, legible and otherwise fully usable for any business or legal purpose?
- Saved / stored all vital, mission-critical records solely to repositories that are fully backed up, secure and protected against the risk of loss or inadvertent disposal from disaster or other causes?

Endnotes

[1]Jones, H. G., Local Government Records: An Introduction to Their Management, Preservation, and Use (Nashville: American Association for State and Local History), 1980, pp. 23-24.

[2]Lamont, Judith, "Unlocking Enterprise Data: Metadata Holds the Key," KMWorld, April 2005.