

Considerations when Converting to a Paperless Law Office

As a growing number of lawyers incorporate new technology into their law practices, many firms are going paperless to reduce clutter and improve file access and organization. Missouri lawyers are permitted to adopt a paperless law firm model so long as certain considerations are made prior to the destruction of the original file.

Digitizing files allows for an attorney to instantly access a client's file from his or her desktop. Prior to integrating a paperless system, law firms must assess their current system and create a plan for implementing the new system. Careful consideration must be taken to establish uniform procedures that will protect the integrity and confidentiality of the client file.

Law firms that wish to transition to a paperless model should consider the following issues:

I. Ethical Requirements

A. Missouri permits conversion of paper file to electronic file

1. See Formal Opinion 127, Advisory Committee of the Supreme Court of Missouri
2. Firm is not required to obtain client consent prior to conversion
3. Certain issues must be addressed:
 - a. Ensure the electronic storage media has integrity for the period the file must be stored
 - b. Ensure that hardware and software necessary to access the data will be available during the storage period.
 - c. Determine how the file be provided to client
 - d. Do not destroy items of intrinsic value
 - e. Encourages firms to offer the paper file for the client prior to destruction.
4. In Missouri, the file belongs to the client from cover to cover
 - a. See Formal Opinion 115, Advisory Committee of the Supreme Court of Missouri

B. Safekeeping property rule applies to electronic files

1. See M.R.P.C. 4-1.15(m) Safekeeping Property
 - a. A lawyer must securely store a client's file for 10 years from the last date of representation absent other arrangements between the lawyer and client.

C. Attorney must safeguard client information after representation concludes

1. See M.R.P.C. 4-1.9 Duties to Former Clients
- D.** Upon termination of representation, lawyer should promptly deliver to the client any property that the client is entitled to receive
1. See Rule 4-1.16(d) Declining or Terminating Representation

II. Create a Plan of Action for Going Paperless

A. Assess Law Firm's Current Paper System

1. Consider the types of documents generated/received in your office
 - a. Paper documents
 - i. letters, pleadings, discovery, evidence, faxes
 - b. Electronic documents
 - i. Emails, pdf attachments, Microsoft Word documents, jpeg pictures, electronic court filings and orders, etc.
2. Assess firm's current procedure for processing inbound/outbound documents
 - a. Filing in storage cabinets or file rooms
 - b. Case management system

B. What is the scope of your future Paperless System?

1. Determine which documents will be converted and stored in electronic format
 - a. Inbound and outbound documents
 - i. Emails, letters, court filings, client documents, billing, discovery, intake forms, faxes
 - ii. Notes from meetings
 - b. How will existing open files be handled?
 - i. Back scan all open files into paperless system or
 - ii. Retain open files in paper form
 - i. Scan new documents into paperless system
 - c. How will firm handle closed files?
2. Determine which documents cannot be converted to electronic format?
 - a. Items of intrinsic value
 - i. Original deeds, wills, certificates, etc.
3. Determine which documents will not be converted for practical reasons
 - a. Older files outside of the 10-year file retention rule
 - b. Large documents
 - c. Certain confidential documents

4. Who is responsible for creating the digital documents?
5. How will documents be organized?
 - a. Nomenclature for each digital document
6. Where will the documents be stored in the digital system?
 - a. How will documents be retrieved?
7. If more than one office, how will remote access be handled?
8. Do you desire the ability to select and export a file to CD-rom?
9. Will the paperless system be integrated with current risk management procedures?
 - a. i.e., conflict of interest checking system, calendaring systems, case management procedures
10. Will system allow for integrated faxing ?
 - a. receive inbound files for indexing
11. Does the paperless procedure allow user to create annotations?
 - a. both permanent and temporary "Post-It" notes
12. Does paperless system allow user to check-out document for editing, while preserving the originals?

C. Hardware and Software requirements for a paperless office

1. Hardware Requirements
 - a. Computers
 - b. Scanners
 - i. Centralized for office use
 - ii. Desktop scanners for individual use
 - c. In-house Data storage
 - i. Data must be accessible
 - d. Backup systems
 - i. Off-site
 - e. Online Data Storage
 - i. Cloud computing services
 - ii. SaaS (Software as a Service)

2. Software Requirements
 - a. Microsoft Outlook or comparable email/calendaring system
 - b. Word Processing Program
 - c. Document management system
 - d. Case management system
 - e. Document sharing protection
 - i. Metadata scrubbing program
 - ii. Encryption
 - f. PDF by Adobe, Inc. conversion software

3. Ensure that all software programs are compatible with each other

D. Assess staff capabilities and office procedures

1. Create a training plan
 - a. Determine which staff members will be responsible for scanning tasks
 - b. Who will train staff members on these procedures?
 - i. Will training be ongoing?
 - ii. Appoint an individual to supervise staff using the new system

2. Establish written procedures and controls for staff to follow
 - a. Create a procedures checklist
 - i. Document Scanning
 - i. Upon receipt or at a later date?
 - ii. How will documents be date stamped?
 - ii. Destruction of Documents
 - i. When will destruction occur?
 1. After scanning?
 2. After Attorney approves destruction?
 - ii. How will documents be destroyed?
 1. Shredding
 2. Return documents to client
 - b. Create Procedures for Protecting Confidential Information
 - i. Clearly label confidential information
 - ii. Protect from inadvertent disclosure to 3rd parties
 - i. Avoid unintended recipients/reply all

3. Adopt Internal Controls
 - a. Convert final documents to PDF format to avoid edits by 3rd parties
 - b. Require employees to sign confidentiality acknowledgements

4. Adopt Controls for Mobile information
 - a. Protect data stored on smart phones
 - i. Remote locking of data if device is lost
 - b. Laptop security
 - c. Assess USB/flash drive portability risks

III. Risk Management Considerations

A. Implement Consistent Procedures

1. inconsistent procedures may result in lost documents and increased malpractice risk

B. File Security

1. Protect file information from outside threats
2. Security at all storage levels
3. Create Secure Passwords
4. Cloud Computing protection
 - a. Ask for a service level agreement detailing the vendor's obligations
 - b. Ensure the service encrypts all data
 - c. Review terms of service carefully

C. File Retention

1. How long will the firm maintain the electronic file?
2. If the file will be retained for less than 10 years from the date of conclusion, obtain client's written acknowledgement of firm's file retention policy

D. File Destruction

1. To avoid disputes, consider consulting with the client prior to file destruction
2. Maintain all items of intrinsic value
3. Destroy file in a manner that maintains confidentiality

E. Production of the File Upon Client's Request

1. If the client requests the file, lawyer must provide it to the client in a manner in which the client will be able to access it using commonly used, relatively inexpensive software and hardware
 - a. If client is unable to access file due to a lack of technological knowledge or access to a computer, attorney may need to provide file in paper format
2. During or after the representation, lawyer must provide the file to the client without charge, except for shipping or delivery charges.

- a. See Formal Opinion 127, Advisory Committee of the Supreme Court of Missouri

F. Inform the Client of the Firm's Policy at the Outset of Representation

1. Explain document conversion, retention, and destruction policy
 - a. Include policy in the engagement letter or fee agreement
2. Allow client the opportunity to ask questions

G. Metadata

1. Data buried within a computer generated document
 - a. Although not visible on the face of the document, it is easily accessible by recipient
 - b. May include: dates of file creation, modifications, comments, prior revisions, identity of file author
 - c. May be found within any computer generated document
2. Protect document by scrubbing metadata or converting the document to PDF format

H. Backup Issues

1. Must have daily, fully automated archiving and recovery protection
2. Other types of backup systems
 - a. Digital backup systems
 - b. External hard drive
 - c. Cloud computing servers
 - d. DVDs
 - e. CDs
 - f. USB/flash drives
 - g. Tape servers
3. Store the remote backup device off site from the main office
4. How often will backup occur?
 - a. hourly
 - b. nightly
5. What level of redundancy will the firm employ?
6. How often will the firm test the backup system?

I. Computer and scanner Disposal

1. Remove hard drive
2. Scrub all information prior to disposal

J. Disaster Recovery

1. Update procedures to ensure they include electronic disaster recovery
2. Educate your appointed successor lawyer on firm's paperless system

