Electronic Records Management in the City of Philadelphia

I. Introduction

Electronic records are records that contain machine readable information. The information may be text, numbers, graphs, line drawings, pictures, images, or sound. Examples of electronic records include word processing files, spreadsheet files, presentation graphics, electronic images, databases, audio or video recordings, voicemail, and e-mail. Electronic records occupy media such as magnetic disks or tapes; audio or video cassettes; and compact or optical disks.

Electronic records comprise a larger and larger part of most departments' information assets and are included under the Philadelphia Home Rule Charter's definition of public records. Electronic records are also covered by the Uniform Records Management Policy (Executive Order 6-92), signed by Mayor Edward G. Rendell in 1992. This policy makes each City department responsible for its own records assets including electronic records and reinforces the Department of Records' mandate to provide City departments with leadership in sound records management practices.

Electronic records raise issues not found with paper documents. Their management requires an understanding of systems used to create and retrieve electronic records as well as the media used to store them. This technical leaflet provides guidance to agency personnel responsible for managing their departments' electronic records and presents information helpful to understanding electronic records systems. As explained later in this leaflet, the designated Records Management Officer (RMO) and Records Management Liaisons (RMLs) from each agency consult with the Records Management Unit of the Department of Records to clarify records management practices related to electronic, as well as paper-based, public records.

II. Issues for Managing Electronic Records

Personal computer technology has greatly expanded ways to create, edit, maintain, and distribute the records of City government. Unlike early computer systems, which were centrally located and managed by a data processing unit, today's systems are dispersed throughout a department. Several issues surround the management of electronic records:

Ownership

Personal computer users should not view the electronic records they create as personal files to be stored, discarded, or otherwise managed as they see fit. Electronic records are considered property of the City of Philadelphia.

Retention

Electronic records are subject to the same retention requirements as paper records and are governed by records retention schedules developed by the Records Management Unit in cooperation with individual City departments. (For more on Records Retention Schedules see Procedural Guide to Records

Management in the City of Philadelphia). An important consideration is the relationship of electronic records to the paper documents produced from them and the need to coordinate retention for both paper and electronic versions.

Access and security
Control of access to public electronic records depends on the time frame surrounding those records retention. Some electronic records may be considered vital to continued operations in event of a disaster. These must be regularly backed up with back up copies stored securely off-site. Other electronic records may have historic value and require special handling to ensure preservation. Even routine electronic records with shorter retention periods must be protected from easy access lest they be altered accidentally or by design, thereby changing them forever.

Organization
It makes sense to organize electronic records so that they are easy to maintain. Official records can be lost if they are poorly organized, saved using unintelligible names, or stored improperly. Consistent naming techniques and standard directory structures are helpful in managing electronic records. The Citywide and agency-specific records schedules provide a useful classifications for organizing electronic records.

III. Records Management Officer's Responsibilities
The Records Management Officer (RMO) is responsible for ensuring that electronic records are managed in compliance with City, State, and Federal statutes. This is accomplished by adherence to policies issued by the Records Management Division of the Department of Records. Like paper records, electronic records are a public resource that support the mission and operations of the department and City government. Electronic records are subject to the same requirements regarding public access, privacy protection, audits, authenticity, retention, and disposition as paper documents.

The RMO enforces policies regarding all aspects of electronic records, and issues directives specifying who has the authority to create, name, alter, and delete documents on electronic systems. The RMO is responsible for consistency of electronic filing techniques, including standardized directory structures and naming conventions.

Working with the Records Management Unit, the RMO establishes retention periods for all electronic records to ensure their orderly preservation or destruction according to the City of Philadelphia's Records Management Program. Working with the Mayor's Office of Information Services (MOIS), the RMO establishes security standards and back-up procedures for all electronic records.
The RMO is responsible for understanding electronic records management requirements, and for communicating them to department staff.

Help in meeting these responsibilities is available to Records Management Officers through the Records Management Unit. The Records Management Unit can be reached at 686-2284. The Mayor's Office of Information Services can provide assistance regarding security of public electronic records at the enterprise, database, application, and end-user levels and can be reached at 686-8213.

IV. Electronic Records Management Procedural Guidelines
In order to manage electronic records in compliance with the City's Records Management Program, Records Management Officers are advised to:

1) Create a controlled central repository for electronic records, and require staff to store all official records there. Designating specific drives for electronic records storage can aid this process. Drives are the equivalent of on-line filing cabinets. Within the City of Philadelphia, some PCs have their own internal storage capacity, called a hard drive, and can save work on the individual computer. Networked PCs may not have internal storage and work is saved on shared storage devices sometimes called network drives. Network drives can be segregated according to the individuals or departments permitted to access them.
2) In a networked setting, one drive can serve as the repository for all official documents, while another serves as personal work space for drafts or working documents. The final version of all documents, as well as any document which has been forwarded for review or transmitted outside the office should be stored on the network drive designated for official documents.
3) Develop standard naming conventions for directories, subdirectories, and documents.

In electronic systems, the directory structure is a way to store items on the hard drive in an organized fashion, just as you would place paper documents into file folders in a filing cabinet.

Directories are like electronic file folders. Standard directories can serve the same purpose as file folders that have been designated to hold specific types of material relating to one project, topic or task. For example, the directory PRISPROJ contains only files relating to the Northeast Prison Project. Directories can be subdivided into subdirectories. Subdirectories provide a convenient way to navigate through a directory. For example, the statement N:\CITYREP\SISCITY\BROCHURE.DOC tells that on drive N in the City Representative's directory there is a subdirectory for the Sister Cities Program that contains a document used as a brochure.

Naming Documents
Consistent document naming conventions make it easier to find and share documents while they are active and facilitate purging documents from the system when they reach the end of a retention period.
All electronic systems require that new files be named in order to save them. File names consist of:
    Document name
    usually eight alpha/numeric characters
    Delimiter
    usually a " . " (pronounced "dot")
    Extension
    usually three additional characters

One common practice in file naming is to use the first two characters of the file name for the initials of the addressee, the next six characters for the subject of the document, and the extension to indicate the document type (e.g. letter - "LTR", memorandum - "MEM", report - "REP", etc.). For example, a document named JSBUDGET.MEM indicates a memo sent to John Smith regarding the budget.

Newer office systems permit more information to be captured when the document is saved. For example, Microsoft Word for Windows and WordPerfect routinely allow users to name a document using the 8-dot-3 method shown above, then presents a second screen to record document title, subject, keywords, and comments if desired. While these are useful for finding documents stored on the system, they are of no help when documents have been saved on diskette, since diskettes capture only the 8-dot-3 name. In Windows 95 with the software designed for it, documents can be named using up to 255 characters all of which are captured on diskette.

C. Develop procedures for managing inactive and obsolete electronic records.

Inactive records are those associated with matters than have reached completion or closure. Too often, inactive records accumulate on the system, cluttering directories and occupying storage space until capacity is reached.

A plan for the periodic removal of inactive records from the system, based on the department's records retention schedule, is advised. Records Management Division Procedure 1995.4 Disposal of City Records in an Originating Unit applies to the disposal of electronic public records and requires appropriate paperwork be filed with the Records Management Division. Note that inactive records may still have legal or historic value and they may still require off-line storage. Off-line storage keeps records available if needed, but usually means that they are not directly accessible.

Obsolete records are those that have reached full retention according to the retention schedule and may be destroyed with proper authorization. See Procedural Guide to Records Management in the City of Philadelphia for more information about how to gain this authorization.

D. Provide for the security of electronic records.

Sensitive records should be placed in special directories that are not widely accessible. Network directory access can be controlled by the network administrator or by the system administrator who assigns the sign-on password to all users. Access to a PC's own hard drive may be much more difficult to control. It is advisable to copy sensitive records to diskette, lock up the diskette, and delete the electronic record from the hard drive.

All sensitive materials should be password protected. Passwords should not consist of anything that is obvious to others, such as birthdates or the names of children, spouses, or pets. Do not keep passwords written down or taped to the underside of the computer keyboard. Diskettes used to back up sensitive materials should be kept in a locked drawer or cabinet. Keys to such areas should not be kept in desk drawers, pencil cups, or other easily found locations.

Special care should be taken when portable PCs are shared by department members. It is possible to create sensitive material on a laptop PC, then save it to the internal drive where it becomes accessible to the next person who borrows the laptop. Instruct users to copy anything created on a laptop PC to a diskette, then delete the electronic files from the laptop's internal drive.

E. Provide for the management of electronic records on magnetic and other media

Office systems store electronic records on magnetic media, which include hard disks, floppy disks, and magnetic tapes. All magnetic media are erasable and information recorded on them can be overwritten. Magnetic media can be damaged by temperature extremes, improper handling, dust, and spills. Magnetic media also suffer wear from interaction between the media itself and the mechanical devices used to access them. Magnetic media also have implications for records with historic value (see "Historic Records" below). The Records Department is moving its Archives and Records Management functions into a modern facility which may ultimately provide for the appropriate storage of electronic media. In the interim, the Records Management Division has developed Form 82-Misc.-108, "Magnetic Media Pre-Site Visit Screening Checklist" to assist agencies in determining the appropriateness of their current magnetic media storage situations.

Media Labeling Guidelines

All magnetic media, including diskettes, audio, or video tapes must be labeled with their content in order to be useful. The label should also contain the identity of the systems and software used to create them. Labels for magnetic media should include the following:

File list
A list of the files that the medium contains. For example: 1995 Budget documents

Creator(s)
The Department, Section, and Person who created the records (or for whom they were created). For example: Public Property, Engineering, B. Jones

Equipment
The name or type of computer, video, or audio system on which the medium is to be used. For example: IBM PC

Application software used
In the case of personal computer media, the label should contain the name and version number of the application software with which the recorded information is meant to be used. For example: Word for Windows 6.0

Other Media

In addition to magnetic media, electronic records may also be stored on alternative media. These are described briefly below.

Optical Disks
Optical imaging systems store document images on special, non-magnetic discs. An imaging system scans paper documents, then compresses and stores their images in digital form on optical disks. Because the document image is burned into the surface of the optical disk, the image itself is unalterable and uneditable. The system displays document images on desktop screens for processing and reference when necessary, and makes document images available for distribution on standard office networks. Laser printers can produce hard copy of the images on request.

Operations handling large volumes of information which require rapid retrieval and simultaneous access by many people to the same records are likely candidates for optical imaging systems. Imaging systems focus on information access and do not guarantee preservation of electronic records.

Other Optical Media
Compact Disk Read Only Memory (CD-ROM) is a cousin of the compact disks used for audio recordings. CD-ROM is a popular media for distributing published information such as directories and reference works.
Computer Output to Laser Disk (COLD) records formatted computer data onto optical disks. It is useful when many people require fast access to voluminous computer print-outs.

F. Special Requirements: Vital and Historic Records
Vital records are those needed for reconstructing operations in the event of a disaster. Vital records in this context refers to files that would affect the ability of a City department as an entity to continue operations in the event of a disaster. Electronic vital records may involve computers whose processing and storage capacity are greater than that of ordinary PCs. The goal of vital records management is to be able to restore the system and the data. Therefore, vital records must include the applications software, operating system software, and system documentation, as well as the data.

Records identified as vital should be backed up on a regular basis, with back up copies maintained off-site, preferably in a storage facility that is specifically designed to store computer tapes, and output in a protected environment.
Procedures for electronic vital records include:

1. All processing systems should be backed up weekly to magnetic tape using the grandfather, father, and son principle. This means that three separate tapes are kept and rotated. The current week's backup goes onto the grandfather tape. Next week's data go on the father tape. The third week's data occupy the son tape. The fourth week's data begins the cycle again by overwriting the grandfather tape.

2. Hard copy computer output considered vital should either be stored off-site as paper, or as computer output microfiche (COM). This technique converts magnetic tape to indexed microfiche and is done by outside service bureaus. Properly handled and stored, microfilm and microfiche can last at least 100 years. Microfilm storage facilities, such as National Underground Storage, ensure optimal environmental storage conditions for such COM output.

3. Note that the IRS requires one set of computer data containing accounting and tax information plus one copy of the visible output (e.g. printed report or computer output microfilm) be maintained as records under the Internal Revenue Service's Procedure 91-59. For assistance with back up of vital electronic records, consult the Mayor's Office of Information Services (MOIS).

V. Historic Records

Historic records form the basis of what future generations will know and understand about the City of Philadelphia. Historic records have enduring value for legal, historical, public policy, or social science research. According to the Records Management Division's stated mission to ensure ". . . the continued use and accessibility of government records for as long as they continue to have value to the government, the citizens of Philadelphia, and the broader research community . . ." it is essential that they be preserved.

Electronic records that have historic value present two main problems: First, there is no guarantee that the equipment and software used to create them will exist in the future. There are many examples of technologic obsolescence: keypunch cards, eight inch diskettes, beta format videotapes, eight-track tape cassettes, and 78 rpm phonograph records. The equipment to read these media is not generally available today, and the effect is that the information recorded on such media is lost. Second, all electronic storage media, such as disks and tapes, can begin to lose bits of what has been recorded on them over time. For example, there is some evidence that magnetic computer tapes can remain useful for 20 years if stored in optimal conditions, but surveys at tape storage facilities show considerable media deterioration.

While 20 years seems like a long time, remember that in some cases historical records must be usable for hundreds of years. Likewise, some electronic storage media, such as optical disks and CD-ROM, have been in existence less than 15 years, so there is no real way to tell how long they remain viable before losing data no matter what their respective manufacturers claim.

The City Archivist reviews all electronic records before disposition to determine whether they have historic value. In general, it is inadvisable to assume that producing paper copies of electronic records is sufficient for archiving purposes; this is not the case. Many types of electronic records, such as databases, occur in formats in which it is impossible to capture all of the content when reformatting the record to paper output (e.g., record indexing information). An agency's primary responsibility in the preservation of electronic records of historic value is in ensuring for appropriate migration and backup of electronic datasets. Section 9 of the Pennsylvania County Records Manual provides guidance in these matters. Diskettes containing the electronic equivalent of historical records should be labeled and maintained following the guidelines for media preparation given in this publication, as should historical records on media such as video or audio tapes. See the section "Media Labeling Guidelines."

VI. Conclusion

Automation of City offices increases productivity, efficiency, and creativity. The transition from paper to electronic records requires Records Management Officers to be aware of the human and technical issues associated with electronic recordkeeping. The Records Management is available to help RMOs and other agency-based personnel meet the challenges of electronic records management.