

Supreme Court of Florida

No. AOSC10-17

IN RE: STANDARDS FOR ELECTRONIC RECORDKEEPING SYSTEMS

ADMINISTRATIVE ORDER

The Judicial Branch Records Management Committee was charged with recommending standards for electronic recordkeeping systems for permanently recorded court records, as referenced in rule 2.430(a)(3), Florida Rules of Judicial Administration. In Re: Judicial Branch Records Management and Retention Program, No. AOSC08-5 (Dec. 15, 2008). In light of the judicial branch's rapid progress toward electronic filing in the trial and appellate courts and implementation of a statewide electronic filing portal, the committee concluded that electronic recordkeeping standards are needed for all court and administrative records of the judicial branch, whether temporarily maintained or permanently recorded. The committee therefore submitted comprehensive standards for electronic recordkeeping systems applicable to all records of the judicial branch. We approve the Judicial Branch Standards for Electronic Recordkeeping Systems

as an administrative matter to facilitate timely modifications that may be required in the future due to evolving technology.

Rules 2.430 and 2.440, Florida Rules of Judicial Administration, govern the retention and disposition of court and administrative records. Rule 2.430(2)(a) defines “permanently recorded” records as those that have been “microfilmed, optically imaged or recorded onto an electronic recordkeeping system in accordance with standards adopted by the Supreme Court of Florida.” The reference to standards for electronic recordkeeping systems “adopted by the Supreme Court” was added to rule 2.430 in 2008 in In Re: Amendments to Florida Rules of Judicial Administration 2.430, 973 So. 2d 437 (Fla. 2008) in recognition of the Court’s decision in 2004 to make the judicial branch fully responsible for maintenance of its own records. See In Re: Judicial Branch Records Management Workgroup, No. AOSC04-1 (Jan. 6, 2004). The Court in 2008 also deleted reference in rule 2.430 to the Department of State Division of Libraries and Information Services’ oversight responsibilities for disposition of court records. In Re: Amendments to Florida Rules of Judicial Administration 2.430. These amendments were consistent with language contained in rule 2.525(a), Electronic Filing, Definitions, Florida Rules of Judicial Administration, providing that a court’s electronic recordkeeping system used in connection with the electronic filing of documents must be “authorized by the Supreme Court of Florida.”

As court and administrative records increasingly originate in electronic form, and existing paper records are digitized, the Court must ensure that electronic recordkeeping systems will be accessible now and in the future, will properly preserve records in accordance with applicable retention schedules, and will keep records secure. In developing standards for electronic recordkeeping systems, the committee adapted standards adopted by the Department of State Division of Library and Information Services in rule 1B-26.003, Florida Administrative Code, Records Management – Standards and Requirements – Electronic Recordkeeping for use in the judicial branch. Because these standards were in effect and applicable to clerk of circuit court electronic recordkeeping systems prior to 2008, when the Court through rule 2.430 amendments assumed authority over maintenance and disposition of judicial branch records, it is anticipated that very few, if any, new recordkeeping system requirements will be imposed on clerks of circuit court, in their capacity as records management officers for trial court records, as a result of the Court’s adoption of the standards.¹

¹ In In Re: Judicial Branch Records Management and Retention Program, No. AOSC08-5 (Dec. 15, 2008), the Court required each trial and appellate court to appoint records management officers for court and administrative records. The chief judge of each trial and appellate court was required to designate a records management officer for administrative records of the court, and to designate the clerk of court, or his or her designee, as the records management officer for court records

The standards establish minimum requirements for the creation, utilization, maintenance, retention, preservation, storage and disposition of electronic records that are permanently recorded or stored either temporarily or for the long term. The standards must be incorporated, to the extent possible without disrupting existing recordkeeping practices, into the system design and implementation of any new recordkeeping systems, and enhancements to existing systems. The standards apply to all electronic recordkeeping systems, including microcomputers, minicomputers, mainframe computers, and image recording systems in network or stand alone configurations.

Each records management officer for court and administrative records shall comply with these standards by developing and implementing a program for the management of electronic records. Such programs must ensure that maintenance of electronic records complies with retention schedules for court and administrative records and the public access requirements contained in Article V, section 24(a), Florida Constitution, as implemented by rule 2.420, Florida Rules of Judicial Administration.

The standards for electronic recordkeeping systems are appended to this order and are effective immediately. The custodians of court and administrative records shall certify annually that they are in compliance with the standards. The

Florida Courts Technology Commission is authorized to oversee compliance with the standards.

DONE AND ORDERED at Tallahassee, Florida, on May 4, 2010.



Chief Justice Peggy A. Quince

ATTEST:



Thomas D. Hall
Clerk, Supreme Court



JUDICIAL BRANCH STANDARDS FOR ELECTRONIC RECORDKEEPING SYSTEMS

(1) PURPOSE. The following are standards for judicial branch_court and administrative_records that reside in electronic recordkeeping systems. These standards apply to permanently recorded, long term and temporarily stored records. These standards must be incorporated into the system design and implementation of new recordkeeping_systems and enhancements to existing systems.

(2) SCOPE.

- (a)1. These standards are applicable to all entities of the judicial branch.
 - 2. These standards establish minimum requirements for the creation, utilization, maintenance, retention, preservation, storage, and disposition of electronic records that are permanently recorded, long term or temporarily stored, regardless of the media.
 - 3. Electronic records include numeric, graphic, audio, video, and textual information that is recorded or transmitted in analog or digital form.
 - 4. These standards apply to all electronic recordkeeping systems, including, but not limited to, microcomputers, minicomputers, mainframe computers, and image recording systems (regardless of storage media) in network or stand-alone configurations.
- (b) Before existing records are committed to an electronic recordkeeping system, a cost benefit analysis must be conducted by the relevant judicial branch entity to ensure that the project or system contemplated is cost effective.

(3) INTENT. Electronic recordkeeping systems in use on the effective date of these standards that are not in compliance with these standards may be used until the systems are replaced or upgraded. New and upgraded electronic recordkeeping systems created after the effective date of these standards must comply with the requirements contained herein. The Supreme Court of Florida is aware that it may not be possible to implement these standards in their entirety immediately upon adoption, and it is not the intent by these standards to disrupt existing recordkeeping practices. These standards are promulgated and enforced solely by the Supreme Court of Florida for the judicial branch. No rights, liabilities, or causes of action at law or equity are created by these standards.

(4) DEFINITIONS. For the purpose of these standards:

- (a) "ASCII" means the American Standard Code for Information Interchange, a 7-bit coded character set for information interchange which was formerly American National Standards Institute (ANSI) Standard X3.4

and has since been incorporated into the Unicode standard as the first 128 Unicode characters.

(b) “Database” means an organized collection of automated information.

(c) “Database management system” means a set of software programs that controls the organization, storage, and retrieval of data (fields, records, and files) in a database. It also controls the security and integrity of the database.

(d) “Digital signature” means a type of electronic signature (any letters, characters, or symbols executed with an intent to authenticate) that can be used to authenticate the identity of the sender of a message or the signer of a document and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures can be created through hashing algorithms.

(e) “Electronic record” means any record that is recorded in machine readable form.

(f) “Electronic recordkeeping system” means an automated information system for the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures.

(g) “Hashing algorithm” (hash function, checksum) means a formula or procedure for checking that electronically transmitted messages or documents have not been altered by transforming a string of characters into a usually shorter fixed-length “hash value” or key that represents the original string. The receiver of the message can execute the same hashing algorithm as the sender and compare the resulting hash values; any difference in the hash values indicates an alteration of the message or document sent. Hashing algorithms can be used to create digital signatures.

(h) “Judicial branch” means the judicial branch of government, which includes the state court system, the clerk of court when acting as an arm of the court, The Florida Bar, the Florida Board of Bar Examiners, the Judicial Qualifications Commission, and all other entities established by or operating under the authority of the supreme court or the chief justice.

(i) “System design” means the design of the nature and content of input, files, procedures, and output and their interrelationships.

(j) “Permanent or long-term records” means any records that have an established retention period of more than 10 years.

(k) “Geographic information system” means a computer system for capturing, storing, checking, integrating, manipulating, analyzing, and displaying data related to positions on the Earth’s surface.

(l) “Open format” means a data format that is defined in complete detail, allows transformation of the data to other formats without loss of

information, and is open and available to the public free of legal restrictions on use. An open format may be either standards-based or proprietary.

(m) “Unicode” means the universal character encoding standard maintained by the Unicode Consortium, providing the basis for processing, storage, and interchange of text data in any language in all modern software and information technology protocols.

(5) DUTIES AND RESPONSIBILITIES. Each entity of the judicial branch shall:

- (a) Develop and implement a program for the management of electronic records;
- (b) Ensure that maintenance of all records complies with retention schedules for court and administrative records;
- (c) Integrate the management of electronic records with other records and information resources management programs of the court;
- (d) Incorporate electronic records management objectives, responsibilities, and authorities in pertinent court directives, or rules, as applicable;
- (e) Establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving, recommending, adopting, or implementing new electronic recordkeeping systems or enhancements to existing systems;
- (f) Provide training for users of electronic recordkeeping systems in the operation, care, and handling of the equipment, software, and media used in the system; and
- (g) Ensure that electronic recordkeeping systems meet requirements for public access to records in accordance with Article 1, Section 24, Florida Constitution, and Florida Rule of Judicial Administration 2.420 and the following standards:

1. In accordance with rule 2.420(f)(2), Florida Rules of Judicial Administration, custodians of court and administrative records may determine the format in which records are provided, upon request. Each entity of the judicial branch that maintains records in an electronic recordkeeping system may provide to any person making a public records request pursuant to Article 1, Section 24, Florida Constitution, as implemented by rule 2.420, a copy of such records that are not confidential or exempt from disclosure.
2. Except as otherwise provided by law, no entity of the judicial branch shall enter into a contract with, or otherwise obligate itself to, any person or entity for electronic recordkeeping hardware, software, systems, or services if such contract or obligation impairs the right of

the public under applicable law to inspect or copy nonexempt public records, or impairs the ability to retain the records in accordance with the applicable retention schedules.

3. In providing access to electronic records, entities of the judicial branch shall ensure that procedures and controls are in place to protect information that is confidential or exempt from public disclosure.

(6) DOCUMENTATION. Records Management Officers for Court and Administrative Records shall develop and maintain adequate and up-to-date technical and descriptive documentation for each electronic recordkeeping system to specify characteristics necessary for reading or processing the records. Documentation for electronic records systems shall be maintained in electronic or printed form as necessary to ensure access to the records. The minimum documentation required is:

- (a) A narrative description of the system, including all inputs and outputs of the system; the organization and contents of the files and records; policies on access and use; security controls; purpose and function of the system; update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and the location and media in which electronic records are maintained and their retention requirements to ensure appropriate disposition of records in accordance with rules 2.430 and 2.440, Florida Rule of Judicial Administration;
- (b) The physical and technical characteristics of the records, including a record layout or markup language that describes each file or field including its name, size, starting or relative position, and description of the form of the data (such as alphabetic, decimal, or numeric), or a data dictionary or the equivalent information associated with a database management system including a description of the relationship between data elements in databases;
- (c) For information coming from geographic information systems, the physical and technical characteristics of the records must be described, including a data dictionary, a quality and accuracy report and a description of the graphic data structure, such as recommended by the federal Spatial Data Transfer Standards; and
- (d) Any other technical information needed to read or process the records.

(7) CREATION AND USE OF ELECTRONIC RECORDS.

(a) Electronic recordkeeping systems that maintain records on electronic media shall meet the following minimum requirements:

1. Provide a method for all authorized users of the system to retrieve desired records;
 2. Provide an appropriate level of security to ensure the integrity of the records, in accordance with the requirements of chapter 282, F.S. Security controls should include, at a minimum, physical and logical access controls, backup and recovery procedures, and training for custodians and users. Automated methods for integrity checking should be incorporated in all systems that generate and use official file copies of records. Hashing algorithms and digital signatures should be considered for all official file copies of electronic records. The use of automated integrity controls, such as hashing algorithms and digital signatures, can reduce the need for other security controls. Hashing algorithms used to protect the integrity of official file copies of records should meet the requirements of U.S. Federal Information Processing Standard Publication 180-2 (FIPS-PUB 180-2) (August 1, 2002) entitled “Secure Hash Standard” (or “Secure Hash Signature Standard”), which is hereby incorporated by reference, and made a part of these standards. This publication is available from the National Technical Information Service (NTIS), 5285 Port Royal Road, U.S. Department of Commerce, Springfield, VA 22161, and at the Internet Uniform Resource Locator: <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>. Courts utilizing hashing algorithms shall only use validated implementations of hashing algorithms;
 3. Identify the open format or standard interchange format when necessary to permit the exchange of records on electronic media between judicial branch electronic recordkeeping systems using different software and operating systems and the conversion or migration of records on electronic media from one system to another. For text records in the absence of other conversion capabilities, the word processing or text creation system should be able to import and export files in the ASCII or Unicode format as prescribed by the Unicode 5.0 Standard (or successor Unicode Standard), which is hereby incorporated by reference, and made a part of these standards. This publication is available from the Unicode Consortium, P. O. Box 391476, Mountain View, CA 94039-1476, and at the Internet Uniform Resource Locator: <http://www.unicode.org/book/bookform.html>; and
 4. Provide for the disposition of the records.
- (b) Before a permanently recorded or temporarily stored record is created on an electronic recordkeeping system, the record shall be uniquely identified to enable authorized personnel to retrieve, protect, and carry out the disposition of records in the system. Records Management Officers for Court and Administrative Records

shall ensure that records maintained in such systems can be correlated with any existing related records on paper, microfilm, or other non-electronic media.

(8) LEGAL AUTHENTICATION. Records Management Officers for Court and Administrative Records shall implement the following procedures to enhance the legal admissibility of electronic records:

- (a) Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach;
- (b) Substantiate that security procedures prevent unauthorized addition, modification, or deletion of a record and ensure systems are protected against such problems as power interruptions;
- (c) Identify the electronic media on which records are stored throughout the required retention period, the maximum time span that records remain on each storage media, and the official retention requirements for the records adopted by the Supreme Court of Florida; and
- (d) Establish and maintain integrity controls for electronic records.

(9) STANDARDS FOR SELECTION OF ELECTRONIC RECORDS STORAGE MEDIA. For storing electronic records throughout the required retention period, Records Management Officers for Court and Administrative Records shall select appropriate media and systems which meet the following requirements:

- (a) Permit easy and accurate retrieval in a timely fashion;
- (b) Retain the records in a usable format until their authorized disposition;
- (c) Floppy disks, audio cassettes, or VHS-format video cassettes shall not be used for the storage of permanent or long-term records. Permanent or long-term records on magnetic tape shall be stored on polyester-based media. Only previously unrecorded audio or video tape shall be used for permanent or long-term audio or video recordings;
- (d) A scanning density with a minimum of 300 dots per inch is required for scanned images from hard copy permanent or long-term records;
- (e) Scanned images from hard copy permanent or long-term records must be stored in accordance with a published International Organization for Standardization (ISO) open standard image format;
- (f) These standards also should be applied to temporarily stored records, as feasible;
- (g) The following factors are to be considered before selecting a storage media or converting from one media to another:

1. The authorized retention of the records as determined during the scheduling process;
2. The maintenance necessary to retain the records;
3. The cost of storing and retrieving the records;
4. The access time to retrieve stored records;
5. The portability of the medium (that is, selecting a medium that can be read by equipment offered by multiple manufacturers); and
6. The ability to transfer the information from one medium to another, such as from optical disk to magnetic tape.

(10) STANDARDS FOR MAINTENANCE OF ELECTRONIC RECORDS.

(a) Electronic records shall be backed up on a regular basis to safeguard against the loss of information due to equipment malfunctions, human error, or other disaster. Backup electronic recording media created for disaster recovery purposes, and all preservation duplicates of permanent or long-term records, shall be maintained in an off-site storage facility with constant temperature (below 68 degrees Fahrenheit and relative humidity 20 to 30 percent) controls. Storage and handling of permanent or long-term records on magnetic tape shall conform to the standards contained in Standard AES22-1997 (r2003). “AES recommended practice for audio preservation and restoration – Storage and handling – Storage of polyester-base magnetic tape” (published 1997, reaffirmed 2003), which is hereby incorporated by reference and made a part of these standards. This publication is available from the Audio Engineering Society, Incorporated, 60 East 42nd Street, Room 2520, New York, New York, 10165-2520, and at the Internet Uniform Resource Locator: <http://www.aes.org/publications/standards/search.cfm>. If a judicial branch entity cannot practicably maintain backups and preservation duplicates as required in this section, the entity shall document the reasons why it cannot do so. Other temporarily stored electronic records media should be stored in a cool, dry, dark environment when possible (maximum temperature 73 degrees Fahrenheit, relative humidity 20-50 percent).

(b) A statistical sample of all electronic media containing permanent or long-term records shall be read annually to identify any loss of information and to discover and correct the cause of data loss.

(c) All permanent or long-term electronic records shall be tested at least every ten years and verified that the media are free of permanent errors. More frequent testing (e.g., at least every five years) is highly recommended.

(d) Tapes shall only be rewound immediately before use to restore proper tension. When tapes with extreme cases of degradation are discovered, they

should be rewound to avoid more permanent damage and copied to new media as soon as possible. Tapes shall be played continuously from end to end to ensure even packing. Tapes shall be stored so that the tape is all on one reel or hub.

(e) Smoking, eating, and drinking shall be prohibited in areas where electronic records are created, stored, used, or tested.

(f) External labels, or the equivalent automated management system for electronic recording media used to store records, shall provide unique identification for each storage media, including:

1. The name of the organizational unit responsible for the data;
2. System title, including the version number of the application;
3. Special security requirements or restrictions on access, if any; and
4. Software in use at the time of creation.

(g) For all media used to store electronic records, human-readable information specifying recording methods, formats, languages, dependencies, and schema sufficient to ensure continued access to, and intellectual control over, the records shall be maintained. Additionally, the following information shall be maintained for each media used to store electronic records:

1. File title;
2. Dates of creation;
3. Dates of coverage; and
4. Character code/software dependency.

(h) Electronic records shall not be stored closer than two meters (about six feet, seven inches) from sources of magnetic fields, including generators, elevators, transformers, loudspeakers, microphones, headphones, magnetic cabinet latches, and magnetized tools.

(i) Electronic records on magnetic tape or disk shall not be stored in metal containers unless the metal is non-magnetic. Storage containers shall be resistant to impact, dust intrusion and moisture. Compact disks shall be stored in hard cases, and not in cardboard, paper, or flimsy sleeves.

(j) Records Management Officers for Court and Administrative Records shall ensure that electronic records are maintained by personnel properly trained in the use and handling of the records and associated equipment.

(k) Records Management Officers for Court and Administrative Records shall establish and adopt procedures for external labeling of the contents of diskettes, disks, tapes, or optical disks so that all authorized users can identify and retrieve the stored information.

(l) Records Management Officers for Court and Administrative Records shall convert storage media to provide compatibility with the current

hardware and software used to ensure that information is not lost due to changing technology or deterioration of storage media. Before conversion of information to different media, Records Management Officers for Court and Administrative Records must determine that authorized disposition of the electronic records can be implemented after conversion. Permanent, long-term and temporarily stored electronic records stored on magnetic tape shall be transferred to new media as needed to prevent loss of information due to changing technology or deterioration of storage media.

(11) STANDARDS FOR RETENTION OF ELECTRONIC RECORDS. Each Records Management Officer for Court and Administrative Records is responsible for ensuring the continued accessibility and readability of public records throughout the required retention period regardless of the format or media in which the records are maintained. Policies and procedures shall be established to ensure that electronic records and their documentation are retained and accessible as long as required. These procedures shall include provisions for:

- (a) Scheduling the retention and disposition of all electronic records, as well as related access documentation and indexes, in accordance with rules 2.430 and 2.440, Florida Rules of Judicial Administration; and
- (b) Establishing procedures for regular recopying, reformatting, and other necessary maintenance to ensure the retention and usability of the electronic records throughout their authorized life cycle.

(12) DESTRUCTION OF ELECTRONIC RECORDS. Electronic records may be destroyed only in accordance with the retention schedules applicable to court and administrative records. At a minimum, each Records Management Officer for Court and Administrative Records shall ensure that:

- (a) Electronic records scheduled for destruction are disposed of in a manner that ensures that any information that is confidential or exempt from disclosure, including proprietary or security information, cannot practicably be read or reconstructed; and
- (b) Recording media previously used for electronic records containing information that is confidential or exempt from disclosure, including proprietary or security information, are not reused if the previously recorded information can be compromised in any way by reuse.