August 15, 2017

SUBJECT: MODEL GUIDELINES FOR ELECTRONIC RECORDS

PURPOSE

The Delaware Public Archives (Archives) is issuing these guidelines for use by all state and local government agencies in Delaware. The goal of these guidelines is to provide agencies with a set of uniform best practices and statutory requirements for developing electronic record systems that create and/or maintain records that meet legally acceptable, auditable, and evidential standards. It is critical for agencies to extend paper-based record keeping policies for access, management, preservation, and retention to include electronic records systems and software. The best time to accomplish this task is during the planning and procurement of any new systems.

Some information systems store information in discrete data sets that can be reformatted and reused later without referencing the original document's context. Agencies using electronic information systems designed in that manner may not be creating legally acceptable records. Records systems differ from basic information systems n that they provide evidence of business transactions, and record and preserve the documentary context in which transactions take place.

Due to the technical nature of developing electronic record systems, it is highly recommended for agency leaders and their designated Records Officers to seek assistance from the information technology (IT) professionals assigned to support their organization. The Model Guidelines is a set of educational tools intended to prevent state and local government agencies from developing or purchasing a system that may not comply with applicable regulations or may not create legally acceptable records, thereby preventing the agency from fulfilling its legal responsibilities and thus unduly subjecting the agency to possible litigation or sanctions in the course of litigation.

DEFINITIONS

Delaware Public Records Law (29 *Del. C.* § 502) defines a Public Record as:

> *"… any document, book, photographic image, electronic data recording, paper, sound recording or other material regardless of physical form or characteristics, including electronic records created or maintained in electronic information systems, made, used, produced, composed, drafted or otherwise compiled or collected or received in connection with the transaction of public business or in any way related to public purposes by any officer or employee of this State or any political subdivision thereof."*

Therefore, the content of a record, not the medium, determines whether a record constitutes a public record.

Electronic record: a 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. Electronic record formats include, but are not limited to, word processing documents, spreadsheets, databases, emails, websites, audio, and video files, etc.

Record Officer: a person, designated by their agency, whose responsibilities include the development and oversight of the agency's records management program.

BACKGROUND

Delaware Public Records Law, 29 *Del. C.* Chapter 5, provides the Archives the legal authority to administer, implement and enforce all provisions of the Delaware Public Records Law and designates the Archives as the repository for the archival records of the State of Delaware and all political subdivisions thereof.

Public records are essential to the administration of state and local government. These records contain information that allows government programs to function, provide officials with a basis for making decisions and ensure continuity with past operations. Additionally, public records document the legal responsibility of government, protect the rights of citizens and provide citizens with a means of monitoring government programs and measuring the performance of public officials.

BENEFIT

The implementation of sound electronic record management practices ensures legal acceptability, reduces costs for storing obsolete records, decreases time and labor resources required to retrieve records, and enables agencies to identify and forecast budgetary requirements for the migration of records and systems to the next generation of technology. Most importantly, an agency is able to create and manage accurate and reliable electronic records. By implementing electronic record keeping, agencies can achieve the full use of information technology (IT) and alleviate many burdens associated with paper record keeping.

MODEL GUIDELINES

I. SPECIFICATION CONSIDERATIONS

The Model Guidelines for electronic record systems are as follows:

A. Legal and administrative requirements. Electronic records systems shall comply with the legal and administrative recordkeeping requirements for Delaware government:

1. Identify any external recordkeeping requirements and link them to internal retention policy.
2. Appoint Records Officers and Authorized Agents (RO/AA) annually.
3. Assign the RO the primary responsibility for maintaining agency compliance with all laws, policies, and regulations concerning record keeping.
4. Maintain accurate records retention agreements that include all electronic records and electronic record systems.
5. Comply with state law and Archives policy by renewing records retention agreements governing electronic records at regular intervals, such as when new systems are developed or when a current system undergoes a major revision or update.

B. Agency policies. Electronic records systems shall be governed by agency policies that accurately articulate procedures, assign responsibilities, and establish formal methodologies for their management:

1. Assign staff members the responsibilities for managing the electronic record system and providing documentation of their assignments through position descriptions, administrative memoranda, or other transmitted means.
2. Maintain an agency register of all policies governing the electronic record system, to include a history file of all superseded policies.
3. Maintain operations manuals for the electronic records system at the agency, to include a history file of all superseded manuals.
4. Maintain training records of the course materials used and document attendance of all training sessions.

C. Official Records. The electronic record system must serve as the official record copy for business functions accomplished by the system:

1. Require all employees with access to the system to sign a consent statement of primary use. The consent statement will state that any records created outside of the system shall be considered unofficial records, unless all exception criteria have been met.
2. Employ the electronic records system at all times. Demonstrate the use of exception procedures during any periods that the electronic system is unavailable.

3. Establish an agency policy that defines the exception criteria of primary use.

D. System Access. Identification and documentation of authorized users.

1. All electronic records must be created by authorized users.

2. Agencies must maintain documentation for the authorization of all users.

3. 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 de-authorization of users.

4. Maintain all reference tables indicating authorized users and a history of these tables as vital and evidential records.

E. Electronic records systems must produce consistent identical outcomes for all data processes and be subject to system logic testing:

1. Agencies must present evidence that the system is compliant with ANSI/AIIM Standard TR31-2004 "Legal Acceptance of Records Produced by Information Technology Systems," to ensure the electronic records system is the product of a consistent and credible set of processes.

2. Test all systems periodically to ensure compliance.

3. Require vendors to provide certification of compliance with ANSI/AIIM Standard TR31-2004.

4. Provide certification that the system is compliant with the applicable State of Delaware Enterprise Standards and Policies.

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

1. Agencies shall collaborate with the Archives to identify the vital and evidential records created by the electronic records system in a retention agreement. These records will provide evidence of the transactions that support the core mission of the agency.

2. Electronic records system must capture these records by using metadata encapsulation and store in a non-proprietary file format.

3. Metadata use is described in paragraph IV. B. 3. Metadata.

G. Maintain accurate contextual information links to the transactions supporting the records created:

1. Contextual information identifies the creator, the time of its creation, its relationship to other records, etc. Contextual information is crucial to the evidentiary function of records.

2. Link the records to the transaction with unique data.

3. Collect, structure, and maintain contextual information with the record at the time of record creation; identify and label (or tag) records and link them to contextual information.

4. Metadata use is described in paragraph IV. B. 3. Metadata.

H. Quality. Records created by the electronic records system must meet accepted definitions of accurate, understandable, and meaningful records.

1. Quality relates to the ability of the electronic record system to reliably produce and preserve records so that they can be used or recognized by the intended audience. It also relates to the quality of information in terms of its accuracy and reliability.

2. Electronic records must:

a. Be accurate: accuracy is accomplished by conducting audits and quality control checks to ensure correct data;

b. Be understandable: accomplished by ensuring the relationship between the information is represented in a way that supports their meaning;

c. Be meaningful: ensure that the contextual linkages of records must carry information that supports a correct understanding of the transactions they support;

3. Agencies ensure systems are acceptable by developing and performing annual quality control checks.

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

1. The electronic records created in the system must meet the accepted definitions of inviolate, coherent, and auditable records.
    a. Inviolate: records must not be damaged, destroyed, or modified;
    b. Coherent: when records are reconstructed, they represent the logical relations established by the original software environment (and not any updated platform or environment); and
    c. Auditable: The system must create and maintain a proper audit trail that documents all actions taken to a record during the course of its life cycle per its business requirements.
2. The applicable retention schedule and business requirements should reflect which fields are auditable and tracked.
3. Require vendors to provide certification of compliance with ANSI/AIIM Standard TR31-2004.

J. Record Service. Systems must be able to output record content, structure, and context:
1. Systems must be capable of exporting the content, structure, and context of a record in an integrated presentation.
2. The information content of a record should be an accurate reflection of a particular business transaction.
3. Require vendors to provide certification of compliance with ANSI/AIIM Standard TR31-2004.

K. System Migration. Records must be able to be exported to other systems without the loss of information:
1. 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 TR31-2004 "Legal Acceptance of Records Produced by Information Technology Systems."
2. Require vendors to provide certification of compliance with ANSI/AIIM Standard TR31-2004.

L. Destruction of obsolete records. Records created by the system must be able to be destroyed (deleted).
1. Destroy any eligible record in accordance with Archives procedures and applicable retention schedules.

M. Redaction and Security of confidential information.
1. Information contained in the records of electronic records systems must be able to be masked and/or redacted when it is necessary to deliver censored copies requiring the exclusion of confidential or exempt information.
2. Establish an agency policy or procedure that defines the actions required to redact confidential/exempt information prior to delivery; include procedure in cases when the system is unable to mask or redact any protected information prior to output.
3. As part of the electronic record system description, agencies must define through policy 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.
4. Provide adequate security for confidential and non-public information and records.

II. ELECTRONIC RECORDS ADMINISTRATION

A. RETENTION

The length of electronic records retention is primarily based on the administrative, legal, fiscal, evidential, and historical value of records created during business operations. The costs for maintaining electronic records or for migrating them to new systems and platforms are not considered when determining the appropriate duration for electronic records retention. The Archives assists agencies with developing a plan to implement the Model Guidelines, allowing agencies the flexibility to develop answers to the challenges of electronic records management.

B. RECORD IDENTIFICATION

An analysis of transactions that occur in a system will replace the traditional records inventory process (which identifies previously created discrete records) to identify events for which records should be created. In order to analyze these transactions, the Archives will need to review available data models, data flow diagrams,

and data dictionaries. The review will identify transactions that meet certain values, such as administrative, fiscal, legal, vital and evidential, and produce recommendations regarding which transactions should result in the creation of electronic records, and their retention instruction. The Archives will document and discuss all recommendations with the agency.

C. ELECTRONIC RECORDS SYSTEMS IDENTIFICATION

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. The Archives will collaborate 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 that created them.

D. MEMORANDUM OF UNDERSTANDING / RETENTION AGREEMENT

There are cases in which the costs, design, or quantity of records contained within an electronic records system may make it impractical to transfer the data to the Archives for permanent preservation. The Archives will work in partnership with agencies to establish a Memorandum of Understanding/Retention Agreements that addresses the electronic records systems. The agreements are renewable at prescribed regular intervals or event such as a major system revision or update. The agreement will ensure agency compliance with the Delaware laws concerning record keeping.

1. The Memorandum of Understanding/Retention Agreements addresses all of the specification considerations explained in Section I. to certify that the agency's electronic records system meets the criteria for electronic records in Delaware. Retention Agreements determine the length of retention for electronic records.
2. Retention agreements are similar to retention schedules; however, there are some differences:
    a. Retention agreements shall be negotiated with agencies;
    b. Retention agreements shall apply only to records meeting vital and evidential value criteria;
    c. Retention agreements provide agencies the flexibility to determine how they will retain electronic records; and
    d. Retention agreements shall be renewed on a periodic basis.
3. Once the agency and the Archives have agreed on two fundamental pieces of the retention agreement, the identification and recommended retention of electronic records and the description and proposed activities of the electronic record system, a draft Memorandum of Understanding/Retention Agreement is to detail the agency's record management plan.
4. The Archives will work in partnership with the agency's staff, including the agency Information Resource Manager, the network administrator, and information technology representative to draft the retention agreements. An agency representative and a representative of the Archives will sign the Memorandum of Understanding.
5. As part of this agreement process, select Archives staff may require remote access to the data system in order to provide continuing ability to view and retrieve any permanently valuable records for research purposes.

III. SELECTION AND USE OF ELECTRONIC RECORDS SYSTEMS AND SOFTWARE

The following suggestions are provided 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 consistent with industry standards.

A. SELECTION AND USE OF ELECTRONIC RECORDS SYSTEMS

Electronic records systems require hardware (equipment) and software (programs) to retrieve and translate information into human readable formats. Because the storage medium is not permanent and because the technology that develops the hardware and software evolves regularly, state and local government agencies must select an appropriate system based on specific information and operational requirements. The system must allow for the retention and retrieval of information over time and for system upgrades as hardware and software technology enhancements evolves. The system must be able to upgrade storage capacity and be able

to replace the storage medium as it physically deteriorates. Agencies must consider the requirements to migrate data and records to subsequent systems as existing contracts are terminated.

B. LEGAL CONSIDERATIONS:

1. The Delaware Freedom of Information Act (29 *Del. C.* §§10001-10007) requires that data in electronic records systems be maintained so that it is available for public access, unless the information is not deemed public. State and local government agencies should adopt and adhere to 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.

2. The Delaware Uniform Electronic Transaction Act (6 *Del. C.* c12A) provides the legal requirements for the use of electronic records as the legal "official" document of record for transactions.

3. As with all records systems, and especially those using electronic formats, the key to admissibility as evidence is the "trustworthiness[1]" of the information, the system, and the operating policies and procedures by which it is produced.

C. 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 that reflects:

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

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

3. Enhancement algorithms.

4. Operating procedures that include 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 systems to provide a full, "trustworthy" audit trail.

5. Full documentation of systems and operating procedures is essential 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.

D. HARDWARE AND SOFTWARE CONSIDERATIONS:

When purchasing hardware and software for your agency:

1. Select programs that meet the Department of Defense criteria for record-keeping capabilities of software programs. The Department of Defense Standard 5015.2, dated April 2007, for certification of software programs is located at jitc.fhu.disa.mil/recmgt/#standard.

2. Selected programs must also meet the standards set by the Delaware Department of Technology and Information. These standards are located at http://dti.delaware.gov/information/standards-policies.shtml

3. 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.

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

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

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

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

[1] As described in ANSI/AIIM Standard TR31-2004, Legal Acceptance of Records Produced by Information Technology Systems.

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

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

E. 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 facility that is secure, fire and flood safe, has back up power, etc. Follow all manufacturers' specifications because the environmental tolerances for storage of electronic media vary greatly.

F. REFRESHMENT, MIGRATION AND CONVERSION PLANS:

Agencies must plan for the migration and conversion of electronic records and data because there is no single digital storage medium that is adequate for the long-term or archival preservation of records. 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. Technological obsolescence of hardware and software usually occurs within five to ten years and may be shorter than the required retention of the record. As a result, agencies' plans should include annual tests of record accessibility as well the migration of all files to new storage mediums on a regular basis to preserve the record for the required period. In the meantime, agencies will need to protect stored data with a comprehensive back-up system.

G. RISK MANAGEMENT AND DISASTER RECOVERY:

Vital records are defined by Delaware Public Records Law 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 shall develop and implement a comprehensive risk or disaster prevention and recovery plan for all record formats.

IV. AGENCY STORAGE AND TRANSFER

A. Agency Storage. Public records that will be retained at the originating agency for the duration of their retention (per paragraph II, D. of this policy), and not scheduled for transfer to the Archives may be maintained on electronic records systems and the original documents, if any, can be destroyed after data verification. Agencies must incorporate consistent data backup, data refresh and migration procedures, as required. And in addition, if records are being transferred to Archives, the following conditions must also be incorporated:

B. Transfer: Basic Requirements for Data Organization:

1. Indexing: information stored on mediums that are not human-readable, such as optical discs and hard drives, must be accurately indexed at the time it is created because the data will be maintained and accessed over a number of years. The indices must be developed and documented with future users in mind and who may need the information for purposes not required by the creating agency.

2. Labeling: it is essential to label disc cases and similar storage media containers 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 have relationships with records stored on different media. Do not write on or affix labels to the media itself (e.g. discs) due to the acid contained within the ink or the adhesives normally used with the labels.

3. Metadata: essentially, metadata is "data about data." It is the information used to describe an electronic record or object (digital or otherwise), its relationships with other records or objects, and how the record or object has been, and should be, treated over time. Metadata uses a basic structured format, usually single word descriptions that can consist of keywords, file type, file name, creator name, date of creation, file contents, etc. (e.g. Smith, DHSS, March, 2013, tests, CSV, spreadsheet, DSTP, etc.). This information enables an agency to provide a precise and comprehensible description of content, location, and value. Suggested information to be captured in the metadata are:

   a. Case/File/Record Name

   b. Originating Organization

   c. Other organizations associated with the records

d. Functional purpose of the records

e. Date created

f. Time period to which the records relate

g. Frequency of use

h. Value or significance of the records in relation to the functions of the organization

i. Record-keeping system used in relation to the records

j. Relationship between the records and other records or materials

k. Governing law, MOU, business practice, procedures affecting the records

C. Microfilm and Computer Output Microfilm (COM): Film produced to acceptable archival standards is also appropriate for transferring archival records to the Archives. See "Guidelines for Utilizing Paper and Computer Output Image Conversion Services."

D. File Formats: Public records scheduled for long-term or permanent transfer to the Archives will only be accepted in the following formats:

1. Tagged Image File Format (TIFF) or Portable Document Format (PDF/PDF-A) is preferred for scanned documents. (Please include all format field data)

2. Text (please identify the format field data and the data dictionary text fields) or PDF/PDF-A for documents born digitally. (Please include data dictionary for text fields)

3. Files created using Microsoft Office productivity software programs (e.g. Word, Excel, Access, PowerPoint) operating under Microsoft Windows operating systems [XP or higher]

4. TIFF or Joint Photographic Experts Group (JPEG) TIFF is preferred for photographs.

Delaware Public Archive's Contact Information:
The Delaware Public Archives has assigned an Information Resources Specialist (IRS) to each state and local government agency. A listing of agency assignments may be located by using the link below.
http://archives.delaware.gov/govsvcs/govsvcs.shtml

For further information and assistance, please review the references listed at the bottom of the information paper or contact the Archives' Government Services section at (302) 744-5000.

Effective March 12, 2012
Revised August 15, 2017

References:
Delaware Public Records Law: 29 *Del. C.* Chapter 5
Delaware Uniform Electronic Transactions Act: 6 *Del. C.* Chapter 12A
Delaware Freedom of Information Act 29 Del. C. Chapter 100-
Delaware Public Archives Information Paper: Suitable Media and Formats for Submitting eRecords to the Delaware Public Archives
Delaware Public Archives: Guidelines for Maintaining and Preserving Web-Based Activities
Delaware Public Archives: Guidelines for Utilizing Paper and Computer Output Image Conversion Services
Delaware Department of Technology and Information: State of Delaware Enterprise Standards and Policies
Department of Defense Standard 5015.2 Electronic Records Management Software Applications Design Criteria Standard; April 25, 2007
ANSI/AIIM Standard TR31-2004 "Legal Acceptance of Records Produced by Information Technology Systems."