DELAWARE PUBLIC ARCHIVES
POLICY STATEMENT AND GUIDELINES

MODEL GUIDELINES FOR ELECTRONIC RECORDS

STATEMENT OF PURPOSE

The Delaware Public Archives (DPA) has issued "Model Guidelines for Electronic Records" for use by all agencies in state and local government in Delaware. These guidelines are intended to guide agencies toward developing electronic records systems that create records to meet the accepted standards for a variety of criteria, including legally acceptable, auditable, and evidential. The purpose of these guidelines is to give agencies some guidance in the development of systems that create electronic records.

Many electronic information systems currently in place throughout government may not be creating legally acceptable records. This is due to the nature of information systems, which store information in discrete chunks that can be recombined and reused without reference to their documentary context. Records systems are slightly different in that they provide evidence of business transactions, and record and preserve the documentary context in which transactions take place. These guidelines are designed to ensure that electronic information systems also support the legal requirements for record keeping in Delaware.

STATEMENT OF AUTHORITY

The Delaware Public Archives has, as part of its mandate, the responsibility for establishing and administering "an archives and records management program for the application of efficient and economical methods to the creation, utilization, maintenance, retention, preservation, and disposal of public records." (29 Del. Code, Chapter 5, §503) Public records are defined by Delaware Code as "any document, book, photographic image, electronic data recording, paper, sound recording or other material regardless of physical form or characteristics." (29 Del. Code, Chapter 5, §502) Electronic record means "a public record that is stored, generated, received, or communicated by electronic means for use by, or storage in, an information system or for transmission from one information system to another." (29 Del. Code, Chapter 5, §502)

STATEMENT OF BENEFIT

The implementation of sound records management practices can result in a number of benefits for government: reduced costs for storage of obsolete records, reduced resources for the retrieval of records required for business activity, and greater accountability on the expenditure of government funds. With electronic records, the benefits can be more substantial. In implementing sound records management practices for electronic records, agencies can ensure the legal acceptability of their electronic records, reduce costs for the retrieval of records no longer needed to be maintained on the system, and identify economies for the migration of records to successive generations of technology and systems.

The most important benefit is to ensure the creation and management of accurate and reliable electronic records. This allows agencies to fulfill legal mandates about the protection of their records and the adequacy of documentation about their operations. In implementing electronic record keeping, agencies can also achieve the full utilization of information technology and reduce the burden of paper records keeping.

RETENTION OF ELECTRONIC RECORDS

The Delaware Public Archives works with agencies to determine the administrative, legal, fiscal, evidential, and historical value of records created during business operations. The length of retention of electronic records is based on these factors as well as other factors, such as costs for maintaining electronic records and potential costs for migrating records to new systems and platforms.

The Delaware Public Archives works with agencies to establish Retention Agreements for electronic records. These agreements are in the form of a renewable memorandum of understanding between the Delaware Public Archives and the agency and serve to ensure agency compliance with the Delaware laws concerning record keeping.

The Retention Agreement certifies that an electronic records system has met the criteria for electronic records in Delaware. The agreements are renewable at regular intervals, such as when a system undergoes a major revision or update. A sample agreement form can be found later within these guidelines.

MODEL GUIDELINES

1. Electronic records systems must comply with the legal and administrative requirements for recordkeeping for Delaware government.

Summary: Agencies must comply with the legal and administrative requirements for recordkeeping within Delaware. The external recordkeeping requirements must be known and linked to internal retention rules.

Activities: Appoint a Records Officer (RO) annually and assign primary responsibility to the RO for maintaining agency compliance with all rules, laws, policies, and regulations concerning record keeping.

Maintain accurate records retention agreements for electronic record systems.

Renew records retention agreements governing electronic records at regular intervals (such as when the system undergoes a major revision or update) to ensure compliance.

2. Electronic records systems must have accurately documented policies, assigned responsibilities, and formal methodologies for their management.

Activities: In order to ensure documented responsibility for the management of electronic records, agencies must:

Maintain a register of all policies governing the electronic record keeping system. This register will be maintained at the agency and will include superseded policies as part of a history file.

Identify staff members assigned responsibilities for managing the electronic record keeping system and provide evidence of their assignments through position descriptions, administrative memoranda, or other transmitted means.

Maintain an operations manual for the electronic records system. This manual will be maintained at the agency and will include superseded policies as part of a history file.

3. The electronic records system must serve as the official record copy for business functions accomplished by the system.

Summary: The electronic records systems must be employed at all times, or documented exception procedures must be demonstrated to have been operating in their absence.

Activities: Implement the use of a statement of primary use to be consented to by all employees who will access the system. The consent will state that any records created outside of the system shall be deemed unofficial records, unless exception criteria have been met.

Define through the policy the exception criteria.

4. Electronic records systems must produce consistent results for the records they create. Electronic records systems must produce identical outcomes for all data processes and be subject to system logic testing.

Summary: In order to ensure that the electronic records system is the product of a consistent and credible set of processes, agencies must present evidence that the system is compliant

with ANSI/AIIM Standard TR31-1994 "Performance Guidelines for the Legal Acceptance of Records Produced by Information Technology Systems." Systems should also be tested periodically to ensure compliance.

Activities: Require vendor certification of compliance with ANSI/AIIM TR31-1994.

Provide certification that system is compliant with State Information Transport Network Acceptable Use Policy.

5. Records must be created for all business transactions identified in the agency's retention agreement.

Summary: In conjunction with the Delaware Public Archives, the agency shall identify the vital records created by the electronic records system in a retention agreement. These records will provide evidence of the transactions which support the core mission of the agency.

Activities: Identify the transactions within the system which meet the criteria for producing vital and evidential records.

Capture these records through the use of metadata encapsulation and store in a software-independent format.

Use the model metadata profile to ensure compliance.

6. Electronic records systems must maintain accurate links to the transactions supporting the records created.

Summary: Records must be linked to the transaction with unique data. These links must be maintained and accurate.

Activity: Use the model metadata profile to ensure compliance.

7. Records which are created by the electronic records system must meet accepted definitions of accurate, understandable, and meaningful records.

Summary: Electronic records must be:
1. accurate, in that there is a quality control check to ensure correct data;
2. understandable, in that the relationship between the information is represented in a way that supports their meaning; and
3. meaningful, in that the contextual linkages of records must carry information that supports a correct understanding of the transactions they support.

Activity: Develop quality control checks on the system to be performed annually.

8. All electronic records must be created by authorized users. Documentation for authorization must exist.

Summary: All electronic records systems must maintain reference tables containing the information and rules governing the identification of authorized users, as well as contextual information on the authorization and deauthorization of users.

Activity: Maintain all reference tables indicating authorized users and a history of these tables as a vital/evidential record.

9. Electronic records created must continue to reflect the content, structure, and context within the system over the entire length of the prescribed retention.

Summary: The electronic records created in the system must meet the accepted definitions of inviolate, coherent, and auditable records:
1. inviolate, in that they are not damaged, destroyed, or modified;
2. coherent, in that when reconstructed, they represent the logical relations established by the original software environment (and not any updated platform or environment); and
3. auditable, in that all actions taken to a record during the course of its life are documented with a proper audit trail.

Activity: Require vendor certification of compliance with ANSI/AIIM TR31-1994.

10. Records created by the system must be deletable.

Summary: In accordance with an approved retention agreement, electronic records eligible for destruction must be deletable according to accepted practices for the destruction of public records.

Activity: Destroy records according to Delaware Public Archives procedures.

11. It must be possible to export records to other systems without the loss of information.

Summary: In order to ensure the proper migration of records to other systems, as well as the transfer of electronic records to other systems, all electronic records systems must be compliant with ANSI/AIIM Standard TR31-1994 "Performance Guidelines for the Legal Acceptance of Records Produced by Information Technology Systems."

Activity: Require vendor certification of compliance with ANSI/AIIM TR31-1994.

12. It must be possible to output record content, structure, and context.

Summary: Systems must be capable of exporting the content, structure, and context of a record in an integrated presentation.

Activity: Require vendor certification of compliance with ANSI/AIIM TR31-1994.

13. Records must be masked when it is necessary to deliver censored copies to exclude confidential or exempt information.

Summary: As part of the electronic record system description, agencies must define and identify the existence of confidential and exempt records, the rules governing access to confidential and exempt records, and operational guidelines on the generation of output reports containing confidential and exempt records.

Activity: Define through policy the confidential records maintained in the system.

ESTABLISHING RETENTION AGREEMENTS FOR ELECTRONIC RECORDS

Retention agreements will be used to determine the length of retention for electronic records. While they may be similar to retention schedules, there are some differences:

- ► retention agreements will be negotiated with agencies
- ► retention agreements will cover only records meeting vital and evidential value criteria
- ► retention agreements will give agencies flexibility in determining how they wish to retain their electronic records
- ► retention agreements will be renewed on a periodic basis

Delaware Public Archives' Information Resources Specialists (IRS) will work with agency staff, including the agency Information Resource Manager (IRM), the network administrator, and the network operator(s) in drafting the retention agreements.

Identifying Electronic Records

The traditional records inventory (which identifies discrete records which have already been created) will be replaced with an analysis of transactions which occur in a system (which identify events for which records should be created). In order to analyze these transactions, the IRSs will need to review available data models, data flow diagrams, and data dictionaries.

The review will identify transactions which meet certain values, such as administrative, fiscal, legal, vital and evidential, and produce two recommendations: which transactions should result in electronic records being created, and how long those electronic records should be retained. The recommendation will be presented to the agency and negotiated.

Identifying Electronic Records Systems

Unlike paper records, where the properties of record keeping systems were inherent and immediately understandable (e.g., filed alphabetically by year, by subject, suspense file, etc.), electronic records are often stored without these logical properties. IRSs will work with agencies to locate these properties and ensure that activities support a clear understanding of not only the creation of electronic records, but also the system which created them. The Model Guidelines for Electronic Records are designed to guide agencies toward practices which support proper electronic records activities.

IRSs will negotiate with agencies how they plan to implement the Model Guidelines, allowing agencies flexibility in developing answers to the problem of electronic records management.

Final Product: Memorandum of Understanding/Retention Agreement

Once the IRS and the agency have agreed on the two fundamental pieces of the retention agreement: the identification and suggested retention of electronic records, plus the identification and suggested activities of the electronic record system, a Memorandum of Understanding/Retention Agreement is drafted which details the agency's agreed upon management plan for the electronic records.

The Memorandum of Understanding is signed by an agency representative and a representative of DPA. The length of its term is negotiable.

SAMPLE

MEMORANDUM OF UNDERSTANDING (MOU)
State Personnel Office (SPO)
Department of Technology and Information (DTI)
Division of Accounting (DOA)
and
Delaware Public Archives (DPA)

The Payroll and Human Resources Statewide Technology system (hereafter referred to as “PHRST”) is an electronic information system owned by the State of Delaware. The system operates in a client-server environment, resides on servers within the Department of Technology and Information, and is administered by the State Personnel Office.

The PHRST system serves as the official information system for life-cycle tracking activities relating to management of Human Resources (HR), Benefits Administration (BA), and Payroll (PR) records. As such, the PHRST system is considered to contain the official record copy of HR, BA and PR transactions.

For the purpose of this MOU the following terms are defined:

- An **electronic record** refers to "a public record that is stored, generated, received, or communicated by electronic means for use by, or storage in, an information system or for transmission from one information system to another." (29 Del. Code, Chapter 5, §502)
- A **record-keeping system** provides evidence of business transactions by recording and preserving the documentary context in which electronic transactions take place.

DPA hereby attests that the PHRST system is in compliance with its "Model Guidelines for Electronic Records" [http://www.state.de.us/sos/dpa/govserv/index.htm] as noted:

Guideline 1: The PHRST system complies with legal and administrative requirements for record keeping for Delaware government. External record keeping requirements have been reviewed and linked to internal retention rules. Records Officers (RO) are appointed or reappointed on or before July 1 of each year.

Guideline 2: PHRST has accurately documented policies, assigned responsibilities, and formal methodologies for its management.

2.1 A register of policies and a history file of superseded policies are available at http://intranet/state.de.us/phrst and 655 South Bay Road, Blue Hen Corporate Center, Dover, DE 19901.

2.2 Staff members assigned responsibilities for managing PHRST are available at http://intranet/state.de.us/phrst and 655 South Bay Road, Blue Hen Corporate Center, Dover, DE 19901.

2.3 An Operations Manual for PHRST is available at http://intranet/state.de.us/phrst.

2.4 Data dictionary and data flow diagram(s) are available at 655 South Bay Road, Blue Hen Corporate Center, Dover, DE 19901.

2.5 A PHRST User Reference Library is available at http://intranet/state.de.us/phrst.

Guideline 3: PHRST serves as the official record copy for business functions accomplished by the system.

3.1 PHRST users have consented in writing as to the nature of PHRST records as official record copies. Records created outside of the system are non-record copies.

Guideline 4: PHRST produces consistent results for created records in that the system produces identical outcomes for all data processes and is subject to system logic testing. (ANSI/AIIM TR31-1994.)

Guideline 5: PHRST creates records for applicable business transactions (e.g. transactions which produce vital and evidential records) identified in the retention schedule. Records are captured and stored in a software independent format. Note: Those not contained in PHRST are maintained in traditional filing systems.

Guideline 6: PHRST maintains accurate links to transactions supporting created records.

Guideline 7: PHRST records meet accepted definitions of being accurate (there is a quality control check to ensure correct data); understandable (the relationship between the information is represented in a way that supports their meaning); and meaningful (contextual linkages of records carry information which support a correct understanding of supported transactions) records.

Guideline 8: PHRST records are created or accessed by authorized users. Reference tables containing information and rules governing the identification of authorized users, as well as contextual information on authorization and deactivation of unauthorized users is available. Authorized users are defined as those persons having access to the system such as identified agency representatives, identified central (SPO and

Division of Accounting) personnel, and those DTI and vendor staff directly supporting the PHRST system. Users sign an "Acceptable Use Policy" and submit appropriate PHRST and Information Security Form (ISF) documentation through their respective agency Information Security Officer (ISO).

Guideline 9: PHRST records reflect content, structure, and context within the system over the length of the prescribed retention (60 years after employment termination per current General Records Retention Schedule requirements for personnel records) and meet the accepted definitions of inviolate (they are not damaged, destroyed, or modified); coherent (when reconstructed they represent the logical relations established by the original software environment); and auditable (actions taken to a record during the course of its life are documented with an audit trail).

Guideline 10: PHRST records can be deleted when eligible for destruction under accepted practices for the destruction of public records.

Guideline 11: PHRST records can be exported to other systems without loss of information.

Guideline 12: PHRST is capable of exporting content, structure, and context of a record in an integrated presentation.

Guideline 13: Confidential and exempt records are identified and rules governing access to confidential and exempt records, and operational guidelines on the generation of output reports containing confidential and exempt records are available.

To maintain effective operations and continue to retrieve data from PHRST as the operating system changes over time, there must be full documentation of:

- hardware and software, including brand names, version numbers, dates of installation, upgrades, replacements and conversions;
- data structures and content, including file layout and data dictionaries;
- enhancement algorithms;
- operating procedures, including methods for scanning and entering data; revising, updating or expunging records; backing up disks, tapes and files; applying safeguards to prevent tampering and unauthorized access to protected information; and carrying out the disposition of original documents;
- logging and tracking to provide a full, trustworthy audit trail;
- indexes;
- labeling of disks, tapes, and similar storage media;
- full, frequent, and regular backing up of records;
- refreshment, migration, and conversion plans; and
- risk management and disaster recovery plans.

The Delaware Public Archives hereby certifies that the PHRST System meets the legal and administrative requirements for record-keeping in Delaware government.

This certification and agreement is valid for the period January 1, 2004 to December 31, 2006.

RECOMMENDED PRACTICES FOR SELECTION AND USE OF ELECTRONIC RECORDS SYSTEMS AND SOFTWARE

SELECTION AND USE OF ELECTRONIC RECORDS SYSTEMS:
Electronic records systems require hardware (equipment) and software (computer programs) to retrieve and translate information into a human readable format. Because the storage medium is not permanent, and because hardware and software evolve regularly, state and local government agencies must select an appropriate system based on specific information/operational needs and operate it in a manner that allows retention and retrieval of information from the system over time as hardware and software change, technology enhancements evolve, and storage media physically deteriorate.

DPA offers the following suggestions to aid state and local government agencies in using technology in ways that comply with the Delaware Public Records Law and the Freedom of Information Act. These recommendations represent generally accepted principles and practices, and address issues of particular concern to government archives and records administrators. In this rapidly changing information technology environment, adherence to the recommendations will help keep state and local government agencies in conformity with industry standards as they develop.

LEGAL CONSIDERATIONS:
The Delaware Freedom of Information Act (29 Delaware Code, §10001-10005) requires that data in electronic records systems be maintained so that it is available for public access, unless the information is specifically restricted. State and local government agencies should adopt procedures that protect restricted records from unauthorized access, ensure the integrity of all data that the system holds, and allow for access to records open for public inspection consistent with this mandate.

As with all records systems, and especially those using electronic formats, the key to admissibility as evidence is the "trustworthiness" of the information and the system and operating policies and procedures that produce it.

SYSTEMS DOCUMENTATION:
To maintain an effective operation and continue to retrieve data from the electronic records system as the operating environment changes over time, there must be full documentation of:

Hardware and software, including brand names, version numbers and dates of installation, upgrades, replacements and conversions.

Data structures and content, including the file layout and data dictionaries.

Enhancement algorithms

Operating procedures, including methods for scanning and entering data; revising, updating or expunging records; backing up disks, tapes and files; applying safeguards to prevent tampering and unauthorized access to protected information; and carrying out the disposition of original documents. In addition, there should be documented procedures for logging and tracking to provide a full, "trustworthy" audit trail. Full documentation of systems and operating procedures is essential and will contribute to the legal acceptability of the records management program and help ensure that data produced by the electronic records systems will be admissible as evidence in legal or administrative proceedings.

HARDWARE AND SOFTWARE CONSIDERATIONS:
When purchasing hardware and software for your agency:

Select programs that meet the Department of Defense criteria for record-keeping capabilities of software programs. The specifics of Department of Defense Standard 5015.2 for certification of software programs can be found at jitc.fhu.disa.mil/recmgt/#standard.

Strongly promote selection of systems with open rather than proprietary designs. Open systems provide the most flexibility when choosing equipment and will support interconnection, information systems integration, and information sharing.

Prepare specifications for hardware and software that will require vendors to continue to support and maintain their products.

Establish performance standards and incorporate them into specifications for hardware and software, requiring vendors to support them with a substantial performance bond.

Select systems that provide sufficient scanning resolution with enough density to produce a high-quality image.

Seek vendors which use standard rather than proprietary compression algorithms to make future migrations of data more certain and reliable.

Require vendors to supply programs or provide services to test the reliability of your systems periodically.

Consider systems that allow for indexing or incorporation of other retrieval information directly into the system.

INDEXING:
When information is stored on a medium that is not human-readable, complete and accurate indices are essential. The electronic records system design must include provisions for appropriate indexing. When information will be maintained and accessed over a number of years, the indices must be developed and documented with future users in mind who may need the information for purposes not required by the creating agency. Operating procedures should include an index check for accuracy at the time the index is created.

LABELING:
It is essential to label disks, tapes, and similar storage media with extreme care since it is impossible to determine content merely by visual inspection. Accurate labeling is even more critical when the information and its index are on different media.

BACKUP AND STORAGE:
Full, frequent, and regular backing up of electronic records and indices are a critical operating procedure to ensure data protection and information “trustworthiness”. Storage of these backups should be off-site in a secure, fire-safe facility. As the environmental tolerances for storage of electronic media vary greatly, the manufacturer's specifications should be followed.

REFRESHMENT, MIGRATION AND CONVERSION PLANS:
There should be an active procedure to refresh data and to migrate and convert images and correlating indices to new storage media as needed to preserve records in an accessible form.

RISK MANAGEMENT AND DISASTER RECOVERY:
Delaware Code requirements for vital records protection include all records formats. Vital records are defined by 29 Delaware Code, Section 502 as "those records which contain information required for government to continue functioning during a disaster, protect the rights of Delaware citizens, and document the obligations of Delaware government, and reestablish operations after a calamity has ended". Each state and local government agency should develop and implement a comprehensive risk or disaster prevention and recovery plan for all record formats.

IN SUMMARY,
(a) Public records not scheduled for transfer to DPA can be maintained on electronic records systems and the original documents, if any, can be destroyed after data verification. Incorporate consistent data backup procedures and refresh and/or migrate data as required.

(b) Public records scheduled for permanent transfer to DPA at some point in their life cycle will be accepted by DPA in the following formats ONLY:

(1) TIFF or PDF (for scanned documents), or
(2) Text or PDF (for documents born digitally), or
(3) Files created using Microsoft Office productivity software programs (e.g. Word, Excel, Access, PowerPoint) operating under Microsoft Windows operating systems [95, 98, 2000 or higher]

Files must be transferred on Compact Disc (CD-R; Read Only Memory, ANSI/NISO/ISO 9660-1990) with appropriate electronic indices.

NOTE: Microfilm and COM (Computer Output Microfilm) produced to archivally acceptable standards are also appropriate for transferring archival records to DPA. See "Guidelines for Utilizing Paper and Computer Output Image Conversion Services" on DPA's website for further discussion of this option.

For further information and assistance, contact the DPA Government Services section at:

Delaware Public Archives
121 Duke of York Street
Dover, DE 19901
ATTN: James Frazier, Government Services Manager
Tel: 302-744-5039
Fax: 302-739-2578
www.state.de.us/sos/dpa

Effective May 1998
Revised October 1999
Revised December 1, 2003