

### Design the system to create or capture a record for each business transaction that complies with identified requirements.

Organizations make or receive records necessary to carry out a business process and to meet the specific record keeping requirements tied to that process. The proper maintenance of those electronic records requires that the system supporting the business process can capture or create records in the required form including content, structure and contextual elements. Records must also be identified to ensure their accessibility, usefulness and preservation.

Records should be created or received for all defined business transactions in the business process. For example, when someone applies for a professional license, a record is created when the application is filled out, when it is paid for, and when it is issued or denied. Every business process will have a point (or points) at which a record is created and must be retained.

Some business transactions require records to be imported from other environments. In order to issue the professional license in the above example, other records will be required. It is necessary to import records such as a valid driver's license, a certificate of graduation, letters of recommendation, as well as other material. This could be done electronically wherever possible, using portable copies.

Each record should comply with the legal and business process requirements as far as content, structure and context discussed in the previous section.

### Ensure the appropriate level and type of security.

To mitigate the risks discussed in Section II, "Identifying the Risks and Benefits of Moving From Paper to Electronic Transactions and Records," section of this document, the appropriate levels and types of security functionality must be built into the system. This functionality must be consistent with the risk assessment and cost/benefit analysis discussed in that section. A detailed discussion of security levels, methods and technologies is beyond the scope of this document. Following is a very high-level description:

1. Levels of security based on risk assessment:
  1. High
  2. Medium
  3. Low
2. Types of security that may be required:
  1. **Authentication** establishes the validity of a transmission, message, and its originator.
  2. **Confidentiality** restricts access of a record to only those authorized to view it.
  3. **Data integrity** addresses the unauthorized or accidental modification of a record.
  4. **Non-repudiation** prevents an individual from denying that previous actions had been performed or intent expressed in a record.
3. Types of security tools:
  1. PINs and passwords
  2. Digital signatures
  3. Encryption
  4. Biometric devices

### Manage and retain electronic records in an accessible form for their legal minimum retention periods established by State Archives through retention schedules and dispose of them appropriately after the legal retention period.

Electronic records should be retained at least as long as required by law or best practices. They should not be

## IV. Managing the Risks of Moving to Electronic Records

---

kept any longer unless their value to the agency offsets the cost of their storage. Each series (a group of identical or related records, which are normally used and filed as a unit) should have its retention period listed on a records retention schedule to avoid appearances that records destruction is capricious.

System requirements and design must reflect the fact that records must be maintained for the length of their retention period in an accessible, reliable and authentic manner. Agencies need to ensure that electronic records remain accessible and useable to support the primary purposes for which they were created and any predicted secondary(7) purposes for as long as the records must be legally retained. System designers should also remember to account for the fact that a record may need to be kept longer than its retention period. For example, records disposal must be suspended in the face of litigation, administrative hearing, or an open records request.

That small percentage of records designated as 'archival' must be preserved permanently in an accessible and useable format by the agency or the relevant archival authority. In the absence of well-established, time-test standards, preserving electronic records raises real migration challenges since technology will change continuously through the life of the record. The use of proprietary formats in the creation and maintenance of electronic records is strongly discouraged because the use of these formats makes the migration and preservation of electronic records more difficult and costly.

Another challenge to records preservation is that it's not always possible to predict secondary use. That is particularly important because most archival use is based on the record's secondary value. It should be possible to retrieve and view the records in a number of ways to enable uses other than those based on primary value and the original functionality of the e-records system.

### Maintaining Reliability and Authenticity

The originating entity must maintain the reliability and authenticity of the records for the time period established by the records retention schedule. To do so, the originating entity must maintain the records and all related metadata, system documentation, procedures and policies, and proofs of authenticity (e.g., electronic signatures) for the entire time period established by the records retention schedule. All data elements that comprise a record of a business transaction must be accessed, displayed and managed as a unit for the entire time period established by the records retention schedule. This does not mean that everyone that accesses the record needs to have access to all of the data elements. For example, when analyzing data for secondary purposes, it may not be necessary to acquire system documentation, procedures and policies.

### Maintaining Accessibility

Records must be easily retrieved in a timely manner throughout the entire retention period. Government officials are responsible for managing records in ways that ensure accessibility under the state and federal Freedom of Information Acts as well as other state and federal statutes and regulations that govern accessibility for disabled populations.

This accessibility is not unlimited, however. The system must include the necessary security to provide full access to individuals and agencies that have the right to full legal access, while limiting access to individuals and agencies that do not have the right to full legal access.

Records must be searchable and retrievable for reference and secondary uses including audits and legal proceedings throughout the entire retention period. Records must remain searchable and retrievable beyond their retention period if – but only if – special circumstances dictate, such as records being relevant to pending or current litigation or because they have been identified as archival.

When a new system is designed to replace an existing system, the requirements for the new system must ensure that complete records along with their corresponding metadata can be migrated to the new system. In addition, functionality necessary for predicted use of records can be reproduced in the new system. Functionality should be based on predicted use based on status of records. For inactive records, the ability to search and retrieve records may be sufficient. For records still actively engaged in a business process, full functionality may be necessary.

In summary, the system must be designed to ensure that copies of records can be produced and supplied in a useable format for business purposes, all public access requirements, and/or transfer to the relevant archival authority.

### Preserve and/or Prepare for Migration

Too often systems are built with the faulty expectation that they will last forever. In reality, systems go through a life cycle, which ends in their complete redesign or retirement from service. The need or requirement to retain accessible and useable electronic records may exceed the life of the system that created them. Electronic records created by one system may need to be moved or migrated to another system. System migrations are extremely complex and should be planned for and accomplished before the original system becomes obsolete and inoperable. Migration should be implemented incrementally along with periodic system and software upgrades and should include quality control checks. While migration has become common, it is still fraught with danger. For example in one case involving FDA-mandated records of drug testing, blood pressure numbers were randomly off by up to 8 digits following data transfer from UNIX platforms to Windows NT operating systems.(8)

The least complex form of migration is simple data migration where the data is pumped from the old system into the new system. For low risk electronic records this may be sufficient to retain them in a useable form. However, even such a seemingly simple task could be problematic depending on the complexity of data structures and the use of proprietary formats. Furthermore, a successful migration of high-risk records will require that information in addition to the informational content of the records be migrated to ensure their integrity and reliability. Information relative to the electronic record's creation and use such as metadata, audit trails, authoritative controls, and documentation need to be migrated to the new system and maintained for the same retention period as the records. In other words, it is not enough that the content or data of the records be migrated to the new system. The context in which the records were created and their structure needs to be maintained for the life of the records as well. The migration of this additional information could be extremely difficult and will involve additional planning and resources.

Most installed technology involves proprietary systems and formats. Proprietary data formats can greatly complicate migrations and jeopardize the accessibility of electronic records. Technology policies should strive to establish standard formats for electronic records. Since software is subject to change – either by the implementation of new releases, by changes to operating systems, or changes in hardware requirements, the use of non-proprietary formats is strongly recommended. Regardless of the medium on which a record is stored the use of non-proprietary formats will minimize the long-term costs associated with maintaining the reliability of and migrating records. The use of widely adopted standard formats (relational databases, ASCII, SGML, etc.) can help reduce the rate of technological obsolescence and the frequency of migrations, as well as facilitate migrations. Be aware, however, that standards change or are replaced over time and must be monitored. The National Institute of Standards and Technology (NIST) is exploring the use of standard e-records storage formats.

Although not a permanent solution, migration is the primary solution for retaining electronic records over extended periods of time, especially if there is a need to retain the records' original functionality. However, other possible solutions to long-term retention are also being explored including:

- **Encapsulation:** Encapsulation refers to a method of capturing the look and feel of the original record along with any required metadata as a single digital object in a portable format. In some ways, encapsulation combines system migration with use of standard formats. Encapsulation strategies are just beginning to be investigated.
- **Emulating obsolete technology:** Emulation consists of using hardware and software to allow one computer technology to act as if it were another technology. This solution allows e-records to remain in their original file formats while the hardware and software change. Emulation is complicated and expensive to achieve for any sophisticated system. Research on emulation solutions is ongoing.

If loss of a record series would place an agency at significant risk, exporting the records to a technologically neutral, durable media such as computer output microfilm or paper as insurance against unforeseen migration problems. Because export will result in a loss of system functionality, this option is unattractive and clearly reserved only for records of extraordinary value. In some instances, it may be possible to export a subset of the essential information. A hybrid approach that preserves the records in both electronic and durable formats can offer functionality and confidence of preservation.

Export to physical media requires the preservation of sufficient context and structure to ensure that the records are acceptable as evidence. This information may be appended as a header or footer, although some can be translated back into the media's physical characteristics. For example, a message digest used to demonstrate the record's integrity is of no further value because the content is fixed on film or paper and subject to traditional forensics tests for altered documents. However, the process of exporting records should verify the message digest as part of the export process so that the records can be certified as authentic.

### Disposition of records

Disposition is the final chapter in the records life cycle, resulting in destruction of the records or their permanent, archival retention. Most states have laws establishing a process that determines which records are to be destroyed and how long those records must be kept before destruction. Often the laws delegate this authority to the state archives or a records management program. These laws apply to all records, regardless of format. It is important to follow the legal process to determine a retention period (called scheduling) and to obtain authorization to dispose of records. Most records laws contain a penalty for unauthorized destruction of records.

The records retention laws are intended to protect information of lasting value to the state. Of greater importance to the agency, the ability to demonstrate that records are destroyed according to the law and routine procedure is a defense against charges of spoliation or tampering with evidence in the case of litigation.

Destruction of records requires that all copies of a record be destroyed. Designing procedures to delete records must address not only the record keeping system, but copies of data kept for backups, disaster recovery, and the like. System designers should also work with risk managers, archivists, and business managers to assess the need to completely erase the data by overwriting it to make recovery unfeasible. Media containing records with private or confidential information should be sanitized as part of destruction.

Records destruction should be coordinated with backup and storage procedures so that deleted records are purged on a regular basis. Ideally, backup and disaster recovery copies should not be kept more than a month to ensure that deleted records do not survive much longer than their official date of destruction.

If records are to be kept permanently, then it is essential to develop a strategy to preserve those records. The challenges of long-term storage of electronic records are compounded when planning to keep records forever. Possible strategies include:

- Archives may negotiate with agencies to maintain records in the agency, rather than transfer those records to the archives. This approach is based on the assumption that the same process to migrate active records in the series can be used to migrate archival records from that series. Because of the caveats for long-term preservation, not all archivists believe this 'post- custodial' approach to archives will succeed in the long term.
- Agencies may have records exported to a standard, well-established file format that have several commercially available applications capable of viewing those records (packaging) before transfer. Packaging electronic records provides a self-contained electronic document that has all the contextual clues of the system from which it was generated. The goal of packaging is to minimize the long-term costs associated with maintaining the software for retrieval and display by using file formats that are based on open source design, specification and algorithms. While ASCII text files lack flair, they are a good example of a standard open source format that has proven the test of time. Likewise, technologies such as XML hope to provide the same transportable package of the electronic record preserved over time. This approach will require archives to address issues of media degradation and obsolescence. If the records are in a marked up format, it will be necessary to ensure that viewers remain functional. (With XML, that may require the preservation of externally referenced components, such as Document Type Definitions and style sheets). Archives will also have to address the problem of indexing the records for access. However, it will not be necessary to worry about the more complicated problems of proprietary applications or changes in operating systems.
- Until standards for electronic records preservation are developed, exporting records to computer output microfilm (COM) remains a viable option for preserving archival e-records.<sup>(9)</sup> As with long-term records, if the loss of the records would put the state at significant risk, agencies should consider transferring these records to a durable medium as a backup. For example, loss of birth and death records or of property records could result in loss of many individuals' rights.

Not all records are equal candidates for transfer to film or electronic preservation. Transfer to COM makes little sense if the ability to analyze or manipulate the records electronically is the basis of their value. However, archival use of records often differs from their primary use by the creating agency and the loss of functionality may not be significant.

The decision to preserve records electronically or on a durable medium is not an either/or proposition. A decision to preserve records exclusively in electronic format should be made in consultation with the archives professional responsible for their preservation.

---

(7) Secondary use is based on the value of the information in records beyond the records' original function. For example, the primary value of the federal census includes the apportioning of representation in the Congress and the distribution of federal funds. The primary value of a

#### IV. Managing the Risks of Moving to Electronic Records

---

census is diminished after the subsequent census. However, the census has secondary value as a genealogical tool that lasts much longer than the primary value.

(8) *Business Week* April 20, 1998

(9) Many archivists believe that in the absence of tested best practices for preserving records in electronic format, COM remains the best – if imperfect – solution for permanent, archival preservation of electronic records because COM's accessibility does not require future resources that may not be available.