

Electronic Records Management

Checklist of Requirements

Summary: Electronic records management requires the records officer to work with agency staff in a life-cycle management process from the creation and receipt of records, through their active life, storage, and to their final disposition. It also requires the participation of every staff member, the cooperation of technology support staff, and the approval of top management. This publication briefly lays out the core issues that must be addressed within any agency to ensure the capture and maintenance of reliable electronic records.

Definitions

Before an agency can begin the process of managing electronic records, it must have an understanding of what it is being managed. This means knowing the difference between documents and records.

Documents are formatted information that can be accessed and used by a person. They have a beginning and an end and may be represented through alphanumeric text, vector data, a digital map, spreadsheets and databases, moving images, or audio data. Regardless of format, documents serve the purpose of conveying information.

Records are documents that have been set aside as evidence and protected from alteration or change. The critical factor is how “set aside” is defined. In paper, “being set aside” means placing a document into a filing system from which it can be retrieved. With digital technologies, the same result is achieved by transferring an electronic document from an operational environment into a record keeping system.

Records come in many forms. According to Georgia statute, records include “all documents, papers, letters, maps, books (except books in formally organized libraries), microfilm, magnetic tape, or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in performance of functions by any agency” (Official Code of Georgia Annotated, § 50-18-91[5]). The International Standards Organization (ISO) states they are “recorded information in any form, including data in computer systems, created or received and maintained by an organization or person in the transaction of business and kept as evidence of such activity” (ISO/DIS 15489). Regardless of their form, all records share in common the elements of (1) content, (2) structure, and (3) context.

Elements of a Record

Content is the information in a record, the idea or concept, the facts about an event, a person, an organization or other similar act that are recorded to document the transaction itself.

Structure refers to the physical and logical attributes of records. Physical attributes of a record include such things as the size and style of type, line spacing, page margins, and agency logo. Logical attributes consist of the logical arrangement of the record. For example, the structure of a memorandum would include a header (the name of the sender, the date, the subject of the memo, and the recipient of the memo), a body (the actual content in one or more paragraphs), and the authentication (signature).

Context explains the “why” of the record. A single record derives its trustworthiness and usefulness from its association with other records that collectively tell the story of an event or activity. A letter from a constituent, for example, may be filed with the letter of response so that anyone viewing the



THE GEORGIA ARCHIVES

response in the future can see it in the context of the request. Without the request, the response could be taken out of context and misconstrued.

The first two elements of a record are straightforward and easily captured by a single staff member working on a computer. But how do you capture the context of a record? Capturing context involves more than just each person working alone at a computer; it involves a framework of administrative *policies* and work *procedures* that ensures the creation of authentic electronic records. The checklist below discusses the issues that will help you complete this process.

Checklist

These twelve components establish a framework in which record creation and maintenance occurs. Each of the components is discussed separately below.

- | | |
|--|--|
| <input type="checkbox"/> Policies and Procedures | <input type="checkbox"/> Storage Management |
| <input type="checkbox"/> Education and Training | <input type="checkbox"/> Record Availability |
| <input type="checkbox"/> Confidentiality and Integrity | <input type="checkbox"/> Audit Trail |
| <input type="checkbox"/> Document Capture | <input type="checkbox"/> Retention |
| <input type="checkbox"/> Metadata | <input type="checkbox"/> Media Renewal or Transfer |
| <input type="checkbox"/> File Management | <input type="checkbox"/> Disposal |

Policies and Procedures

Government officials frequently hear that records that are legally admissible must be created in the normal course of business. But what does that mean? Simply put, “normal course of business” refers to the business processes and administrative procedures of an agency—how the agency conducts its day-to-day operations—and the ability of these processes to repeatedly create and maintain accurate records. This last part is extremely important: does the agency consistently create accurate records and maintain them in a way that prevents unauthorized access and alteration? An agency’s “normal course of business” should consistently result in accurate records as a by-product of the business process.

In order to control business processes and employee behavior, a how-to manual of policies, regulations, standards, and procedures must exist.

- Policies supply top-level guidance providing a statement of intent on the part of the agency.
- Regulations provide interpretations of the law and how the law has impact on agency business processes. Regulations also serve to identify all the requirements affecting the performance of a business process.
- Standards establish codes of behavior with regard to the performance of work.
- Procedures control each step in a business process and ensure compliance with standards.

Information in the operating procedures for a computer system would include, at minimum:

- a description of the methods for scanning or entering data
- a description of how records are revised, updated, or deleted
- hardware and software manuals, including the name of the software, version numbers and dates of installation, upgrades, replacements, and conversions
- a description of how the records are indexed
- access policies (log-on controls), security features (for example: use of Public-key Infrastructure (PKI) technologies, encryption techniques, secure socket layer encryption technology)
- data structure and content, including the file layout and data dictionaries

- file naming conventions and hierarchy
- enhancement algorithms (digital imaging systems)
- backup procedures for disks, tapes, microfilm, etc.
- procedures for testing the readability of records
- on-line, off-line, near-line storage procedures
- security safeguards to prevent tampering and unauthorized access to protected information
- disposition of the records (including over-writing of backup tapes)
- approved retention schedules

If the agency intends to rely on the electronic record as its official record, it is of the utmost importance that a statement of intent to rely on the electronic record exists. Such a statement would identify the electronic record as the agency's official record. Official records reflect the information and position that the agency believes is true and complete and will rely upon to conduct its business. The official record, once designated by the agency, must be subject to rigorous procedures for creation, modification, and destruction under a records management program. A statement designating the electronic record as the official record must exist as part of the agency's overall records management program.

□ Education and Training

Staff members will comply with policies and procedures only if they are aware of the procedures and understand them. Use training efforts to convey:

- policies and procedures
- new/revised business processes
- what records staff must keep in order to document the business process
- the fact that everyone (not just the information technology office) is responsible for creating authentic records
- retention and disposition

Training is a vital element of compliance. It is the primary way in which an agency communicates what it wants done and how it wants it done. Training is an ongoing effort. It should provide a review of existing policies and procedures for staff and an introduction to new policies and procedures.

□ Confidentiality and Integrity

Confidentiality and integrity refer to protecting records from unauthorized access or change in an active business environment. This can be accomplished through access controls, authorizations, encryption of documents, and endorser techniques. To ensure the integrity of agency records, adequate protection against tampering, alteration, revision, and deletion must be included as part of the electronic system. Such protections must exist throughout the entire life span of the records.

It is important to remember that *documents* can be revised; *records* are never altered. Records should be protected as read-only and never over-written. Revisions must be done only as copies, which then become new records. These controls must also be considered in migration planning so that records are not altered when they are moved to new technologies.

□ Document Capture

An agency must capture all three elements—content, structure, and context—to create a record. Content is the most straightforward one to address—ensuring that staff uses the “save command” on a computer is relatively simple. But what happens to the related datasets that make the document a

record—the record metadata (discussed below)? All electronic sources of information making a record a record must be captured and maintained along with the document itself.

With imaging systems it is important to maintain the hardcopy sources, both paper and microforms, until the images can be verified. If you are reformatting a record that has a retention period of more than 15 years, you should keep the original or a microfilm copy as a backup.

Also, consider the issues of quality control and quality assurance. Quality control is the real-time inspection of business processes to ensure that they are being performed repeatedly and consistently. Quality assurance is the post-process inspection of business processes to evaluate whether they are working as designed or if alterations are needed.

□ Metadata

The term metadata literally means data about data or, in this case, information about your records. In addition to indexing information, there are five additional areas of metadata that should be collected and maintained as part of every record. These are:

- Accessibility includes information about statutory restrictions that may apply to the record
- Retention and disposition includes information about how long the record is being kept and what is the trigger for destruction (end of year, etc.)
- Security information about restrictions on the information as well as information about how the data is encrypted
- Audit trails includes information documenting all actions (for example, revisions) taken on the record
- Migration includes information on software versions and technology platforms used to create and store the record

This metadata is not necessarily all in electronic format. For example, migration metadata would include the hardware and software documentation manuals created and maintained by the agency during installation of a system.

□ File Management

Your file management system is the component that physically takes care of the records during their active and inactive life. A file management system must preserve the integrity of the records through a non-erasable medium (such as WORM) or through controls providing the same level of protection. It should manage the entire record including the associated metadata, audit trails, and histories through either logical (all records, metadata, audit trails linked as a logical entity) or physical (all records, metadata, audit trails on a single volume of media) means. The file management system must also support the copying, reformatting, or transfer of records across media and through system technology changes. Finally, the system must support the full recovery of records in the event of a disaster. This means the system should provide or have an added component that provides the ability to duplicate all vital and permanent records and the software necessary to view the records.

□ Storage Management

The selection and management of your storage technology—the *file format* and the *storage medium*—is very important. When you select a file format, keep in mind that if the company that owns the patents on that format goes out of business or stops supporting the format, you may be unable to access and view your records. There is no guaranteed way to avoid this, but if the format you adopt is widely-used, it is more likely to be supported for years to come. Currently, the leading document file formats are .PDF (Portable Document Format) and .TIFF (Tagged Image File Format).

A second area where file formats are important is in the management of spreadsheets. Commonly used file formats for converting spreadsheets include DIF (Data Interchange Format) and CSV (Comma Separated Value or comma delimited). However, most vendors provide backward compatibility over several generations of spreadsheet software (such as Excel), so in the short term it should be possible to convert a spreadsheet in an older version to one in a newer version.

A third area of file formats includes those used in the transfer of data and document encapsulation technologies used to make information available on the World Wide Web. This area is dominated by markup languages such as SGML (Standard Generalized Markup Language), HTML (Hypertext Markup Language), and XML (Extensible Markup Language). These file formats allow a document to be read and processed by any computer system.

The selection of a storage medium (CD-ROM, 3480 Cartridge Tapes, Open Reel Magnetic Tapes, or Digital Versatile Disks (DVDs), etc.) is equally important. Current trends are toward media independence (meaning the storage device will work with computers from many different manufacturers, not just one.) Agencies should adopt media that are mainstream, widely-used devices that comply with industry standards; avoid both cutting-edge and obsolete technologies.

❑ **Record Availability**

A record is available if it can be rendered in a human-readable form such as a printout or as an image on a computer screen. Records, including associated metadata and audit trails, must be accessible to authorized individuals for the record's entire life span.

❑ **Audit Trail**

An audit trail documents who, what, when, and why of all actions or events related to documents and records. It is a key component needed to show a responsible chain of custody in the event of litigation. An audit trail will document the creator, recipient, content, date of creation, date of revision, date of sending, any and all alterations, and authorizations connected with an individual record.

❑ **Retention**

Your agency should have an approved retention schedule that must apply to all electronic records, too—not just your paper records. Remember that an electronic record is more than just content, so the schedule must also consider the retention of the associated metadata and audit trails. Your file management system must be capable of notifying you of a retention trigger (such as “10 years from filing date,” or “upon completion of the case,” or “expiration plus 3 years”). Equally important is the ability to place a hold or freeze on all records destruction.

❑ **Media Renewal, Copy, or Transfer**

There are three components involved with the long-term preservation of electronic records: renewal, copy, and transfer.

- *Media renewal* is the copying of records from one type of medium to the same type. Example: copying records from one 650 megabyte CD to another 650 megabyte CD. There is no change to any of the records.
- *Media copying* is the copying or reformatting of records from one medium to another. Example: transferring records from a 650 megabyte CD to a 3480-cartridge tape. This may result in a slight change to the record because of the way data is recorded on different media. Therefore, comparing a sampling of the records on the new medium with the same records on the old medium can verify that any changes are insignificant.

- *Media transfer or migration* is the complete change of the file management system as you move from one software platform or technology to another. The file format of the record may change as a result of transfer. A bit by bit comparison (validation) of each record will be required to preserve the integrity of the records.

When copying and transferring records, it is important to remember that not only the content needs to move, but also the metadata, audit trails, and any links must be preserved and moved.

❑ Disposal

Disposal is the ability to identify, gain authorization, and completely purge a record from a computer system. Procedures for disposal of records must exist and be implemented consistently. Disposal may be logical or physical depending on the storage medium for the records.

- Logical disposal is used with non-erasable media. It involves the purging of all metadata, index points, audit trails, and links to the records. While the record itself remains in storage, all pointers to it are destroyed making it inaccessible.
- Physical disposal means removing the record itself from the medium and renders a record non-reconstructable. It must include both the primary storage medium and the backup media.

Procedures for the physical destruction of electronic records should be detailed enough to specify the number of overwrites that must occur to a backup tape to ensure the total destruction of the records.

More Information

For additional information on electronic records management, reference the following Georgia Archives publications:

- *Adopting Electronic Records (RIMS 3)*
- *Electronic Document Management System Technologies (RIMS 6)*

The Georgia Archives is ready to provide assistance to state and local governments that have questions about records—paper, microfilm, or electronic. Please contact us:

Georgia Division of Archives and History
330 Capitol Avenue SE
Atlanta, GA 30334
Tel: (404) 656-2379
Fax: (404) 656-2949
Email: garecords@sos.state.ga.us
Web: www.GeorgiaArchives.org