FCTC
Action Summary
February 2018

- FCTC approved a motion from the Portal Subcommittee for second reading: Motion to recommend the Portal, for those documents not filed as PDF/A, begin the process to ultimately convert received documents to PDF/A, understanding that the Portal will continue to provide the documents to each individual clerk in the format that the clerk can process. In support of this process, the Portal will notify and provide educational opportunities to the filers as to the requirement of filing documents in PDF/A format.

- FCTC approved a motion from the Joint RJA Workgroup for second reading: Motion to refer and recommend to the Florida Rules of Judicial Administration Committee consideration of amendments to the court records retention rule – rule 2.430 – to:

    - Clarify the retention schedule for electronic court records, which have been Permanently Recorded;
    - Require that prospective court records that have been Permanently Recorded be retained in the format, PDF/A; and,
    - Consider and include a date by which Permanently Recorded court records shall be maintained in the format, PDF/A.

  Additionally, recommend the creation of a Florida Courts Technology Standard that would provide guidance and technical information on the retention and storage of Permanently Recorded court records under amended rule 2.420.

- FCTC approved a motion from the Technical Standards Subcommittee for first reading: Motion to recommend that the court work with the clerks and FCCC so the record copy will be a PDF/A document which will retain the original intelligence. The redacted copy will not be required to maintain the original intelligence. The clerks will need to follow acceptable ADA requirements with on demand redacted documents.

- FCTC approved a motion from the Technical Standards Subcommittee for first reading: Motion to recommend a two-year timeframe for clerks to implement PDF/A storage of court documents after the Supreme Court approval of technical standards. Clerks may request an extension for good cause to the Supreme Court.

- FCTC approved a motion from the Technical Standards Subcommittee for first reading: Motion to recommend that digital signatures and electronic notarization (or anything with a digital hash) are not required. However, if they are included in the PDF, the signatures will be flattened. The technology to maintain those processes will not be required.

- FCTC approved a motion from the Access Governance Board for the FCTC to make a recommendation to the Supreme Court that Brevard County move its online electronic records access system from the pilot phase into production and to discontinue the submission of monthly progress reports be approved. Within 90 days from the Court's approval, the clerk must implement their access system in accordance with AOSC17-47.

- FCTC approved the following three motions from the Access Governance Board on first reading and waiver of second reading without objection:

    - Motion to accept the proposed changes to the Standards for Access to Electronic Court Records as amended at the Access Governance Board's February 8, 2018 meeting.
        - Remove the following sentence from the Redaction section: "The default view for judges is the non-redacted version of the record."
        - Update the following sentence in the Performance section: "Search capability, if available, will be limited to such requested document and must not support automated bulk search~~es requests~~.

    - Motion to modify the Access Security Matrix to include updating the User Roles to align with the User Roles identified in the Standards for Access to Electronic Court Records; adding Professional Guardian to the Guardianship Miscellaneous cases type; adding Mental Health Miscellaneous to the Baker Act case type; deleting Emergency Admission from the Substance Abuse case type and adding Assessment/Treatment; adding Tuberculosis/STD Treatment/Other Confidential case type, all with appropriate rules and statutes; and removing Substance Abuse cases filed pre 10-1-2010 disabled case type from the matrix.

    - Motion to request the FCTC expedite the approval of the changes to the Standards for Access to Electronic Court Records and the Access Security Matrix and forego the need for a second reading.

- FCTC approved a motion on second reading: Motion that the Clerks of Court, in consultation with the Court, develop technical and functional standards for their case maintenance systems to assure that such systems meet the needs of the clerks of the court, the Bar, and other court partners.

- FCTC approved a motion from the Technical Standards Subcommittee for first reading: Motion to recommend approval of the Backup of Electronic Records language.

Backup of Electronic Records

Electronic court records custodians are responsible for the security, availability, and integrity of electronic court records (images and data) under their care. Custodians shall ensure that:

- Electronic court records in their care are securely backed-up and any backup data stored at a third party location must also be encrypted. The custodian of the electronic court records shall have exclusive access to the encryption key. In instances where vendors are supporting appliances onsite and are required to maintain an encryption key, the custodian will have operational policies and procedures that serve as a control prohibiting vendor access without invitation and monitoring.
- The production data or backup copy will reside in a hardened (CAT 5) facility. If a hardened (CAT 5) facility is unavailable, a tertiary copy (redundant backup) will also be maintained in its own off site, independent facility. The production electronic court records and at least one copy of the backup(s) shall not be housed in the same building.
- Agreements with third party offsite vendors acknowledge the confidentiality of electronic court data they store, and prohibit data mining and other access/use of the data for any purpose other than to make the data accessible to the custodian.
- All backup copies of court data must be readily available to the custodian for access and restoration.
- Random sample testing is performed annually to verify that data is accessible and recoverable.
- Any known breach, or other malicious event, is reported to the chief judge or his/her designee and the Chief Information Security Officer at the Office of the State Courts Administrator Office of Information Technology as part of the custodian's Computer Security Incident Response plan.
- All court backup data is stored in the United States.
- Physical and electronic data transfer processes conform to the confidentiality and security guidelines set forth in the Data Exchange Standards.

These standards are minimum standards. If a custodian stores court-related data from another jurisdiction or agency with stricter requirements, the custodian must comply with the stricter standards for that data.