JTC Resource Bulletin

Developing an Electronic Records Preservation and Disposition Plan

Version 1.0
Adopted December 5, 2014

Executive Summary

Courts have long had records retention and destruction schedules for paper case records. However, courts often lack the staffing resources needed to actually go through old files, sort and then destroy records. Thus, many such standing court record retention and destruction policies are generally permissive in nature, not closely followed and out-of-date in this new era of digital records.

Now that more jurisdictions are digitizing court records (data and documents), it is possible to systematically purge electronic records on an automated basis. However, before a court does so, a number of questions must be addressed in order to develop a sound electronic records policy.

This technology resource bulletin addresses the following policy areas and provides recommendations surrounding best practices in electronic records retention and destruction:

1. Should the electronic records destruction be automatic and, if so, what kinds of safeguards should be in place to ensure that the automated system is operating pursuant to court policy?
2. Should the electronic records destruction include both data and electronic documents?
3. What is the best way to delete court case data?
4. How long should a court system publish court records on-line, via the internet?
5. How long do records need to be maintained for research purposes and are records maintained beyond the standard retention periods subject to public disclosure?
6. How do courts designate historically significant cases for preservation? Should such designated case records be maintained by the court, the state office of record archives, or both?

After reviewing and consider the concepts in this bulletin, Court leaders will be able to develop a robust electronic court records retention and destruction policy for their courts.

Acknowledgments

This document is a product of the Joint Technology Committee (JTC) established by the Conference of State Court Administrators (COSCA), the National Association for Court Management (NACM) and the National Center for State Courts (NCSC).

JTC Mission:
To improve the administration of justice through technology

JTC Electronic Records Preservation and Destruction Work Group

David Slayton (Chair)
Texas Office of Court Administration

David K. Byers
Supreme Court of Arizona

The Honorable O. John Kuenhold
State of Colorado

Marcus Reinkensmeyer
Supreme Court of Arizona

Nial Raaen
National Center for State Courts

Joint Technology Committee:

COSCA Appointments

David Slayton (Co-Chair)
Texas Office of Court Administration

David K. Byers
Arizona Supreme Court

Laurie Dudgeon
Kentucky Administrative Office of the Courts

Gerald A. Marroney
Colorado Administrative Office of the Courts

Robin Sweet
Nevada Administrative Office of the Courts

NACM Appointments

Kevin Bowling (Co-Chair)
Michigan 20th Judicial Circuit Court

Paul DeLosh
Supreme Court of Virginia

Yolanda Lewis
Superior Court of Fulton County, Georgia

Kelly C. Steele
Florida Ninth Judicial Circuit Court

Jeffrey Tsunekawa
Seattle Municipal Court

NCSC Appointments

The Honorable O. John Kuenhold
State of Colorado

The Honorable Michael Trickey
Washington Court of Appeals, Division 1

CITOC Appointments

Jorge Basto
Judicial Council of Georgia

Craig Burlingame
Massachusetts Trial Court

Ex-officio Appointments

John Greacen
Forum on the Advancement of Court Technology

NCSC Staff

Paul Embley
Jim Harris
Ilonka Dazevedo

Document History and Version Control

Version	Date Approved	Approved by	Brief Description
1.0	12/5/2014	JTC	Release document

Contents

Background

Most state and local courts probably have a records retention and destruction schedule for paper case records. However, courts often lack the staffing resources needed to actually go through old files, sort and then destroy records. Thus, many existing policies are generally permissive in nature, not closely followed and do not address the retention and destruction of digital records.

Now that more jurisdictions are digitizing court records (data and documents), it is increasingly important that courts have a sound electronic records policy. While it is possible to systematically purge electronic records on an automated basis, the policies and processes that drive that automation must address a number of new and complex issues. Because paper records have historically not been destroyed on a consistent basis - at least not without microfilming - the standing destruction policies must be revisited, bearing in mind that the purged records will no longer exist.

Courts may address that concern by instituting a policy requiring no destruction of electronic records. However, that will lead to rapid growth in required storage space. Not only is the maintenance of this storage costly, but an automated records management system will quickly reach the point that backup and restore features can become unworkable due to the volume of records. Ultimately, large data stores will also result in inordinately long search and retrieval times, reducing efficiency of court operations. Life cycle costs associated with data and document storage are delineated in Figure 1.

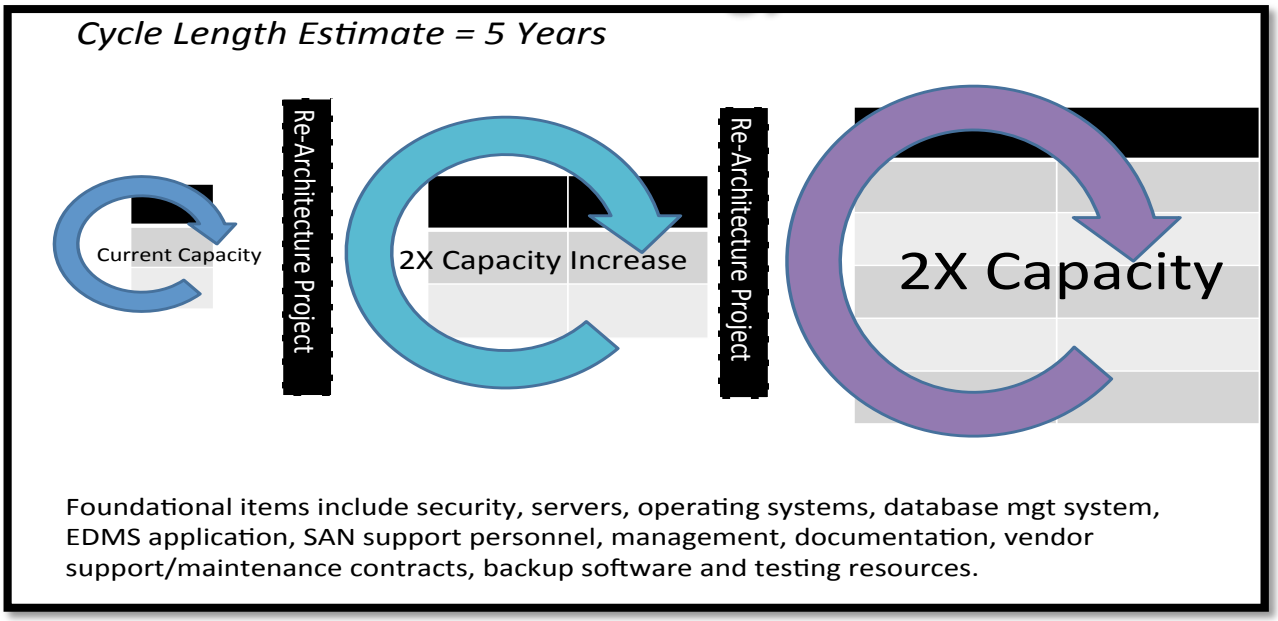

Figure 1: Future Cycles of Storage Technology

Questions in Development of an Electronic Records Policy

In developing comprehensive electronic records retention and destruction policies, courts must consider records access, operations and technical issues. Once the retention period for a particular category of case has been reached, will the destruction of records be mandatory or permissive?[1]

Whether a centralized or decentralized court system, there are good arguments that records management policies be consistent throughout the statewide judicial system. Litigants can be harmed or helped by the status and availability of their records.[2] Other justice entities also regularly access court records and expect consistency in the availability of records. Thus, as a general guiding principle, electronic records management policy and practices should not be a local option.

Other electronic records policy issues include the scope of records under consideration, methods of records destruction, the length of time records are available to the public on-line and the historical value of certain court records. These issues fall in three interrelated areas of policy, which are best considered collectively in record policy formation: retention, destruction and public access.

[1] Addressing best practices under the principle of disposition, the COSCA 2012-2013 Policy Paper, "To Protect and Preserve: Standards for Maintaining and Managing 21st Century Court Records," states that courts should, "Remove non-essential, obsolete or duplicate records routinely."

[2] "State court systems must ensure that records disposition policies are implemented in a consistent manner statewide, particularly considering the fact that individuals rights can be adversely affected by such records and manage them consistently from jurisdiction to jurisdiction." COSCA 2012-2013 Policy Paper.

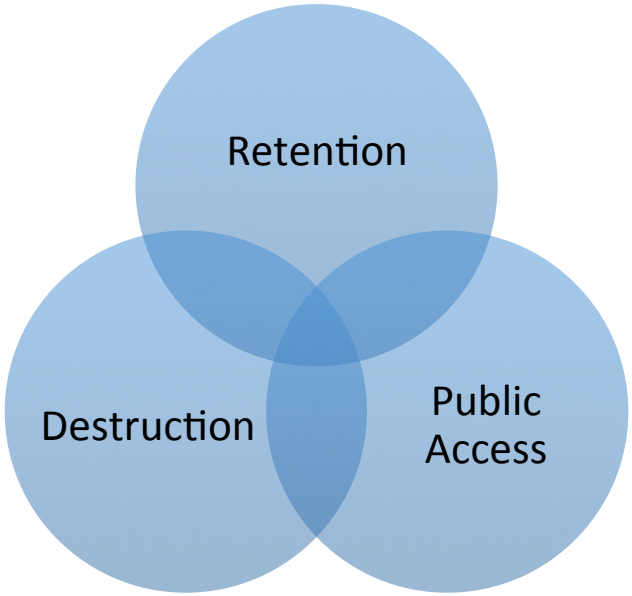

Figure 2: Electronic Court Records Policy

Specifically, a comprehensive electronic court records policy should address the following questions and clearly delineate supporting procedures:

Should the electronic records destruction be automatic?

If so, what kinds of safeguards should be in place to ensure that the automated system is operating pursuant to court policy?

Should the electronic records destruction include both data and electronic documents?

It is unlikely that a policy should allow for maintenance of case management data, while at the same time mandating destruction of supporting court documents. This situation would be problematical when a litigant returns to court for some action, following the destruction of the records, e.g., a motion to set aside a conviction.

How best to delete court case data?

Deleting case data is not easy. Case management systems will place data about a case in a variety of locations. Actual deletion of a case may have to be mapped. Local courts using the same CMS may not use it consistently. An alternative is “soft deletion,” wherein the data remains, but the searchable link is broken. This approach would prevent a case lookup. While this method is easier than that of physical data destruction from a technical standpoint, it does not reduce data storage space needs. Thus there are pros and cons of each method. Compounding the problem is the issue of financial records associated with a

case. Deleting records that have data linked to the general ledger system will cause technical and operational issues.

How long should a court system publish court records on-line?

Many court systems have a case look-up system on-line. One approach is to make the time period consistent with the records destruction time period. Another approach is to make the on-line access time period subject to any "look back" requirements, e.g., reference to criminal convictions for prior offenses as provided by statute or court rule. The Arizona state courts found that even after expiration of this time period, there was still a need for the courts to maintain records to allow involved litigants to return to court to request a "set aside" of conviction or records expungement.[3] Litigants may need this extended records availability "service" in order to qualify for a job related licensing requirement, housing, passport and visa requirements or other reasons. This is true both for misdemeanor and local ordinance violations, as well as criminal felony convictions.

How long do records need to be maintained for research purposes and are records maintained beyond the standard retention periods subject to public disclosure?

In considering the optimal scope of records required for research purposes, it is advisable for courts to fully consider data/document requirements for legislative inquires, program evaluation and longitudinal studies.

How do courts designate historically significant cases for preservation?

Should such designated case records be maintained by the court, the state office of record archives, or both?

In addressing the foregoing policy questions, courts are challenged to balance the public's need for long-term access to court records with the high cost of digital records storage. Potential harm to litigants due to longstanding convictions in limited jurisdiction courts (e.g., convictions for misdemeanor and local ordinances offenses) should also be considered in this context. The analysis should take into account the frequency of reference to disposed records for each specific case type (e.g., civil, criminal, probate, family, juvenile) for each jurisdictional level of court (limited, general and appellate jurisdiction courts).

---

[3] *Report of the Advisory Committee to Develop Policies for Retention, Destruction, and Access to Electronic Court Records*. Rep. Supreme Court - State of Arizona, Dec. 2013. Web. 6 Nov. 2014.

Figure 3 depicts a framework for defining an optimal retention period ("sweet spot"), predicated upon the likelihood that records will be needed, versus long-term storage costs. This analysis is best informed with input from court record users, including litigants, the media, data aggregators, investigators, etc. Input can readily be gathered through surveys, focus groups and on-line public comments regarding proposed electronic records policies.

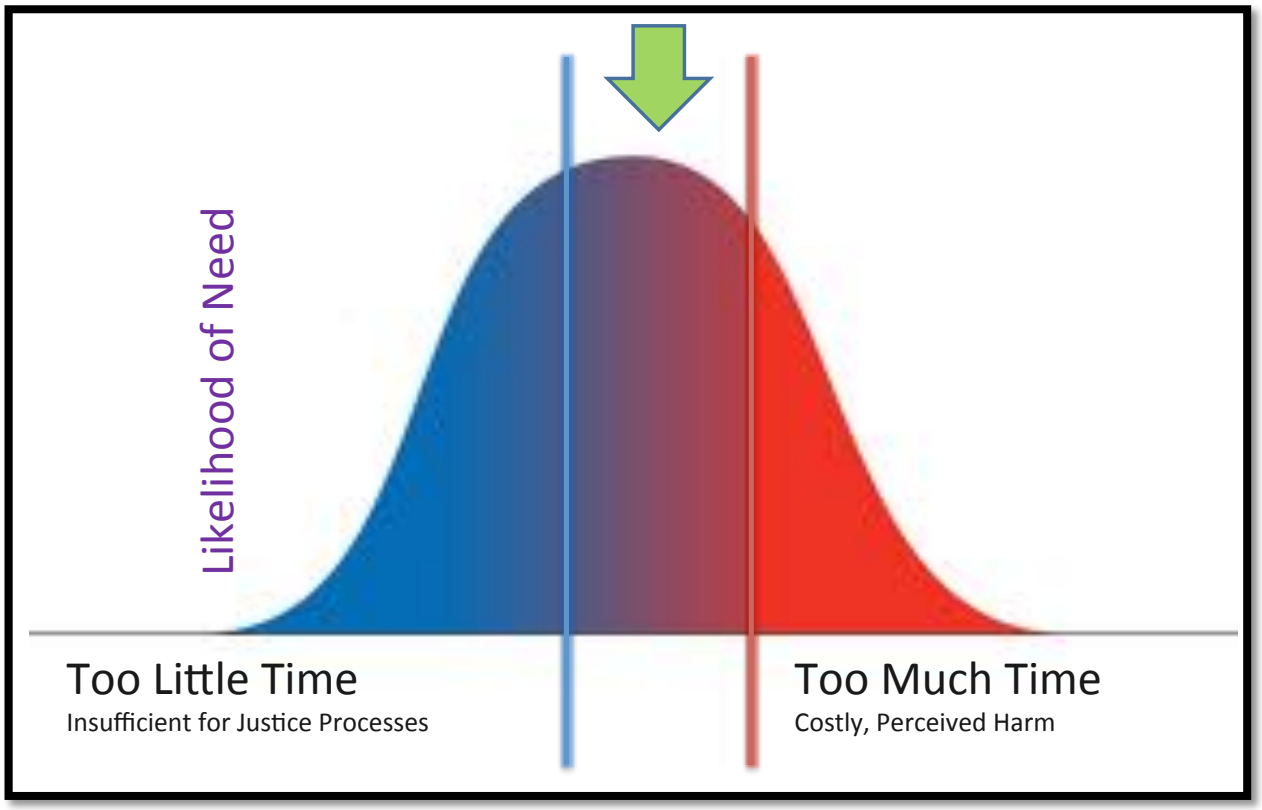

Figure 3: Locating the "Sweet Spot" for Records Retention

Records Preservation

Records preservation is one of six key principles identified by the 2012-2013 COSCA white paper, *To Protect and Preserve: Standards for Maintaining and Managing 21st Century Court Records.*[4] The paper sets forth a set of principles as a framework for assessing and implementing effective judicial records management practices based on the Generally Accepted Recordkeeping Principles© developed by ARMA

[4] Linhares, Gregory J., and Nial Raaen. *To Protect and Preserve: Standards for Maintaining and Managing 21st Century Court Records*. Conference of State Court Administrators, 2012-2013 Web. 10 Nov. 2014.

International[5]. This paper explores the issues, key elements, and emerging solutions for preserving electronic records.

The increasing adoption of e-filing and digital imaging systems is bringing the courts closer to the promise of truly paper-on-demand record systems. Rules in many states now authorize courts to destroy paper records upon digitization and authorize the digital version as the official record. However, record retention requirements for long-term preservation of some record types will require preserving digital records over periods of time exceeding ten years. The readiness of many courts to maintain digital records in the face of continuing hardware, software, and storage media obsolescence and evolution is a matter of concern. Further, many courts have not applied retention schedule requirements to the destruction of digital records that have exceeded their required retention period or engaged in adequate preservation planning.

Responses to a 2011 survey distributed on the COSCA list serve illustrated the variety of policies concerning approved media for long-term preservation of court records. Most survey respondents indicated that their state has adopted standards for short-term retention of records in both paper and digital form, however, only a few had adopted standards for long-term digital preservation. The respondents were about equally divided on the continued reliance on microfilm as the primary media for long-term records preservation.

The lack of readiness of governmental agencies to ensure the long-term preservation of digital records has been an issue of increasing concern outside the courts as well. A 2011 survey of state archives in fifty states and four territories conducted by the Council of State Archivists (CoSA) confirmed the inadequacy of electronic records programs across the country:[6]

- 35 states reported they do not have an electronic records program;
- 34% do not accession electronic records;

---

[5] **About ARMA International and the Generally Accepted Recordkeeping Principles®**
ARMA International (www.arma.org) is a not-for-profit professional association and the authority on information governance. Formed in 1955, ARMA International is the oldest and largest association for the information management profession with a current international membership of more than 10,000. It provides education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy. It also publishes Information Management magazine, and the Generally Accepted Recordkeeping Principles®. More information about the Principles can be found at www.arma.org/principles.

[6] *State Electronic Records Initiative - Phase I Report.* Council of State Archivists', State Electronic Records Initiative (SERI) Committee, June 2012. Web. 6 Nov. 2014.

- Few state archives have the resources and support necessary to integrate special project results into long-term electronic records management strategies;
- Few state archives have a working relationship with their state IT departments, and most are not integrated into the system decision making processes;
- One-quarter of the state archives and all four territorial archives indicated that they had done nothing to manage and preserve electronic records;
- Only five state archives indicated that they have a planned system for developing electronic records management and preservation.

The CoSA report concludes that it is "likely [that] no state has a system which would pass the test audit for the ISO standards for a Trusted Digital Repository." The apparent lack of capability of state archival agencies to maintain electronic records raises concerns that other state and local government agencies, including the judiciary, are similarly unprepared.

The CoSA findings are supported by many experts who maintain that few organizations currently have the technical capacity for long-term preservation, and that a substantial proportion of digital information is therefore at risk for loss. The following graph from savingthedigitalworld.com, an organization dedicated to raising awareness of digital preservation issues, predicts substantial loss of information over time in traditional data centers:

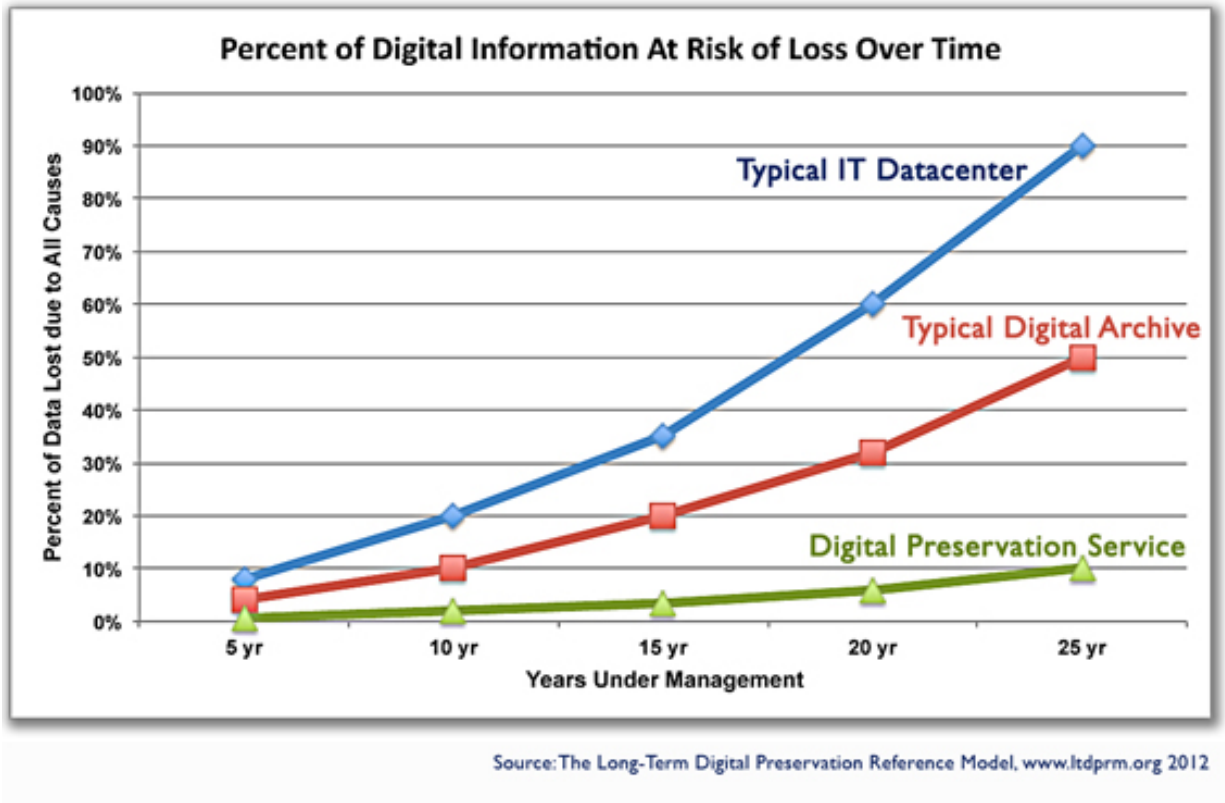

Figure 4: Percent of Digital Information at Risk of Loss Over Time

Compared to their paper and microfilm counterparts, electronic recordkeeping systems are generally more vulnerable to undetected alteration or loss. This vulnerability means that there is the need for more comprehensive and detailed planning to preserve digital records over time.[7] The preservation of digital records also requires more intervention and expertise than is the case with paper records. Stored under the proper conditions, paper records have survived for centuries. Long-term digital preservation, on the other hand, involves regular monitoring, frequent intervention, and specialized technical capabilities. Finally, the longevity (market life) of digital records technology products and the vendor community providing systems and support services is volatile. Maintaining this long-term commitment to use digitally stored information requires a series of activities that maintain its retrievability, readability, and intelligibility.

Perhaps the greatest challenge to long-term usability of digital information are the rapid improvements in software applications and computer hardware that have led to what is

[7] "Electronic Records Management Handbook." (n.d.): n. pag. *DGS Digital Services, Office of State Publishing*. State of California, Department of General Services, Feb. 2002. Web. 7 Nov. 2014.

known as technological obsolescence. Technological obsolescence is attributable to a number of factors unique to the digital world. These include:[8]

Media obsolescence. The options for storage and presentation of digital data continue to evolve. New technologies and higher density storage materials are regularly replacing older products and techniques.

Media failure. Various media have estimated life spans which represent their useful life cycle under ideal conditions. All media are susceptible to various levels of failure, with removable media being more vulnerable. Manufacturing defects, poor storage conditions, frequent handling, physical damage and deterioration of media surfaces are factors that can reduce the useful life span.

Hardware and software obsolescence. The continuing development and increasing sophistication of hardware and application software results in rapid obsolescence of software used to create and process electronic information.

File format obsolescence. The increasing range and complexity of formats in which data is maintained creates another challenge. Features such as hidden text and change history make digital documents more useful, but also create challenges with long term storage and retrieval.

Forward/Backward Compatibility. The need for wholesale conversion or migration of records can be deferred when newer systems are able to read data and files from older versions. However, older files may lose their formatting or other characteristics that have been improved or no longer exist in newer versions.

The term “readiness” as defined by the National Archives and Records Administration implies the need for a proactive approach to electronic records management. The following are some of the activities that are part of a planned response to preservation:[9]

1. Continually identifying records that are endangered by technology obsolescence, media fragility and other threats;
2. Developing preservation rules and methodologies for the entire lifecycle of electronic records;
3. Addressing security, privacy and custodial issues to ensure authorized and authenticated access to digital materials;

---

[8] Tilbury, Jonathan. *The Active Preservation of Digital Information* (July 2013). Web. 8 Nov. 2014.

[9] "Fast Track Guidance." *National Archives and Records Administration*. National Archives and Records Administration, n.d. Web. 11 Nov. 2014.

4. Planning for obsolescence of formats, software and hardware by adopting preservation methods to ensure that electronic records will remain accessible;
5. Developing appropriate storage architecture and infrastructure for electronic records and related preservation metadata.

Clearly, effective preservation is not an afterthought but requires attention to long-term needs throughout the records lifecycle.

Preservation Policy Recommendations

While there is no single comprehensive solution to this challenge, there are a number of steps that judicial organizations can take to address digital preservation, including policies, planning, and technical conditions that collectively contribute to a higher probability that today's records will still be usable tomorrow. These are described and summarized in a series of policy recommendations that courts should consider adopting as part of an overall records management plan. The elements described below should be incorporated into a *digital preservation strategy* to ensure that digital records remain accessible and usable over time.

Preservation Planning

Plan and implement processes and procedures for the conversion and migration of digital records and the systems that support them to new formats, storage media, and technologies.

A preservation strategy may involve planning for one or more of the following methods of preserving digital information:[10]

Migration – Migration transfers data or objects from one format to another in order to ensure continued access using new technologies. There are a number of strategies that can be employed, including normalization, migration at obsolescence, and migration on demand. It is possible that bits of data may be modified during migration, which can compromise data integrity.

A sound migration strategy requires technical support and supervision to ensure the preservation of the original characteristics of the record upon migration. The long-term usability of digitally stored information, including scanned document

[10] Brown, Adrian, Shadrack Katuu, Peter Sebina, Anthea Seles, and International Records Management Trust. "Training in Electronic Records Management, Module 4: Preserving Electronic Records." 2009. Web. 7 Nov. 2014.

images, digital data, and descriptive index data, will best be achieved by implementing a sound policy for migrating data to future technology generations, adhering to well-documented image file-header formats, and monitoring media degradation.

Preserving Legacy Systems - Many courts are now using second or third generation electronic case management systems. Older data may still reside on legacy hardware accessed by software that is no longer supported by the vendor. In many instances data residing on these systems will be used for information purposes only. However, information retained under these circumstances will remain viable only as long as replacement hardware and qualified programmers are available to keep these systems running. As a strategy, maintaining outdated systems can be risky but may be the only viable option in some instances.

Emulation – Emulation involves using a computer or software program to imitate the functionality of an older system and offer the best possible rendition of the original document or data. Emulation may include application software, hardware, and operating systems. However, this strategy may only prolong technical dependence on the emulator itself.

Transfer to Other Media - At some point the original software may no longer be available to access or read information. Digital records which are at the point in their life cycle where case processing functionality is not needed but the content of those records must be maintained for reference or archival purposes can be migrated to other less volatile media, including laser disk, microforms, and even paper.[11]

The best preservation option will depend on a number of factors, including the record lifespan, format, frequency of and need for access, cost, and support capabilities.

Storage Management

Digital records must be maintained under physical storage conditions appropriate to the type of media and in compliance with manufacturer and industry standards.

The longevity of all records, regardless of the type of media, is determined in part by the conditions under which they are stored. In addition to maintaining

[11] Stephens, David, and Roderick Wallace. "Electronic Records Retention: Fourteen Basic Principles." *Information Management Journal* Oct. 2000: 38-52. .

environmental stability (temperature and humidity) and protection from contaminants and sunlight, digital media require other specialized storage conditions. Redundant and separate logical or physical storage mitigates the risk of losing records from device failure, unintended deletion, and natural disaster, among other factors. The selection of storage systems should consider acquisition and maintenance costs, as well as the projected system life cycle.

The selection of storage methodologies should be based on the preservation requirements specific to the record series and media, along with the need for access by information users.

Various media and storage systems offer different options for maintaining digital records. For Instance, hierarchical storage systems can organize data storage between higher-cost, more accessible storage media and lower cost off-line storage according to the need to access or update a record series. Specialized software is available to monitor data utilization and can automatically move information from higher cost disk storage to tapes or other storage devices which more economically storage large volumes of data.

One approach is to implement an "active archive" solution combining disk and tape storage for storage of archival data while allowing more active data or documents to reside on more readily accessible disk storage. Before adopting a storage architecture approach the court must be able to clearly define the conditions or circumstances under which documents or information are most economically and efficiently maintained between various storage levels.[12]

Security Access and Control

All digital records under the judiciary's control should be protected from inadvertent or intentional alteration, destruction, or disposal through the maintenance of security access controls appropriate to the record and corresponding users' rights.

All digital information should be subject to user controls and physical protection. This includes protection of the physical infrastructure from accidental or deliberate damage, protection from external intrusion or unauthorized users, and maintaining clearly defined access and permission controls so that the ability to alter or delete objects in a digital repository is limited to those responsible for

[12] Moore, Fred. *The Data Archive Challenge - What's Your Game Plan?* Horison Information Strategies, n.d. Web. 7 Nov. 2014.

preservation tasks. Access or duplicate versions of records should be created for public access.

Disaster Mitigation and Preparedness

A written disaster plan and recovery protocol should be in place and periodically updated to identify roles and responsibilities in the event of a natural or man-made disaster.

Judicial organizations must include the protection and preservation of mission-critical records and information in an overall continuity of operations and risk management planning. *Risk mitigation* includes conducting a regular assessment of records systems and storage conditions to identify potential risks or hazards before they compromise record integrity and access. A *risk assessment* is a systematic process that helps identify the chances of a damaging event, estimate the costs of remediation, and set priorities for corrective action. A *hazard audit* focuses on the identification of immediate and potential risks that exist in the workplace. *Continuity planning* includes planning and preparation for the most likely disaster scenarios to enable the organization to identify its most critical records and take immediate steps to minimize further loss and damage.

Auditing and Quality Control

Digital records and storage systems should be audited for integrity on a routine basis, as well as during migration, transfer, or system change events to test for data corruption and media failure.

A program of audits and reviews of records media and systems is a good strategy for all types of records. This includes monitoring media for deterioration, checking the accuracy of metadata entry and indexing by staff, comparing original documents with the captured electronic images and index data, and ensuring overall compliance with records policies. The integrity of digital objects should be validated through the use of check sums and other tools. Checks should occur upon creation, before and after migration, and at other points where digital objects are at risk of alteration. Media should be sampled at time of acquisition to check for manufacturing defects. Maintenance and review of system logs provide a record of who has accessed or modified digital records. When corruption or deterioration of any record or its associated metadata is found, steps should be taken to recover the record if possible, and documentation of the result maintained for the planned lifecycle of the record.

Adoption of Open Standards

Open standards and formats should be adopted to facilitate access, exchange, and transferability of digital records over time.

The use of archival, open formats for electronic record preservation is a recommended best practice in the records management field. Approaches include saving records to an archival format upon record creation, or moving records from proprietary systems and formats at a later stage in the lifecycle, such as at point of transfer to a digital archive. Open system computing promotes interoperability between differing systems, flexibility in upgrading and migration, and sustained access to content. While open formats do not solve the problem of hardware obsolescence, they do improve the chances that documents will remain readable and accessible over time provided the integrity of storage media is maintained.[13]

Classification, Indexing and Metadata

All records should be subject to an organizationally-defined indexing or classification scheme to promote efficient access and management.

Many records under care and control of the judiciary are maintained in structured databases and indexes. However, there are increasing amounts of "unstructured records" being created in all organizations that may be maintained on shared drives, tablets and personal computers that are created by employees as part of their daily work. The most common examples are office automation work products, email, and social media exchanges. It is often difficult to determine the extent and value of this information. A records inventory or information "map" can assist in determining the location and nature of unstructured information. The results of an inventory can be used to identify records and information that are transitory or duplicative from more critical information that supports on-going organizational functions. This information can be used to develop appropriate policies and procedures for naming, indexing, and preserving records.

Create and maintain appropriate metadata to ensure that digital information can be accessed and authenticated over time.

Metadata plays an important role in long term digital storage and preservation by recording the information necessary for accessing records, ensuring record integrity, and facilitating conversion and migration activities. Metadata serves

[13] Hoke, Gordon E.J., CRM. "Future Watch: Strategies for Long-Term Preservation of Electronic Records." *Information Management*. ARMA International, May-June 2012. Web. 7 Nov. 2014.

multiple purposes in the records lifecycle, and models which are designed to address preservation are available for adoption. The use of metadata to define changes in the logical and physical structure of records, define changes in technical attributes, and document changing relationships with other records is critical to maintaining record integrity and documenting chain of custody.

Archival Storage

Archival storage should be planned for retaining digital information over longer periods of time or for records which are considered "permanent."

Digital archiving is a set of processes, activities, and technical conditions for managing digital information over time to prolong its accessibility and security. Dedicated archival storage, whether in-house or provided by a third party, is often required for records which are no longer in active use but which require preservation for historical or legal purposes. A number of standards and conditions for digital archives have been developed and continue to be refined. These are described in more detail in the Emerging Models section of this report.

Adoption of Standards and Performance Measures

Appropriate industry standards for digital preservation should be adopted along with performance measures to determine the effectiveness of preservation efforts.

There is also a growing body of records management standards available for reference and use, covering paper, microfilm and electronic records. Recognized standards have been developed by the International Organization for Standardization (ISO),[14] U.S. Department of Defense (DoD),[15] ARMA International,[16] the Association for Information and Image Management (AIIM),[17] and the American National Standards Institute (ANSI). Court leadership and their

---

[14] "ISO/TC 46/SC 11 - Archives/records Management." *ISO*. International Organization for Standardization, Web. 13 Dec. 2014

[15] Office of the Deputy Assistant Secretary of Defense/ Deputy Chief Information Officer, Information Policy Directorate. *Electronic Records Management Software Applications Design Criteria Standard*. 25 Apr. 2007. DoD 5015.02-STD. Arlington, Virginia.

[16] "Records Management Is The Foundation Of Compliance." *Electronic Records Management*. ARMA International, n.d. Web. 12 Dec. 2014.

[17] "Analysis, Selection, and Implementation of Electronic Document Management Systems (EDMS)." *aiim: The Global Community of Information Professionals*. Association for Information and Image Management International, 5 June 2009. Web. 13 Dec. 2014.

technical partners should refer to these standards and adopt those that are relevant to the types of record systems under their control and care.

Multi-media records

Special provisions for the disposition of records containing multi-media content may need to be made for those records being preserved over longer periods of time.

The increasing sophistication of office automation products allows the embedding of files and materials created with un-related software programs. An example includes a Word or .pdf document with an embedded video or audio file. This may be problematic if the document is subject to long-term preservation in an archive, as it may be difficult to ensure that the supporting software for an embedded file will still be available at a later date.

Historical / research value holds

Records should be periodically assessed for their historical and research value in consultation with interested agencies and institutions.

Many state retention schedules require that courts notify the state archives of pending destruction of court files to provide an opportunity for action to be taken to preserve items of historical interest. Certain individual cases and related records may have historical value by virtue of their notoriety or precedential value. The research value of court information is more difficult to estimate, however, judicial leadership may wish to consult with other agencies or educational institutions regarding information that would most likely be used for research purposes.

Records Disposition

The foundation of this principle of disposition is the recognition that all records reach a point in their lifecycle where they are committed to archival storage and preservation, or scheduled for destruction. This section addressed the transfer and accession of digital information to archives, as well as the destruction or deletion of electronic information as activities that fall under the principle of disposition.

Storing terabytes or even petabytes of information is no longer unusual. The decreasing cost and increasing capacity of storage technologies for electronic records has had the unfortunate consequence of making it easy for many organizations, including courts, to retain digital information well beyond its useful life. However, it has also become evident that the retention of ever-increasing amounts of information that has passed its useful

lifecycle is costly. In addition to the costs for physical storage, electronic records must be periodically migrated to stay ahead of hardware and software obsolescence. Large volumes of data complicate search and retrieval. The indirect costs of managing data cannot be ignored. Further, the longer electronic records are retained the greater the risk to their integrity and accessibility.

All records have a life cycle which begins with their creation or acceptance through their final disposition. A comprehensive records management program ensures that attention is given to records over the entire life cycle from creation to disposition, regardless of format. As courts increasingly rely on electronic case management systems, office automation products, and document management systems, giving attention to the disposition of electronic records at the end of the life cycle is of critical importance.

Retention Schedules

A record retention schedule is the source of authority for records disposition and should address all records under the organization's care and control, including administrative records. The schedule should provide for the systematic destruction of electronic records which no longer serve business or legal needs, while ensuring the continued retention of those records that have an ongoing value. Disposition therefore includes both records destruction and long-term preservation.

Case files and related documents in the state courts are typically covered by general records retention schedules created by statute, court rule or policy directives. These schedules are unique to each jurisdiction, but in many cases have not kept up with the rapid change in record-keeping technologies. Further, many records created and maintained by the courts may not be specifically covered under general schedules. Courts therefore may need to develop internal retention schedules for records not covered by a general state schedule.

Although many schedules do address both paper and electronic records, there are different approaches to the format of retention schedules in a hybrid (multimedia) environment:[18]

Media specific – provides separate schedules for electronic and human-readable records

[18] Stephens, David and Roderick Wallace. "Electronic Records Retention: Fourteen Basic Principles". *Information Management*, October 2000, Vol. 34, No. 4; ARMA International.

Media independent – specifies the retention period for each record series without reference to the storage media, even though records may reside on several media simultaneously or during various stages of the lifecycle.

Multimedia – one that contains all media within a single schedule, but with separate retention periods for the records contained on each type of media

An informal NCSC review of state retention schedules found that most feature a media independent approach to retention and disposition. Typically, media issues are addressed in terms of approved formats and standards for preservation of digital records.

Records Appraisal

The process of determining the retention value of a record is often referred to as a *records appraisal*. The value of records can be evaluated on the basis of their *primary* and *secondary* value. Primary values are those which meet the basic business purpose of the record, such as maintaining a verbatim record of court proceedings for review and possible appeal. Secondary values are other uses for the information, which frequently follow the expiration of the period of primary value retention. Examples include retaining information for historical or research purposes.

There are four values that are generally used as guidelines in assessing records for retention:

Operational value – This is the period of time during which the court requires the record to perform its primary function. This may reflect only the time that records are required to meet user needs; they are not necessarily legal requirements.

Legal value – This refers to those records whose retention is defined by statute or court rule, or those that may be needed in case of further litigation or investigation. Legal value is determined by factors such as:

1. Statutes, court rules, or judicial orders requiring records to be kept for specific periods;
2. Statutes or regulations requiring records to be kept, but not specifying retention time periods;
3. Records which set legal precedent.

Fiscal value – This refers to records that are created for administrative purposes as well as case-related transactions. These include payment transactions, budget documents, purchasing records, and payable records. In addition to the

need to preserve fiscal records to meet business or operational requirements, fiscal value is generally determined by the time that these records must be retained for audit purposes under state or local statutes.

Historical value – This is the long-term value of records which may, by virtue of their exceptional age and/or connection with some significant historical event or precedent, have long-term value. In some situations, individual cases or records will be identified for historical preservation, or an entire series, by virtue of its age, may be retained for its historical value. There are requirements in many states that local or state archive agencies be consulted prior to the destruction of certain judicial records, or that records be moved to the custody of the archive.

A record series or individual records within a series can possess more than one value at the same time, or sequentially, over the record's life cycle.

A useful metric for determining operational value is the *reference rate.* This simply refers to the frequency with which a record in a given series is accessed by court staff, litigants, or the public. Determining the reference rate for a record series is useful in deciding when records should be moved from active to inactive or archival storage, as well as determining the appropriate retention and destruction period.

The increasing reliance on email communications and the emergence of business applications for social media contributes to the complexity of managing organizational records. Electronic record keeping in particular has resulted in widespread information redundancy due to the ease in which records can be duplicated, distributed, and modified. Part of the task of developing a retention schedule is determining what should not be considered a record for business purposes.

Deletion/Destruction of Data

There are currently a number of techniques which are available for the permanent disposal of electronic records. The choice of method depends on a variety of factors, most significantly the type of media on which the records are retained, the cost, and the need to protect confidentiality. Some of the most common techniques currently in use include:[19]

[19] Stephens, David and Roderick Wallace. "Electronic Records Retention: Fourteen Basic Principles". *Information Management*, October 2000, Vol. 34, No. 4; ARMA International.

Removable Media Destruction (Shredding). Various types of removable electronic media, including CDs, DVDs, diskettes, magnetic tapes, and cartridges can be shredded into particles. Shredding standards have been established that meet the needs for destruction of classified information.

Degaussing. Degaussing is a process that renders data stored on magnetic media unreadable by changing the magnetic properties of the media surface. The application of a strong alternating magnetic field results in the loss of exposed data and renders the media in a magnetically neutral state. Degaussing is appropriate for hard drives and certain types of removable electronic media, such as backup and digital tapes.

Hard Drive Destruction (Punching/Crushing). Hard drives can be destroyed by machines that hydraulically crush machines. The crusher utilizes a punch that causes irreparable damage to the hard drive chassis, while also destroying the internal platter. This force is sufficient to alter the drive so that it cannot be reconnected or inserted into a functioning computer.

Encryption and Media Overwrites. Digital information may also be rendered inaccessible through encryption and overwriting of the media with new information. These techniques may not be suited to records which are confidential, but are adequate for situations in which the physical media is still in good, reusable condition.

"Soft" Deletion. Information which is no longer required to be retained for public access or business purposes can be rendered inaccessible through the deletion of links or flagging the record to be deleted. The action will render the information temporarily inaccessible. A full or hard deletion of a record may be scheduled for a set period of time following the soft delete, after which the record is permanently deleted. The advantage of a soft delete is that it provides some protection in case records need to be accessed to correct errors in publication of court records which have passed their normal retention period.

The widespread use and dissemination of court records by private companies and the publication of court information to the internet increases the potential harm from incorrect or outdated information. Despite limitations on the use of public records for commercial purposes under the Fair Reporting Credit Act, information may remain published for periods of time that exceed the normal retention period for the particular record series. For this reason many courts have continued to retain case information, which would normally have been destroyed, well beyond the retention period as insurance against later disputes over information accuracy.

Disposition by Transfer (Archiving)

Electronic records which are no longer of business value but are required to be retained for longer (over ten years) periods of time may be disposed through transfer to an internal digital archives. Archiving is often a way of migrating documents and data from more costly, online media to secondary and less expensive storage based on the declining need to access the record series. Archiving is often confused with backups. Backups are copies of data which may be used to restore the original after a data loss event. Archives are not synonymous with storage of low-value data. Archives are an important method of disposition for records whose preservation is required for legal or historical purposes. New standards and approaches are being developed to address the need for longer term digital archiving. Another archiving option is to dispose electronic records by transfer to non-electronic or analog media for long-term preservation.

Disposition by Accession

Accession is defined as the transfer of a record to a third party or external agency for preservation. For court records, accession usually involves transfer of records to a state or local archives, which assumes responsibility for the records' further preservation. This procedure is used to preserve historical records by moving them to a facility where conditions and oversight are more conducive to long-term preservation. Several state archives have now begun to accept digital court records for long-term preservation. Successful accession requires attention to these additional tasks[20]:

- Ensuring that each digital object is properly labeled with a unique identifier and associated metadata or finding aids
- Conversion of records, if necessary, to open standards formats (i.e., PDF/A, XML) as part of the transfer process
- Scanning of digital objects and hardware used in the process for viruses or malicious code
- Documentation of the transfer process in detail and verification of receipt for audit purposes
- Testing of transferred records before and after the process using checksums or other validation processes to verify integrity

Whether records are archived internally or to another agency, the judiciary must be certain that all operational and administrative needs have been satisfied prior

[20] International Records Management Trust. "Training in Electronic Records Management, Module 4: Preserving Electronic Records." 2009. Web. 7 Nov. 2014.

to transfer or accession, as well as maintain backup copies of transferred records until the transfer process has been completed and verified.

Disposition Policy Recommendations

The following are some of the policy considerations that should be taken into account when developing policies and procedures for the disposition of electronic records:

Criteria for disposition

The criteria for disposition of all records must be clearly specified in the records retention schedule.

When disposition is contingent upon a triggering date, the events associated with a records series must be clear and actionable. Triggering events typically will have associated dates such as a final verdict or disposition in a case file, or "employee termination" event date for employee personnel files. The meaning of "disposition" or "termination" must be clear and generally understood, particularly if the court relies on an automated process to delete or transfer the record or file. Exceptions must be clearly defined in the system, for instance, whether a re-open event resets the timer for disposition. The information must be properly and accurately captured in an information system. This is generally straight-forward in most case management systems, but may be more problematic with unstructured records such as office documents.

Robust records management software for removal of records should be in place with retention rules applied to effectively obliterate the data once all conditions for disposition are met. The system should further provide monitoring and oversight to ensure that only eligible records (i.e., those meeting retention requirements with no legal preservation holds) are destroyed.

When records are being held by an outside agency or vendor at the time of disposition, the court must ensure that the organization has the requisite capabilities to properly destroy the materials and require that verification of the destruction be provided.

Approval Mechanism

Policies for disposition of records should clearly identify the approval process for disposition, including whether disposition occurs automatically or requires human intervention for the disposition event.

Ensuring the proper disposition of electronic records requires a determination of the most appropriate manner for approval of destruction or transfer. This includes whether the migration of records and data from the primary storage system to secondary storage occurs automatically through system software controls, and whether any human intervention is required before this occurs. Some experts[21] suggest that this depends on the type of storage management software that exists in the computing environment, if any. For instance, hierarchical storage management software may support the automatic migration of records from primary to secondary storage media without intervention.

Documentation

The disposition of all records, whether through destruction, transfer, or accession, must be accompanied by a record of that action.

Just as with paper records disposition, documentation must be retained that adequately describes the records series, the date and method of disposition, the authority for disposition, etc. An audit trail should exist and disposition metadata maintained for information such as disposition date and type, retention trigger and date, original creation date, closure date, etc. As with all records there must be documentation of the destruction process. For physical records this is often accomplished through a certificate of destruction. For electronic records it may be done using the audit trail from the destruction process and preserving related metadata.

Metadata

All records subject to disposition should have been assigned sufficient metadata to ensure proper identification of those records, including preservation metadata for records which are archived and a metadata "footprint" of records destroyed in accordance with the retention schedule.

Depending on the operating definition of public records, dispositional metadata may be considered to be a public record. As proof of proper disposition metadata may be the most reliable method of ensuring transparency and accountability. Steps will need to be taken to determine how the dispositional metadata itself is stored and made available.

[21] Stephens, David, and Roderick Wallace. "Electronic Records Retention: Fourteen Basic Principles." *Information Management Journal* Oct. 2000: 38-52. .

Related Records

Related or integrated records with differing retention requirements must be identified and steps taken to ensure that disposition of one record does not compromise or cause a related record to be disposed of prematurely.

Court records are increasingly interrelated. Case management information residing in databases may be linked to court records on dedicated servers and documents in document management systems through hyperlinks. In addition, documents may be generated from data fields in the case management system. Staggered disposition of inter-dependent systems may disable certain features. In some cases, inter-related records may be subject to differing retention periods. This needs to be taken into account prior to disposition.

Selection of Disposition Methods

Retention schedules should specify the allowable methods of destroying digital records in accordance with record content and type of media.

The appropriate methods for disposing of records will need to be determined based on the type of media, relative confidentiality of the record, local technical capability, and availability of third party resources for archiving or destruction. As noted in the foregoing discussion, there are a number of commercial processes for properly destroying digital records, as well as archival systems for longer-term preservation that may be employed.

Alignment with Paper Destruction

Retention schedules should identify records preserved on more than one form of media (paper, microform, digital) and should clearly specify if there are different disposition timelines and types for each record/media type.

Many courts will continue to operate in a hybrid environment for the foreseeable future, maintaining hard-copy versions of records which also exist in digital form. If the current records retention schedule only addresses hard copy records, the court is left with a choice of either applying the same standard or adopting a separate period for electronic records. There may also be good reasons for separate retention periods, as electronic records may be more readily accessible to the public and court users.

The destruction of source (paper) documents within a short time following their conversion to a digital format is an important policy consideration. One of the great advantages of imaging systems is the savings in the access, storage and maintenance costs of paper records. The answer to this depends on the legal

authority to maintain the digital version as the official copy, as well as the retention requirement for the record, and agency capacity to maintain a digital version that is reliable and accessible for the full term of the document lifecycle.

Holds and exceptions

Disposition policies should include protocols and procedures for deferring the disposition of individual records or groups of records which may be subject to legal discovery or other circumstances that warrant their deferred disposition.

Accommodation should be made for individual records which are exempted from disposition for specific reasons. These would include records which are related to pending or expected litigation, have historical value, or for other reasons should be retained for a longer period of time than that specified for the records series.

Widespread access to court records for commercial purposes such as background checks has created a particular challenge for the courts. Without control over how long and in what format court information is made commercially available by a third party, a court may be destroying a record in compliance with the retention schedule but long before the same record disappears from the public domain. This potentially creates problems when an individual seeks to correct or update the information, for instance in the case where a criminal record is later expunged or information has been recorded in error by a third party. Many courts have continued to maintain case files or records of judgments well past their retention period for this reason.

Duplicates and non-records

Policies and procedures should be implemented to identify and eliminate duplicate and non-record material as soon as its usefulness has expired.

During the normal course of business multiple versions and copies of certain records may be created. Policies should define what records constitute the original version and identify the record owner. In addition, some of the material held by a court is not directly related to business needs. Examples of items which are typically considered non-records and therefore not included on a record retention and disposition schedule include:

- Identical copies of documents created for convenience or reference.
- Records created by staff for personal convenience.
- Blank forms and publications.

Jointly held records

The primary record-holder for records which are held jointly by the judiciary and other agencies should be identified for purpose of determining responsibility for disposition.

Certain records, such as personnel and finance records, may be maintained jointly by the judiciary and outside agencies. It will be necessary for the court to determine, in consultation with the other record holder, whether two versions should be maintained and for how long. If one copy is maintained as a reference for convenience, the reference copy should only be retained as long as needed for business purposes.

"Unstructured" records

All records created, accepted and managed by the judiciary that have business value should be adequately indexed and associated with sufficient metadata for assignment to the retention schedule.

Much of the information created and maintained by courts outside case files and records is "unstructured". Unstructured records are not maintained in a database and may have little or no metadata or labels to identify their contents. Some of these records may be created and organized by individuals with little or no guidance. Examples include documents, spreadsheets, images, and recordings which residing on network servers, PC hard drives and removable media. The value and lifecycle of these records depends to a great extent on their content and it is therefore critical that these records not be overlooked in disposition planning.

Email Management

Email classification systems should be designed to identify those items which contain business content and to assign them to the corresponding record series category in the retention schedule.

One of the significant sources of unstructured records is email. Email itself is not considered a records series or category, but rather a means of communication and transfer of information. However, email messages containing content that is related to the work of the court may be considered records.

Email management has created a new set of problems for organizations, such as determining who maintains the record copy of a message, classifying the information contained in an email, determining the appropriate retention period, and managing the sheer size and volume of email and related attachments.

Before considering how to deal with email-related information in the retention schedule, it may be necessary to develop an email classification system and accompanying policies to ensure that the disposition of email content is compliant with applicable laws and regulations.

Social networking records

The value and relevancy of social networking communications should be assessed and steps taken to classify and include those that are deemed to be official records on the retention schedule.

A relatively new demand on electronic records management and disposition is the emergence of social networking exchanges. This shift in human communication patterns, while not fully tapped in the judiciary, will no doubt contribute to the increasing volume and complexity of electronic record management in the future. Judicial record managers should be assessing the business value of social networking communication for preservation needs. As with email, the relevancy of content is key to determining the retention and disposition requirements of these records.

Exhibits and other submissions by parties

The retention and disposition of exhibits and other records submitted by litigants and other third parties should be specified in the retention schedule.

Exhibits and other documents or information submitted by parties that are not entered into the court record but are in the court's custody may need to be addressed. Common practices provide for the return of exhibits and similar records to the submitting party shortly after the conclusion of the case. Unclaimed records will generally be destroyed after a period of time and notice is given to the submitting party. Similar procedures should be taken to document the disposition of electronic evidence as is the case for other court records.

Purging documents

Retention schedules should include any approved policies or procedures for removal of documents from case files or other collections at the time of transfer to other media or record holders.

The conversion of paper records to other storage media can be a time-consuming and costly process. Generally this process occurs at one of the following points in the case file life cycle:

- final disposition or closure
- transfer to archives or inactive storage
- conclusion of a specified minimum retention period

Purging is often justified by the time saved by users in not having to search and view non-essential documents and the additional cost of scanning and storing non-critical records on digital or microfilm medium, including staff time, equipment and consumable costs. The benefits are weighed against the potential consequences and likelihood of errors of omission of important documents, how readily documents can be identified and separated from each other during the purge process, and the cost in terms of staff time to separate documents before scanning.

Generally speaking, separating critical from non-critical documents is easier when documents are scanned upon intake, eliminating the need to go back through court files and review each document for scanning. If purging can be performed at the time the file is disassembled for scanning it should take less time than having a separate step that requires court staff to purge files prior to sending them out for scanning. This requires personnel who are performing the scanning function to have the training and knowledge to make accurate decisions regarding which documents should be purged.

Conclusion

Courts have long struggled with records retention and destruction. This problem is only exacerbated by the transition to electronic records. As courts continue to migrate to a fully electronic environment, consideration of a comprehensive electronic records retention and destruction plan will be critical. Following the suggestions of this resource bulletin should provide courts with a roadmap toward developing a plan that will ensure appropriate access to court records is maintained well into the future.

Reference

Emerging Models

In 2002 the Research Libraries Group (RLG) defined the concept of a trusted digital repository as an institution created to ensure long-term access to digital resources.[22] As the most basic level a repository must maintain digital resources

[22] RLG/OCLC Working Group on Digital Archive Attributes. *Trusted Digital Repositories: Attributes and Responsibilities*. Rep. Research Libraries Group, May 2002. Web. 7 Nov. 2014.

over the long term in a consistent manner, meet or exceed standards for access, management and security, and be audited for performance and quality management. The concept has continued to evolve with the development of various models and related standards.[23] These models are described further in the following sections.

Open Archival Information System Reference Model

The Open Archival Information System (OAIS) reference model has become the de facto standard for evaluating digital repositories. In addition to the reference model, other tools have been recently developed as guides for assessing the readiness of an organization to preserve digital materials. The following schematic gives a high-level view of the OAIS model and its components:[24]

Figure 5: OAIS Model

Ingest: The steps required to transfer items from their current location into the archive in a managed manner.

Archival Storage: The storage of the bulk data (usually files) based on standard storage management tools.

Data Management: Tools to manage archival storage, including metadata.

Administration: Tools for system administration and access.

Access: Tools to search, browse and download content.

---

[23] Brown, Adrian, Shadrack Katuu, Peter Sebina, Anthea Seles, and International Records Management Trust. "Training in Electronic Records Management, Module 4: Preserving Electronic Records." 2009. Web. 7 Nov. 2014.

[24] Tilbury, Jonathan. *The Active Preservation of Digital Information* (July 2013). Web. 8 Nov. 2014.

Preservation Planning: Overall management to ensure long term access.

In addition to these fundamental characteristics, an OAIS-compliant repository should employ best practices in all areas, including:

- Standards for metadata encoding, management and records description
- Proper environmental controls for storage
- Timely and appropriate backups
- Emergency recovery, business continuity and contingency planning, and risk mitigation activities
- Adequate security features, including hierarchical password access, audit trails, firewalls, virus protection and encryption

The OAIS Reference Model has been adopted by the International Organization for Standardization as ISO 14721. Additional standards have been developed, such as ISO 16363, specify auditing criteria for certifying a trustworthy repository.

Digital Preservation Capability Preservation Model

Building on the trustworthy repository concept, authors Lori Ashley and Charles Dollar developed the Digital Preservation Capability Maturity Model.[25] This model is designed to provide a high level analysis of organizational capability for long-term digital preservation. Based on the Capability Maturity Model developed by the Software Engineering Institute of Carnegie Mellon University, the DPCMM defines seven components that are critical to a sustained effort to preserve electronic records:

- Digital preservation policy
- Digital preservation strategy
- Governance
- Collaboration
- Technical expertise
- Open standard/technology neutral formats
- Designated community

The model further defines eight components that are required to sustain an electronic record repository. The model includes five levels of capability or maturity as a metric to assess current program capability, identify gaps, and

[25] Dollar, Charles M., and Lori J. Ashley. "Assessing Digital Preservation Capability Using a Maturity Model Process Improvement Approach." Feb. 2013. Web. 7 Nov. 2014.

create a roadmap to achieve a higher level of organizational competency. The maturity model was updated in April 2014.

Levels of Digital Preservation Framework

The National Digital Stewardship Alliance (NDSA) has also developed a set of recommendations to guide organizations in the development of digital preservations systems and activities. NDSA is described as a group of "over 140 organizations whose mission is to establish, maintain, and advance the capacity to preserve our nation's digital resources for the benefit of present and future generations."[26]

The Levels of Digital Preservation framework defines five functional areas required for effective digital preservation:

1. Storage and geographic location
2. File fixity and data integrity
3. Information security
4. Metadata
5. File formats

Similar to the DPCMM, the Levels of Digital Preservation framework includes four tiers or levels of compliance in each of these areas, with the goal of providing a tool to evaluate capacity to mitigate risk of information loss and identify technical steps that can be taken to improve preservation.

Applicable Standards

The following are examples of records management standards that have application to records preservation. This list is by no means exhaustive and it should be noted that standards are being continually updated with the emergence of new technologies and best practices.[27]

Digital Document Management

ISO 19005-1:2005 *Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)* – specifies how to

[26] Phillips, Meg, Jefferson Bailey, Andrea Goethals, and Trevor Owens. *The NDSA Levels of Digital Preservation: An Explanation and Uses*. Working paper. Library of Congress, NSDA Infrastructure Working Group, n.d. Web. 05 Nov. 2014.

[27] Jones, Virginia, "Standards for Establishing Records and Information Management Programs," *Information Management*, July – August 2012, p.38.

use the portable document format (PDF) 1.4 for long-term preservation of electronic documents.

NIST SP 500-252 *Care and Handling of CDs and DVDs – A Guide for Librarians and Archivists* – provides guidance on how to maximize the lifetime and usefulness of optical discs, specifically CD and DVD media, by minimizing chances of information loss caused by environmental influences or physical handling.[28]

ISO 13008:2012 *Information and documentation – Digital records conversion and migration process* –provides guidance in understanding recordkeeping requirements, the organizational and business framework for conducting the conversion and migration process, technology planning issues, and monitoring/controls for the process. *[Supersedes ANSI/ARMA 16-2007 The Digital Records Conversion Process.]*

ISO/TR 13028:2010 *Information and documentation – Implementation guidelines for digitization of records* –establishes guidelines for creating and maintaining records in digital format only and establishes best practice guidelines for digitization to ensure the trustworthiness and reliability of records.

ISO/TR 15801:2009 *Document management – Information stored electronically – Recommendations for trustworthiness and reliability* – describes the implementation and operation of document management systems that can be considered to store electronic information in a trustworthy and reliable manner.

Indexing and Metadata

Controlled Language in Records and Information Management (ARMA International) – describes what controlled language is and how it benefits organizations by reducing search time and increasing the reliability of search results, improving organizational communication, avoiding duplication, and reducing corporate risk exposure in legal and other discovery processes.

ISO 23081-1:2006 *Information and documentation – Records management processes – Metadata for records – Part 1: Principles* – covers the principles that underpin and govern records management metadata.

---

[28] Byers, Fred R., and Chris Keithley. *Care and Handling of CDs and DVDs — A Guide for Librarians and Archivists*. Washington, CD: US Dept. of Commerce, 2003. NIST Information Technology Laboratory. National Institute of Standards and Technology and Council on Library and Information Resources, Oct. 2003. Web. 17 Nov. 2014.NIST Special Publication 500-252

ISO 23081-2:2009 *Information and documentation – Managing metadata for records – Part 2: Conceptual and implementation issues* – establishes a framework for defining metadata elements consistent with the principles and implementation considerations outlined in ISO 23081-1:2006.

Facilities and Storage

ARMA TR01-2011 *Records Center Operations, 3rd Ed.* – assists organizations with selecting an appropriate records center site and designing, equipping, staffing, operating, and managing a records center. Additional sections discuss vaults, security, records center software, and commercial records storage facilities.

Guideline for Evaluating Offsite Records Storage Facilities (ARMA International) – assists organizations with evaluating storage needs, determining whether business practices make outsourcing the best decision, and assessing the ability of vendors to meet storage requirements.

Guideline for Outsourcing Electronic Records Storage and Disposition (ARMA International) – provides information to assist organizations in making decisions about outsourcing electronic records storage, retrieval, disposition to third-party providers and evaluating and selecting a service provider.

Guideline for Outsourcing Electronic Records Storage to the Cloud (ARMA International) – addresses information management issues related to cloud-based records storage, including benefits and risks of using cloud-based records storage, how to mitigate legal risks, issues related to retention, disposition, privacy, and security, standards and best practices, and vendor selection.

Vital Records and Risk Mitigation

ANSI/ARMA 5-2010 *Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records* – sets the requirements for establishing a vital records program including requirements for: identifying and protecting vital records, assessing and analyzing their vulnerability, and determining the impact of their loss on the organization.

Guideline for Evaluating and Mitigating Records and Information Risks (ARMA International) – provides a framework for establishing systems to evaluate information risks and describes a process for framing a risk management system using a risk quadrant of administrative risks, records control risks, legal/regulatory risks, and technology risks.

ISO/IEC 27002: 2005 *Information Technology – Security techniques – Code of Practice for Information Security* – establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It outlines objectives that provide general guidance on the commonly accepted goals of information security management. *[Formerly ISO 17799:2005.]*