Running a Paperless Law Practice

August 2015

Michael W. Reagor, Esq.

Part One: Basic Issues in Setting Up a Paperless Practice

Introduction/My Practice

My practice is primarily devoted to trust planning and administration, probate litigation and administration, and related elder law practice areas. The planning portion of our practice focuses on three pillars: practical or applied estate and trust law to assist clients in their planning goals; using and incorporating “best practices” in all procedures; and using technology within a paperless law practice to improve service.

What drove us to the paperless law office?

1. Where did we come from?

Thoughts on a short history

The paperless law office movement is part of the larger “green” office movement. http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/gogreen.html

2. What is the paperless law office?

My firm became “paperless” in 2008. What is the paperless law office? In our experience, the paperless law office is an office:

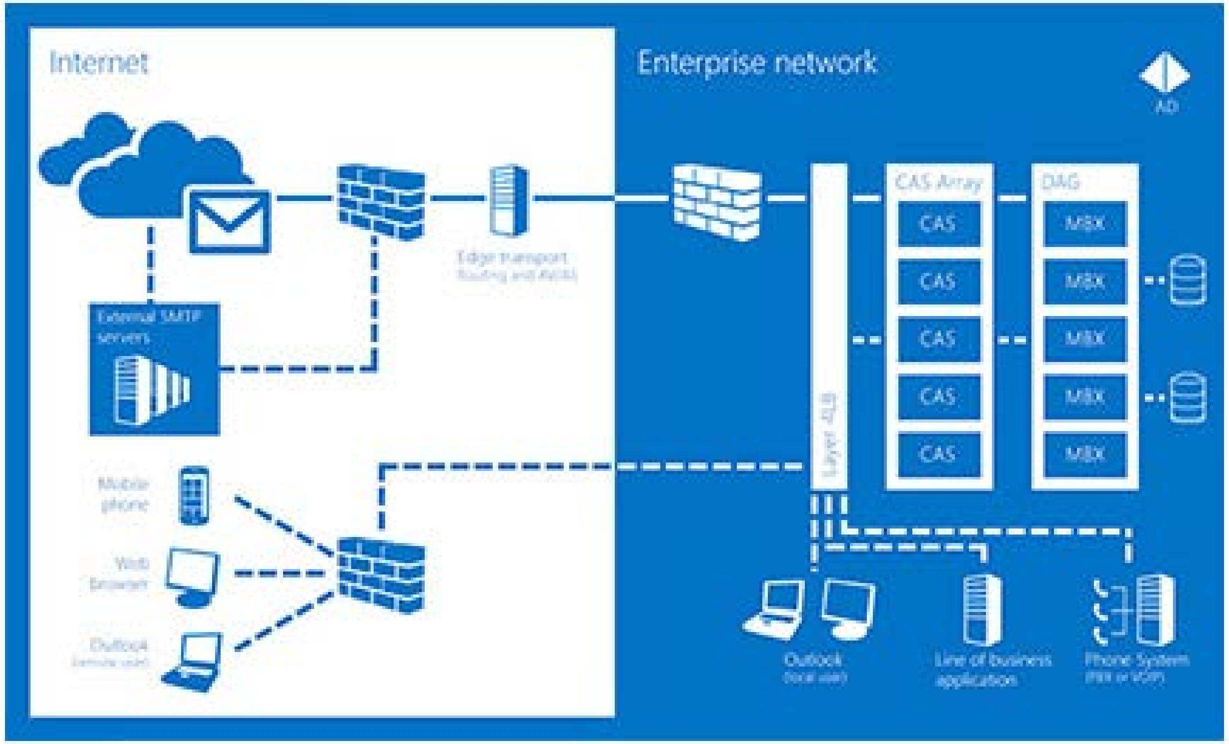
- That is dedicated to reducing and eventually eliminating the use of paper in every possible aspect of the practice
- That focuses on converting paper to data upon receipt and using and storing such digital documents electronically
- That implements paperless technology at particular points and in particular processes
- That involves a change of attitude and approach from the paper practice: abandon paper files as our basic organizational approach and instead embrace electronic documents as our primary files
- Where the paperless system is tied to every aspect of the firm’s operation
- That creates a single workflow process which is applied to all cases, transactional and litigation, small and large

The paperless law office: a practical exercise

- Establishing a “paperless” law office is a very practical pursuit. There is no single set of protocols that define a paperless law office. Further, while lawyers do have certain common ethical duties in every jurisdiction, such as those relating to file retention and termination of representation, those duties have generally been “superimposed” on paperless practices after the general structure of a paperless practice has been determined.
- Establish a plan/white paper to provide the structure, goals and guidelines for both the transition and the operation of the firm.
- The beginning of the project involves a strategy to convert paper files into digital files. This strategy involves (1) converting closed paper files to digital files, (2) converting and maintaining existing files as digital files, and (3) setting up new files within this system. Each of these file types presents different issues and requires different strategies.
- After conversion and staff “buy-in” to the paperless conversion strategy, there is a period of transition.
- A clear and comprehensive set of protocols or rules is the key to successfully operating a paperless law office. These protocols must be periodically updated in consideration of all of the following factors: type of practice; number of staff involved; skill set of staff; type of technology used or desired; client needs or requirements; and available budget.

3. Technology architecture of a paperless firm/practice

LANs:



The “cloud”

In recent years, a new software model has emerged: Software as a Service (or "SaaS").

- SaaS is distinguished from traditional software in several ways.
    - Rather than installing the software to your computer or the firm's server, SaaS is accessed via a web browser (like Internet Explorer or FireFox) over the Internet.
    - Data is stored in the vendor's data center rather than on the firm's computers.
    - Upgrades and updates, both major and minor, are rolled out continuously.
    - And perhaps most importantly, SaaS is usually sold on a subscription model, meaning that users pay a monthly fee rather than purchasing a license up front.

- In a typical LAN system, employees of a law firm are connected via a LAN server which manages all the information generated by individual users.
- Many practices now use cloud-based systems. These systems eliminate the need for a centralized server and in-house or resident software. In an entirely cloud-based system, users access and manage data, which is held on off-site servers, through a browser like Chrome or Internet Explorer. Cloud-based solutions eliminate the need for a server by generally deploying tools to a firm through a browser.
- Whether LAN or cloud-based, most law firms now use database managers for their data management. Data management includes managing calendaring software, contact data and email. Some systems also manage other data, such as billing information (e.g., Amicus Attorney; and AbacusLaw which integrates with TimeSlips).
- However, for various reasons, including concerns relating to security and data loss, many firms continue to use non-cloud LAN servers. Within such structure, many smaller firms continue to use Microsoft Exchange Server, which includes calendaring software, a mail server and contact manager . Microsoft Exchange Server 2013 is an example of a LAN based system that incorporates cloud-based attributes:
- The most commonly used law office practice management software suites (PMS) include AbacusLaw, Amicus (Amicus Attorney for LAN and Amicus Cloud), CosmoxLex, Clio, Credenza, Firm Central, HoudiniEsq, MyCase, ProLaw, and Rocket Matter.
  - A comparison chart of these products is at http://www.americanbar.org/content/dam/aba/migrated/tech/ltrc/charts/pmtbchart.authcheckdam.pdf.

This document includes two charts: a Practice/Case Management Software Comparison Chart for Solo/Small Firm, and a Time & Billing Software Comparison Chart for Solo/Small Firm. Scroll down to view the Time & Billing chart. Last updated: December 30, 2014.

Practice/Case Management Software Comparison Chart for Solo/Small Firm

(Note: May include time/billing features. See below for Time & Billing specific chart.)

	Pricing	Technical Requirements	Front Office Tasks	Back Office Tasks	Software Compatibility (Import/export, etc.)	Mobile Access	Technical Support
AbacusLaw	AbacusLaw from just $47/month/user Abacus Private Cloud™ (full virtual law practice) starts at just $197/month Custom, no risk proposal: http://www.abacuslaw.com/pricing/ ABA members save 15% on AbacusLaw through ABA Member Advantage.	AbacusLaw: Windows 8, Windows 7, Windows Vista Business or Ultimate or Windows Server 2003-2012 Abacus Private Cloud™: Any modern device with an Internet connection. (more info)	Integrated rules-based calendaring, case, contact & document management, email management, document assembly, auto-fill court forms, instant messaging, case notes and more. (more info) Practice Area Legal Solutions (PALS) are pre-configured products for specific areas of law. These out-of-the-box solutions come with the screens, rules, reports, documents, and forums. The experienced Professional Services team offers law practice solutions to customize how you use the AbacusLaw™ platform to meet your firm's needs. (more info)	Available in AbacusLaw Gold: One-click time tracking, billing, accounting, trust accounting, general ledger, check writing, payroll, integrated credit card processing and ACH billing and more. (more info)	Abacus Private Cloud™ is software agnostic so you can use any applications, per your firm's requirements. Abacus Law: Microsoft Word, Outlook, WordPerfect Data Migration: Abacus Professional Services provides expert data migration from existing Case Management Software systems to the AbacusLaw platform (or platform for your choice) (more info)	Access your practice anytime, anywhere and from any device. Abacus offers both In-Office or Virtual Practice Environments. Not sure which is right for your needs? Let our experts help you assess your options with a no-obligation Technology Readiness Assessment. (more info)	Abacus Private Cloud includes fully managed IT, 24x7 monitoring, managed backups, inherent disaster recovery, antivirus and malware protection, firewall & intrusion prevention, unlimited technical support and more all from the U.S. AbacusLaw offers U.S. based support, M-F from 6am-5pmPST, by remote desktop, telephone, email and fax. (more info)

Note: these charts do not provide a comprehensive comparison of all Practice Management/Time & Billing products on the market. Inclusion in the chart should not be construed as an endorsement or recommendation. If you have an update to a listing or if you'd like to submit a product for consideration in future chart revisions, please contact the LTRC at ltrc@americanbar.org.

4. Hardware in a paperless office

- Digital scanners
  - Type, number, capabilities depends on firm size and nature of practice
- Networked workstations or cloud based system
- Backup systems
- Monitors
- VoIP system
- Wireless networking

See http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis.html

5. Software in a paperless office

- Calendar and docketing software
- Case and practice management software
    - Conflict management
    - CRM functions
- Email client/software
    - Uniform software and personalization
- PDF software
    - OCR capable
    - Add-ins:
        - bookmarks:
        - Inking:
- Time and billing software
- Document assembly software

6. Digital Strategies for Opening or Updating a Client File

Modern technology has become a planner’s best friend, allowing the modern law firm to use technology to complete tasks that once took significant human effort. The keys are, first, creating a comprehensive set of protocols that are followed in every case and, second, using technology where it can assist.

Paperless protocols for practices

- Each paperless law office should establish a comprehensive set of protocols that every team member should follow in every case. Standardization of tasks ensures consistency, establishes best practices for all team members, and reduces errors.
- These protocols should cover each step of client intake.

First, below is a standard set of protocols for client intake that might be used in a paperless office:

Client intake procedures:

- *Client and matter are set up in Case Management Software (CMS):*
- *Assistant runs conflict check and sets up the matter within CMS*
- *Office manager and receptionist coordinate on billing (e.g., Timeslips) set up*
- *Assistant emails new client/matter intake sheet to entire team*
- *Each client/matter intake sheet is electronically saved by assistant*

Second, protocols are needed to set up electronic folders. Below is example of EP client for my firm:

File and folder set up procedures:

- *EP Files*
- *Note: the below folders should be established for each new EP/Trust planning client intake. At responsible attorney's discretion, a file may incorporate a corresponding paper/redrope folder. Such folder should hold only that information which cannot be retained electronically, such as original documents that must be returned to client.*
- *For all EP files, the electronic folder structure should be:*
- *ATTORNEY NOTES*
- *CORRESPONDENCE*
- *DOCUMENTS (SUBFOLDERS DRAFTS/SIGNED DOCUMENTS)*
- *FEE AGREEMENT*
- *FUNDING*
- *RESEARCH*

Folders are available and should be pasted from H:__________.

Note that all that has to be done to set up the folder is to copy the folder and its subfolders from the server location and rename it in the appropriate location for the particular client (in the correct folder under the correct names). The structure of the folder can be varied by the responsible attorney as necessary. However, the primary goal of data and document retention must be achieved, regardless of which structure or procedures are used.

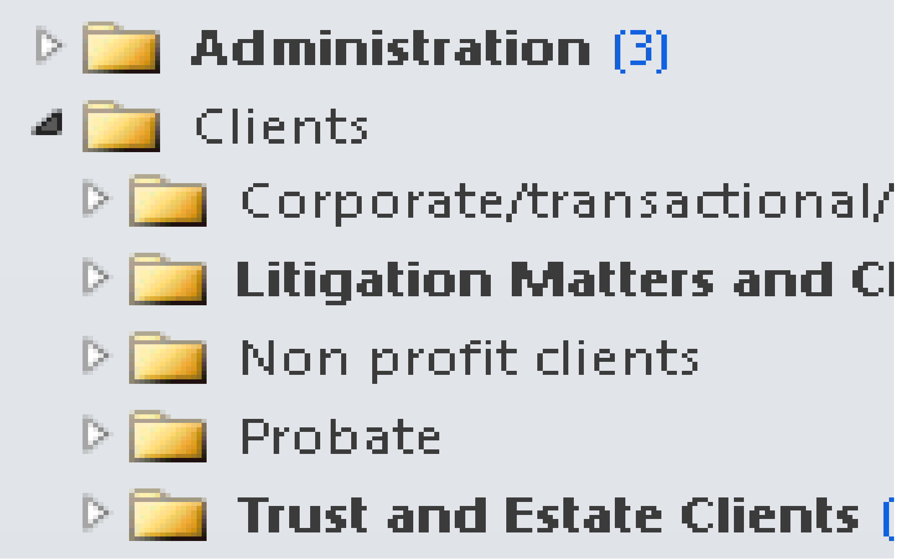
Several important rules must be followed for the digital folder system to work properly.

- First, the firm must have a universal folder naming convention. Some offices using more sophisticated CMS use a numbering system for both clients and documents. Other firms may use a naming convention with the name of the client (last name first) followed by the matter name, as follows: JONES/2015 EP.
- Second, the firm must identify the format for digital documents. Because of the value of Adobe Acrobat in the paperless office, the portable document format, or PDF, has become the accepted format in almost all paperless firms.
- Third, documents must uniformly be placed in the correct folder. That will be a matter of practice developed between an attorney and staff. Second, whenever possible, AVOID DUPLICATION. Duplicate digital docs create confusion and added client cost.
- Fourth, additional folders should not be created on an ad hoc basis without authorization. Such practice creates confusion and only encourages duplication.

7. Email procedures in the paperless law office

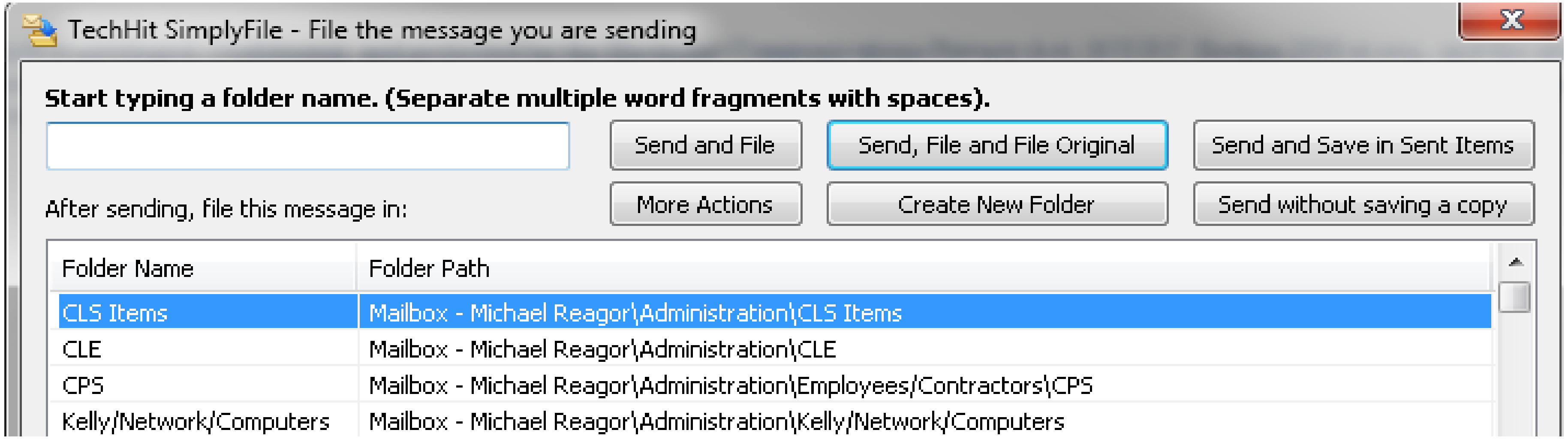
Email procedures need to be set up to retain information exchanged at the firm and with the client. The best practice is to adopt a system that can work with your office. Some firms use systems that require the user to save each digital document (including each email) within a client folder. Most smaller or boutique practices use Outlook or similar POP3 email client system and have protocols regarding retention of emails and attachments.

One potential solution is to use a LAN based email system and purchase add-ons to accommodate your practice. Outlook/Exchange is commonly used as an email client by both large and small firms. Outlook itself allows a user to create folders for specific matters and then “save” emails to specific folders:



- Administration (3)
- Clients
  - Corporate/transactional/
  - Litigation Matters and Cl
  - Non profit clients
  - Probate
  - Trust and Estate Clients (

Some very useful folder add-ins are available from third party vendors. Simply File for Outlook, for instance, automatically files an email in both “sent” emails and a user-designated folder. The user simply selects the designated folder when the first email on the matter is sent and then the software thereafter “learns” the email language and automatically selects the folder before the email is sent:


TechHit SimplyFile - File the message you are sending
Send and File
Send, File and File Original
Send and Save in Sent Items
More Actions
Create New Folder
Send without saving a copy

Start typing a folder name. (Separate multiple word fragments with spaces).

After sending, file this message in:

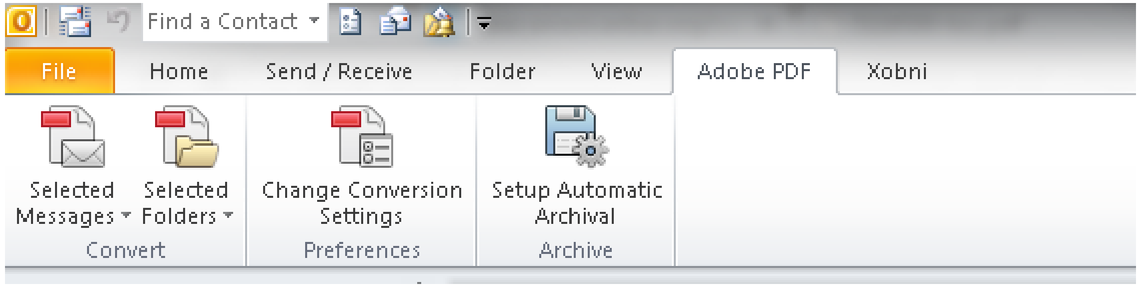
Folder Name	Folder Path
CLS Items	Mailbox - Michael Reagor\Administration\CLS Items
CLE	Mailbox - Michael Reagor\Administration\CLE
CPS	Mailbox - Michael Reagor\Administration\Employees/Contractors\CPS
Kelly/Network/Computers	Mailbox - Michael Reagor\Administration\Kelly/Network/Computers

Email retention: archiving solutions

Many larger firms use robust and effective email archiving software solutions.

- These systems ensure that email is retained and not inadvertently destroyed.
- However, these systems do not provide effective solutions for paperless firms that use email folders as part of their document retention process.

An effective email folder system along with retention policies allows a firm to bypass the time and expense of individually saving each email and attachment. Further, when a matter is ready to close, the email folder can be quickly and easily converted to a PDF organizer using the Adobe Acrobat Add-In for Outlook:



8. Document retention

Most states require attorneys to retain client files for a minimum period.

- For instance, Rule 1.15 of the Model Rules of Professional Conduct suggests that records relating to client property (i.e. trust account funds) be kept for a period of five years.
- Colorado's version of this rule requires retention of such documents for a period of seven (7) years.
- The relevant documents includes receipt and disbursement records, bills, and accounting records. Additionally, all fee agreements (hourly, contingent or other) must be retained for the same time period and therefore, should be placed in the client billing folders.

Further, most states require pleadings and signature pages to be retained for a minimum period.

For instance, Colorado Rule of Procedure Rule 121 §1-26(7), applicable to actions in Colorado state courts, provides that a “printed or printable copy of an e-filed or e-served document with original or scanned signatures shall be maintained by the filing party…required to maintain the document for a period of two (2) years after the final resolution of the action, including the final resolution of all appeals”.

For this reason, firms should retain digital copies of ALL client documents for a period not less than the period of retention required in that jurisdiction.

- Many practices are now able to retain and maintain digital copies of all client files as well planning documents indefinitely.
- Consistent with proper backup practices, firms should maintain duplicate digital copies of closed files.

9. Automated Reminders to Contact Clients for Periodic Updates

Ethical considerations:

Under the Model Rules of Professional Conduct 1.4(a), Communication,

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

Comment 1 to the rule states that “reasonable communication between the lawyer and the client is necessary for the client effectively to participate in the representation.”

Different methods used by different attorneys

- Almost all systems are now electronically based
  - Litigation practices
    - Calendaring systems with daily reminders
    - Systems which create dates from rules
  - Non-litigation or transactional practices
    - Calendaring systems with daily reminders
    - Rules with automated deadlines
  - Most malpractice insurance coverages accommodate entirely electronic systems

Newsletters

Back

Print Close

D·R·C LAW
Doing Right By Our Clients ™

DYMOND • REAGOR • COLVILLE, LLP
ATTORNEYS AND COUNSELORS
THE EDWARD BUILDING, SUITE 1040
8400 E. PRENTICE AVENUE, GREENWOOD VILLAGE, CO 80111
(303) 793-3400
MAIL@DRC-LAW.COM

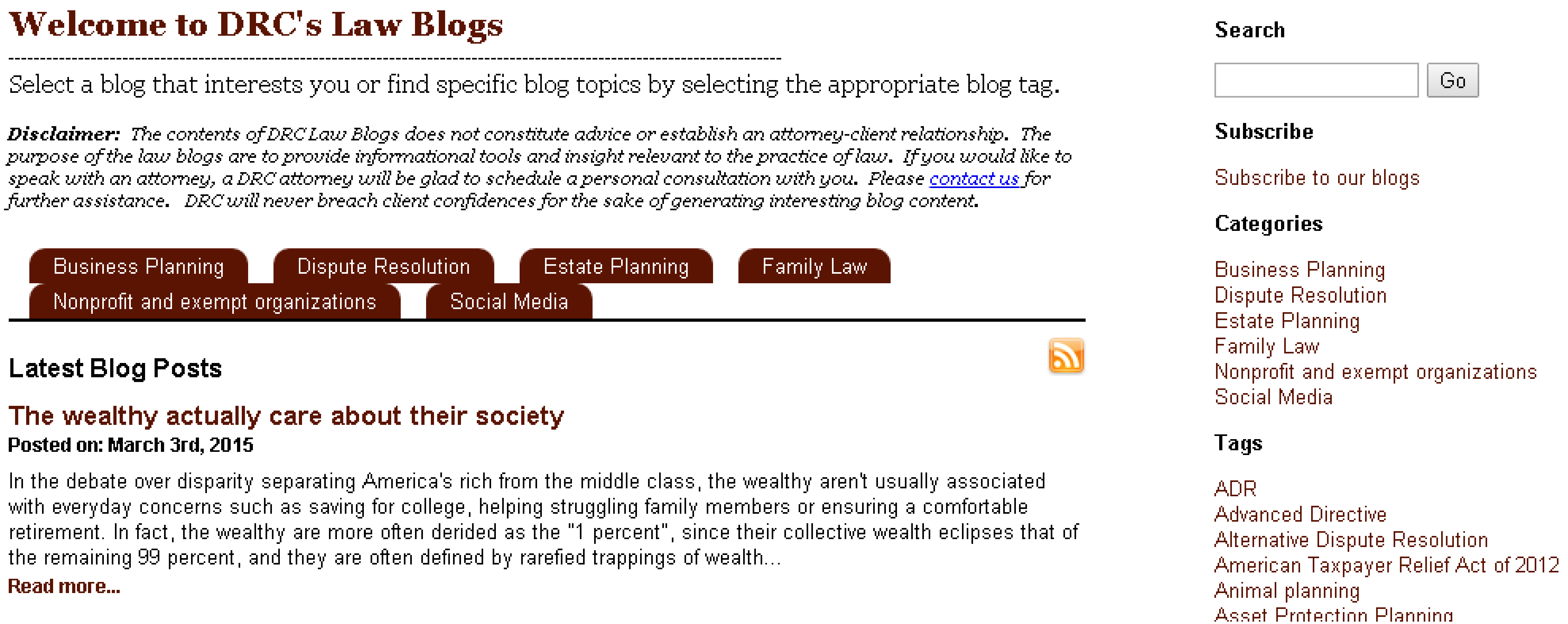
The Wealth Counselor

Protecting assets against loss has become a common goal of estate planning. Asset protection trusts come in many different forms and can be used to protect property for the use and benefit of clients as well as their families and other beneficiaries. In this issue you will learn how clients can easily integrate asset protection trusts into their estate plans.

What Is an Asset Protection Trust?
An asset protection trust is a special type of irrevocable trust in which the trust funds are held and invested by the Trustee and are only distributed on a discretionary basis. The purpose of an asset protection trust is to keep the trust assets secure for the beneficiaries instead of being exposed to loss to the beneficiary's creditors, in a divorce, or to predators.

Asset protection trusts come in two forms: third party trusts and self-settled trusts. A third party trust is set up by one party for the benefit of another, while a self-settled trust is set up by one party for their own benefit.

Third Party Asset Protection Trusts Provide Inheritance Protection



Welcome to DRC's Law Blogs

Select a blog that interests you or find specific blog topics by selecting the appropriate blog tag.

Disclaimer: *The contents of DRC Law Blogs does not constitute advice or establish an attorney-client relationship. The purpose of the law blogs are to provide informational tools and insight relevant to the practice of law. If you would like to speak with an attorney, a DRC attorney will be glad to schedule a personal consultation with you. Please contact us for further assistance. DRC will never breach client confidences for the sake of generating interesting blog content.*

Latest Blog Posts

The wealthy actually care about their society

Posted on: March 3rd, 2015

In the debate over disparity separating America's rich from the middle class, the wealthy aren't usually associated with everyday concerns such as saving for college, helping struggling family members or ensuring a comfortable retirement. In fact, the wealthy are more often derided as the "1 percent", since their collective wealth eclipses that of the remaining 99 percent, and they are often defined by rarefied trappings of wealth...

Read more...

Subscribe

Subscribe to our blogs

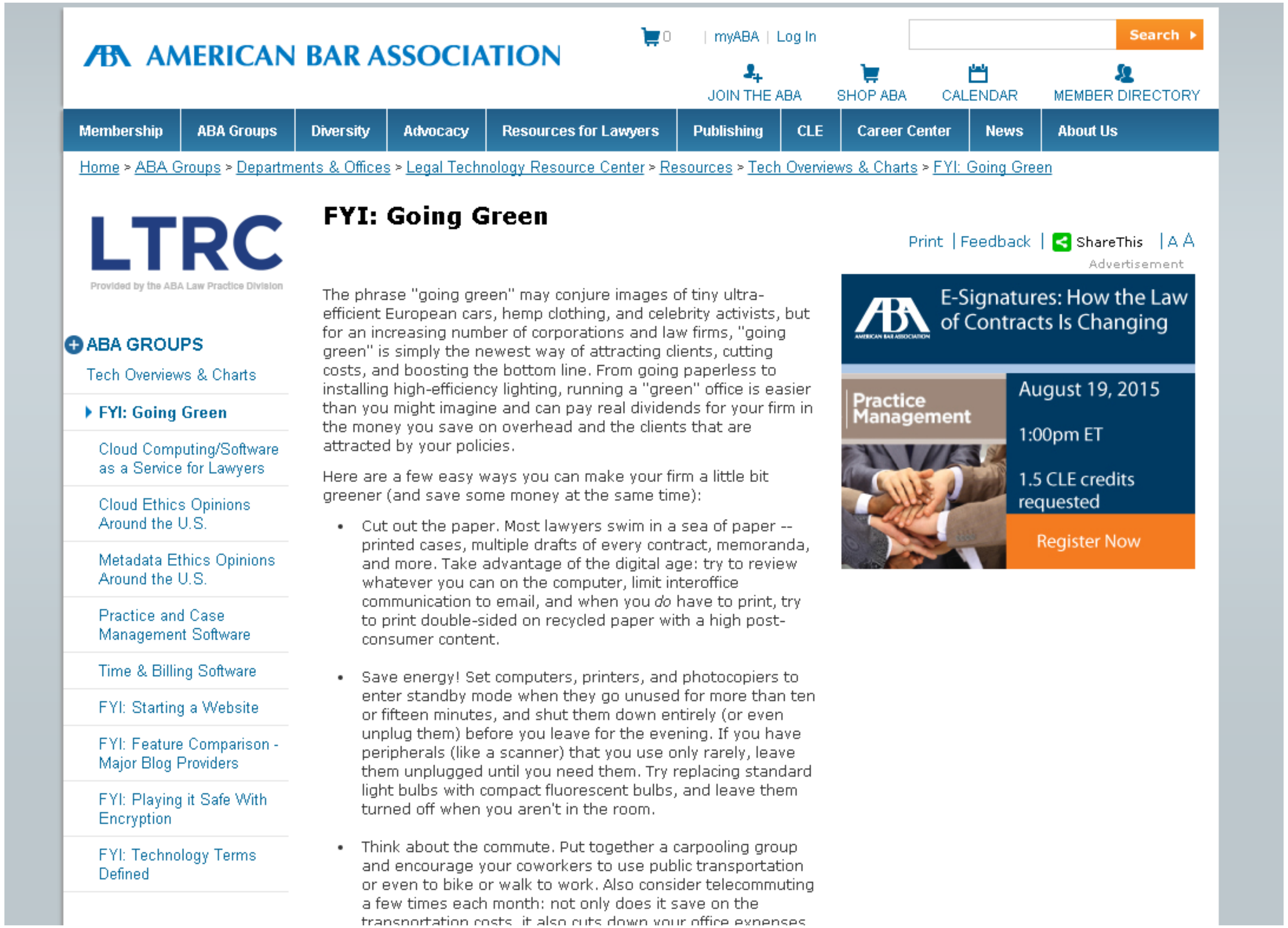
Categories

Business Planning
Dispute Resolution
Estate Planning
Family Law
Nonprofit and exempt organizations
Social Media

Tags

ADR
Advanced Directive
Alternative Dispute Resolution
American Taxpayer Relief Act of 2012
Animal planning
Asset Protection Planning

10. Resources for getting started



AMERICAN BAR ASSOCIATION
0 | myABA | Log In
Search
JOIN THE ABA
SHOP ABA
CALENDAR
MEMBER DIRECTORY
Membership
ABA Groups
Diversity
Advocacy
Resources for Lawyers
Publishing
CLE
Career Center
News
About Us
Home > ABA Groups > Departments & Offices > Legal Technology Resource Center > Resources > Tech Overviews & Charts > FYI: Going Green
LTRC
Provided by the ABA Law Practice Division
ABA GROUPS
Tech Overviews & Charts
FYI: Going Green
Cloud Computing/Software as a Service for Lawyers
Cloud Ethics Opinions Around the U.S.
Metadata Ethics Opinions Around the U.S.
Practice and Case Management Software
Time & Billing Software
FYI: Starting a Website
FYI: Feature Comparison - Major Blog Providers
FYI: Playing it Safe With Encryption
FYI: Technology Terms Defined
Print | Feedback | ShareThis | A A

FYI: Going Green

The phrase "going green" may conjure images of tiny ultra-efficient European cars, hemp clothing, and celebrity activists, but for an increasing number of corporations and law firms, "going green" is simply the newest way of attracting clients, cutting costs, and boosting the bottom line. From going paperless to installing high-efficiency lighting, running a "green" office is easier than you might imagine and can pay real dividends for your firm in the money you save on overhead and the clients that are attracted by your policies.

Here are a few easy ways you can make your firm a little bit greener (and save some money at the same time):

- Cut out the paper. Most lawyers swim in a sea of paper -- printed cases, multiple drafts of every contract, memoranda, and more. Take advantage of the digital age: try to review whatever you can on the computer, limit interoffice communication to email, and when you *do* have to print, try to print double-sided on recycled paper with a high post-consumer content.

- Save energy! Set computers, printers, and photocopiers to enter standby mode when they go unused for more than ten or fifteen minutes, and shut them down entirely (or even unplug them) before you leave for the evening. If you have peripherals (like a scanner) that you use only rarely, leave them unplugged until you need them. Try replacing standard light bulbs with compact fluorescent bulbs, and leave them turned off when you aren't in the room.

- Think about the commute. Put together a carpooling group and encourage your coworkers to use public transportation or even to bike or walk to work. Also consider telecommuting a few times each month: not only does it save on the transportation costs, it also cuts down your office expenses

Part Two: Data Security

1. Special duty of lawyers to protect information

- Special duty of lawyers to protect data
- Data security risks threatening client information are complex issues often beyond the ken of most lawyers. Hire a consultant.
- Lawyers in paperless firms must have some background knowledge relating to basic network architecture and security issues and must stay abreast of best practices relating to protection of data.

2. Establishing Multiple Layers of Backup for Electronic Files

- Law firms and other businesses increasingly create and store their business documents electronically. Today, up to 90% of documents created and received by businesses are “born digital,” created digitally on a computer or some other electronic device, as opposed to having been created by analog means (pencil, pen, typewriter, etc).
- Documents that are not born or received digitally are often converted into electronic format through scanning in order to fulfill space saving and document organizing/document management purposes (such as in the creation of paperless offices).
- Lawyers increasingly depend upon the integrity of their computer systems and document management systems for access to their vital practice-related information such as correspondence, memos, and financial records.

Electronic data can be threatened in several ways:

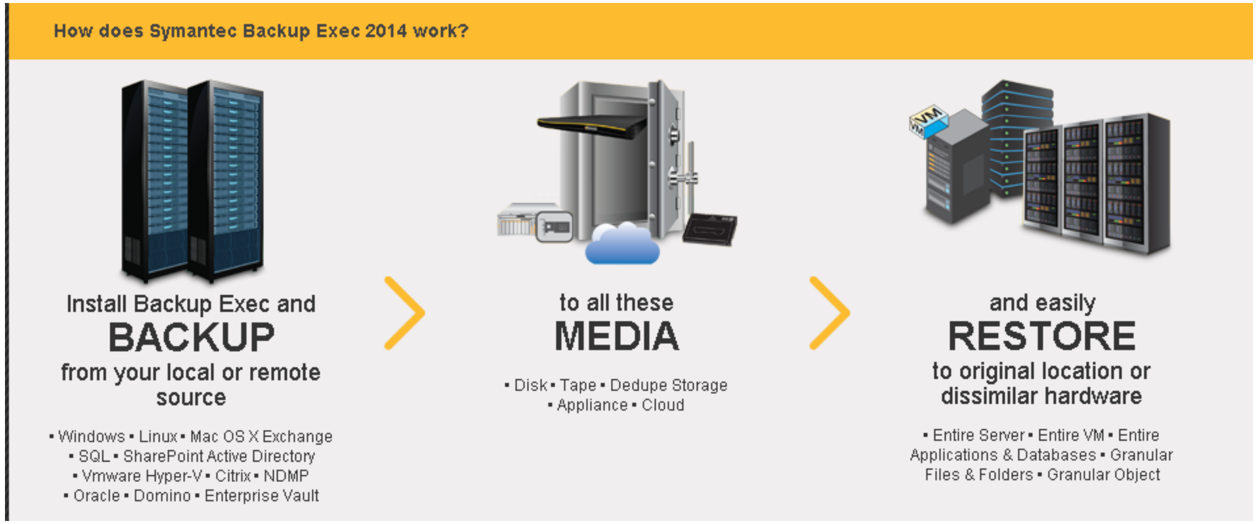
- computer hard drives can fail
- laptops can be lost or stolen
- data can be overwritten or erased due to computer or human error or due to malicious attacks
- office equipment may be destroyed by natural disasters such as earthquakes or fire

To guard against data loss, the paperless law office must set up a data backup system through which data is regularly copied from computers and servers to other storage devices.

3. Backup media and software

- Data can be backed up to several different types of media.
- First, backups are often made to an external hard drive or network-attached storage devices, to DVDs, CDs, USB/flash drives, tapes, or to remote servers over the internet.
- Offices often use a combination of media to store their backups both onsite and offsite.
- Several different software products are available to help with the process of making file backups and disk images.
- RAID systems ("redundant array of inexpensive disks") for hard drives can help preserve firm data in the case of a hard disk failure. However, RAID systems should be paired with periodic backup systems.

Backup systems can involve either onsite or offsite storage. Current solutions involve a software and hardware component that work together to ensure backup, allow an office to select the backup media (onsite or offsite), and then allow easy restoration. Symantec's Backup Exec is a typical system:



How does Symantec Backup Exec 2014 work?

Install Backup Exec and **BACKUP** from your local or remote source

▪ Windows ▪ Linux ▪ Mac OS X Exchange ▪ SQL ▪ SharePoint Active Directory ▪ Vmware Hyper-V ▪ Citrix ▪ NDMP ▪ Oracle ▪ Domino ▪ Enterprise Vault

to all these **MEDIA**

▪ Disk ▪ Tape ▪ Dedupe Storage ▪ Appliance ▪ Cloud

and easily **RESTORE** to original location or dissimilar hardware

▪ Entire Server ▪ Entire VM ▪ Entire Applications & Databases ▪ Granular Files & Folders ▪ Granular Object

Whatever system is selected, it should be compliant with the various international security standards used (such as SOC1, SOC2 and ISAE 3000 Type II).

- These standards assure proper security, physical security, storage and network infrastructure, firewalls, network configuration and account management.
- Ensure your consultant considers all these issues when selecting a system.

- Onsite storage of backup media generally requires staff to rotate media daily or weekly, and ensure that backup copies are stored in safe, fireproof locations.
- Further, each law office must ensure that backup systems are always operational.
  - Many offices now use software which provides email notification when a backup system has failed or has issues.

- Several current systems, such as the Backup Exec, use hard drives rather than movable media, such as portable drives, that can be safely stored.
  - These types of systems do protect against data loss but do not prevent physical destruction and so should probably be avoided as sole means of backup.
  - Onsite storage of media backed up through systems like Backup Exec are a lower cost but acceptable solution so long as regular backups are made and safely stored.
  - A typical system might involve weekly backups of file and mail servers and the domain controller, and then daily backups of the mail server.

4. Backup Location

Backups of your data can be kept onsite for easy access, but it is recommended to keep backups of your data offsite as well.

Offsite backup or cloud storage protects your data from destruction or theft and enables restoration of data even if your main computer and onsite backups are destroyed or stolen.

Offsite backups:

- Can be in external media in the form of CDs, DVDs, USB/flash drives, external hard drives, tapes, or other media which you then store in an offsite location, or
- In the form of backup data uploaded over the internet and stored on a remote server, referred to as “cloud backup”.

5. What is backed up? File Backups vs. Disk imaging

When you perform a file backup you manually or automatically (using backup software) copy your computer data such as word processing documents, music, photographs, and other computer files to some form of electronic storage.

File backups are limited in that they do not result in working copies of your operating system and installed software programs.

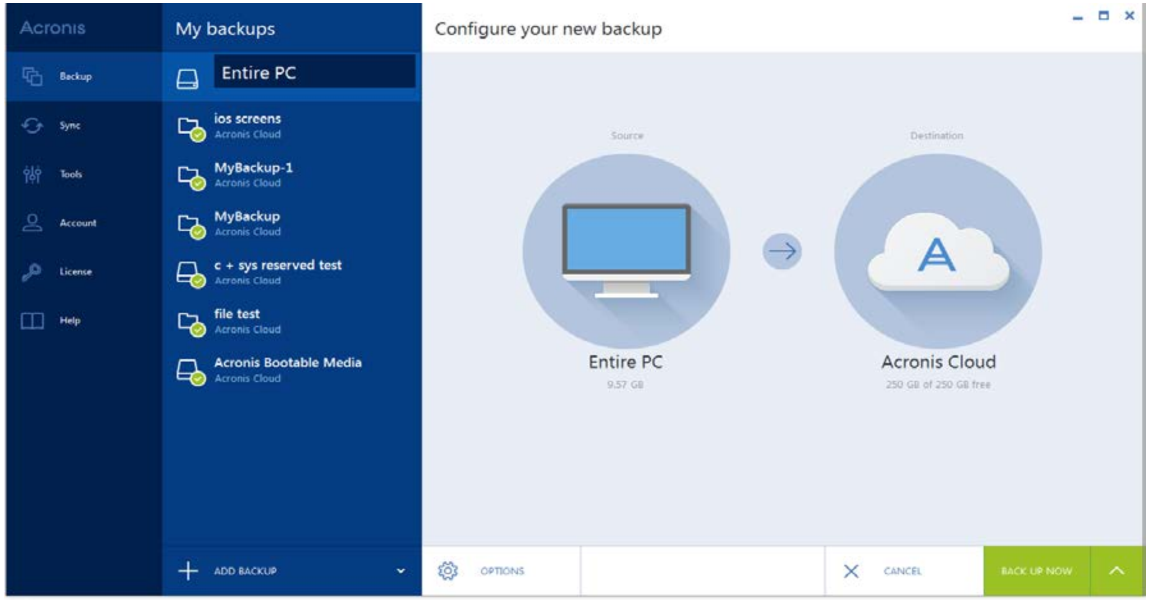
Backups

- Can involve complete file backups, where every file on a server or computer is copied
- Incremental backups use software to detect and copy only new and modified files over your entire server or computer or specific folders you specify
- Partial backups only backup specified files.

“Disk imaging” is another method of backing up data.

- A disk image is a copy not only of your files but also your entire file system, resulting in a copy of your operating system, applications, and drivers as currently set up on your computer.
- Thus, you can use the disk image to recreate your entire computing system.
    - After restoring from a disk image, all of your programs will all work exactly how they worked at the moment your disk image was created, without having to reinstall your operating system, individual applications, and drivers.

Most imaging backup systems are similar to full system disk imaging software like Acronis True Image. Like file backup systems such as Backup Exec, the software now allows an office to easily setup the backup system, select the data to be imaged, and to select the destination for the imaging. Acronis users typically now use offsite cloud-based storage solutions:



In general disk images can take more time and more memory to create than file backups, as everything on your computer is copied when creating a disk image, including the file system.

- Because of the amount of time and memory generally required to make disk images, and to install a disk image to a computer, disk images may not be suitable for routine backup.
- Some offices use a strategy of making disk images periodically, such as once a week, to capture their entire computing environment, and also performing incremental file backups more often, such as daily, to backup their important business files and documents.

If you do not use disk imaging software, you must maintain access to software needed to restore systems.

- Since most software is now available through downloads, security should only require retaining installation/license codes.
- Microsoft Office 365, for example, can be installed locally or used online through a browser. If an operating system is destroyed, the office products can be quickly reinstalled online.
- Other important software used by the firm should similarly be available for reinstallation in the event of data loss.

Backups for networks

- In a client-server network, users save their files to the central server, and then backup software can be set to backup the entire server or certain folders from the server automatically at set times.
- For peer-to-peer networks, which are not commonly used any more, multiple users can store their files on a computer dedicated to storage or on a network attached storage device, either of which can be backed up automatically using backup software.
- Network attached storage devices are usually external hard drives which connect to a router and are accessible on a local network.

With higher speed internet available to users throughout the world and continued development of cloud-based solutions, there are various inexpensive off-the-shelf solutions that will fit almost every firm or need.

- For instance, Carbonite and similar companies offer a suite of backup solutions which will fit almost every law firm and need.
- However, as discussed below, attorneys have a special duty to protect the confidentiality of client information and thus lawyers must either have proper third party server agreements with backup data providers or use technology solutions such as encryption. Those are discussed below.

6. Automating Backup Procedures

Onsite backup systems

- The primary risks with onsite backup systems are loss by physical destruction and hardware failure.
- Firms that continue to use onsite systems, such as Backup Exec, must ensure that software and hardware are regularly tested to ensure that regular backups are made.

Offsite/cloud-based backup solutions

There are a variety of effective cloud-based backup systems now available.

- Most of the file imaging systems, such as Backup Exec, as well as disk imaging systems such as the Acronis True Image software, offer both onsite and cloud-based backup options for firms.
- Most of these systems have user interfaces which allow both small and larger firms to easily and cost-effectively select backup options, monitor and ensure effective backup, and ensure security of data.

7. Security of On-Site and Off-Site Digital Files

Onsite and offsite digital files from a paperless practice must be properly protected.

Under the Model Rules of Professional Conduct, a lawyer may not reveal information relating to the representation of a client unless the client gives informed consent or the disclosure is impliedly authorized in order to carry out the representation.

This duty has generally been interpreted to mean that lawyers have a duty to prevent unauthorized access to client data.

Internal data security policies

Generally, paperless firms should consider these actions and issues relating to internal security policies:

- Adopt policies addressing computer and Internet usage, and enforce those policies.
- Ensure use of a strong firewall and regularly update firewall technology.
- Ensure use of only strong passwords (e.g., passwords more than eight characters in length containing non-alphanumeric and non-dictionary words).
- Ensure use of comprehensive antivirus software which is regularly and automatically updated.

Internal data security policies (cont’d)

- Ensure continuous software updates of both servers and workstations.
  - For both Windows and Apple based systems, as long as the software is properly licensed, both servers and workstations can be easily set to automatically update security patches.
- The firm or its consultant should actively monitor system logs and security alerts.
  - As noted, most current software can be set to send automatically notify the firm when there are issues or suspicious activity.
- Ensure that system security is reviewed annually by a third party.
- Ensure there is a policy to handle suspected security incidents.

Further, every paperless practice should establish comprehensive user policies.

- These policies should be made available to all users of the system in written form and on a regular basis.
- Firms should require users to review and accept the policy on a regular basis.

Every comprehensive user policy should consider addressing these policies:

- Network/System Access. Authorized users of the system should be identified. Access limitations should be described. Use of passwords and other access security processes should be described and made mandatory. The firm may want to require that all system users shut down their terminals at the end of each day to help control access.
- Network Use Restrictions. The policy should clearly indicate that the system is to be used for the firm’s purposes only. Personal use of the system should be prohibited. If access to certain databases or the Internet is to be denied or limited, those limitations should be described. To the extent that there are limits on downloading and use of software from sources outside the firm (e.g., to reduce the risk of virus infection in the system), those restrictions should be defined.
- Penalties. Users of the system should be advised that violations of the network use policy can result in disciplinary action, including termination of employment.
- Privacy. The policy should indicate that all use of the network may be monitored by the firm (including monitoring of e-mail, Internet use, and database access). It should provide for express written acknowledgment of that policy by all users of the system. The policy should also specifically describe obligations imposed on users of the network to maintain the confidentiality of data contained in the network.

Firm user policies (cont’d)

- Encryption. Firms should address when email messages should be encrypted. The firm may also want to require specific markings/designations on all confidential electronic documents (e.g., mark designating confidential status in the subject line of e-mail message headers).
- Record Retention. The policy should define the duration and method of retention for all of the firm’s electronic records. This should include a description of what types of documents should be retained (e.g., e-mail messages). For firms that use complete backup procedures, users usually need only be instructed to avoid improperly destroying data. To the extent that the firm needs to limit distribution/proliferation of electronic documents, the policy should include restrictions on copying and distribution of electronic messages.
- Content Controls. In addition to requiring that all messages be work-related, the firm should emphasize that message content should be appropriate for a work setting. Users should be reminded that inappropriate system content includes material which could constitute harassment and material which infringes on intellectual property rights of others.
- Identification of Responsible Personnel. The policy should designate specific individuals who will bear responsibility for enforcement of the policy and management of the network.
- Procedures in the Event of Unauthorized Use. The firm should develop procedures to identify and investigate incidents of unauthorized system use in advance of such incidents. These procedures should be designed to minimize the damage cause by the unauthorized use and to limit harm in the event of an incident.

External security policies

- User security policies should address issues of security and confidentiality for information disclosed by firm personnel to persons outside the firm or when using potentially insecure systems.
- For data backup, paperless firms should generally be implementing security systems for offsite data that are certified compliant with international standards such as SOC 1/SOC2 and ISAE 3000 Type II.
    - These standards address all aspects of cloud infrastructure, operations, and control, including facilities, physical security, storage and network infrastructure, firewalls, network configuration, account management, and more.

Security for cloud-based digital files

- In order to preserve security and confidentiality of off-site files, paperless firms using cloud-based backup systems must ensure that third party server agreements protect data held offsite.
  - However, this solution does not address risks relating to un-encrypted data. Those risks were recently exposed with the NSA PRISM program, where cloud providers were compelled to produce encryption keys under subpoena.
  - Thus, it may be unwise to provide encryption keys to a cloud provider and there is the additional risk that such provider may have a rogue employee who improperly accesses data.

Options for encryption and off-site storage of data with third parties

- Under the "key and data" model, your key is stored alongside your data, making it easy retrieve. However, in this model, the key is subject to the same subpoena as the data and a rogue employee could use the key.
- Some service providers have responded to these concerns by purporting to "escrow" encryption keys with a third-party escrow service, saving it separately from data, and rotating it frequently. However, a subpoena can still force these service providers to produce keys as part of a customer's data.
- Another option is to use an onsite server, behind the firm's server firewall, and to encrypt data before it is saved to the cloud ("key server model"). By keeping encryption keys in-house behind a secure server a firm guarantees sole ownership and access of the data. Using this system, data is encrypted locally and then the encrypted data is backed up in the cloud. One minor limitation to this system is that it requires some additional user management.

Options for encryption and off-site storage of data with third parties (cont'd)

- Some now argue that maximum security and privacy can be provided by using a two-factor encryption key management system. In this setup, a unique key is generated, encrypted, and turned into a token, which is then stored with the third party provider. This token can only be accessed by the administrator or end user providing his credentials as the complementary part to decrypt the stored token; and second, the data is also encrypted. In order to access the encrypted data, both parts of the equation need to work together to recreate the key, which only exists in that unique session. Since only the administrator or end user has access to that token, anyone who wants the data would have to go to him to get the first piece of the puzzle. Effectively, no one can access the data without your knowledge.
- For paperless firms using cloud-based backup, these last two options seem the most appropriate.

8. Security and Confidentiality with Third Party Server Agreements

As noted, many state bars have provided ethics opinions regarding use of cloud computing and cloud-based backup systems. Generally, these opinions provide that attorneys may use offsite backup provided that certain requirements are met. Most of the opinions (at http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html) include these basic requirements:

- First, the firm must know and understand how the provider handles the storage and security of data.
- Second, the provider must reasonably ensure the confidentiality of firm data and the firm must ensure that a confidentiality agreement is made and followed by the provider.

- Third, the firm must periodically review security measures and implement best practices were available to protect the confidentiality of data.

The NSA PRISM program exposed the fact that providers can be compelled to disclose to the government data held for customers. Even before this risk was publicly disclosed, many firms had adopted policies requiring that only encrypted data would be backed up in the cloud.

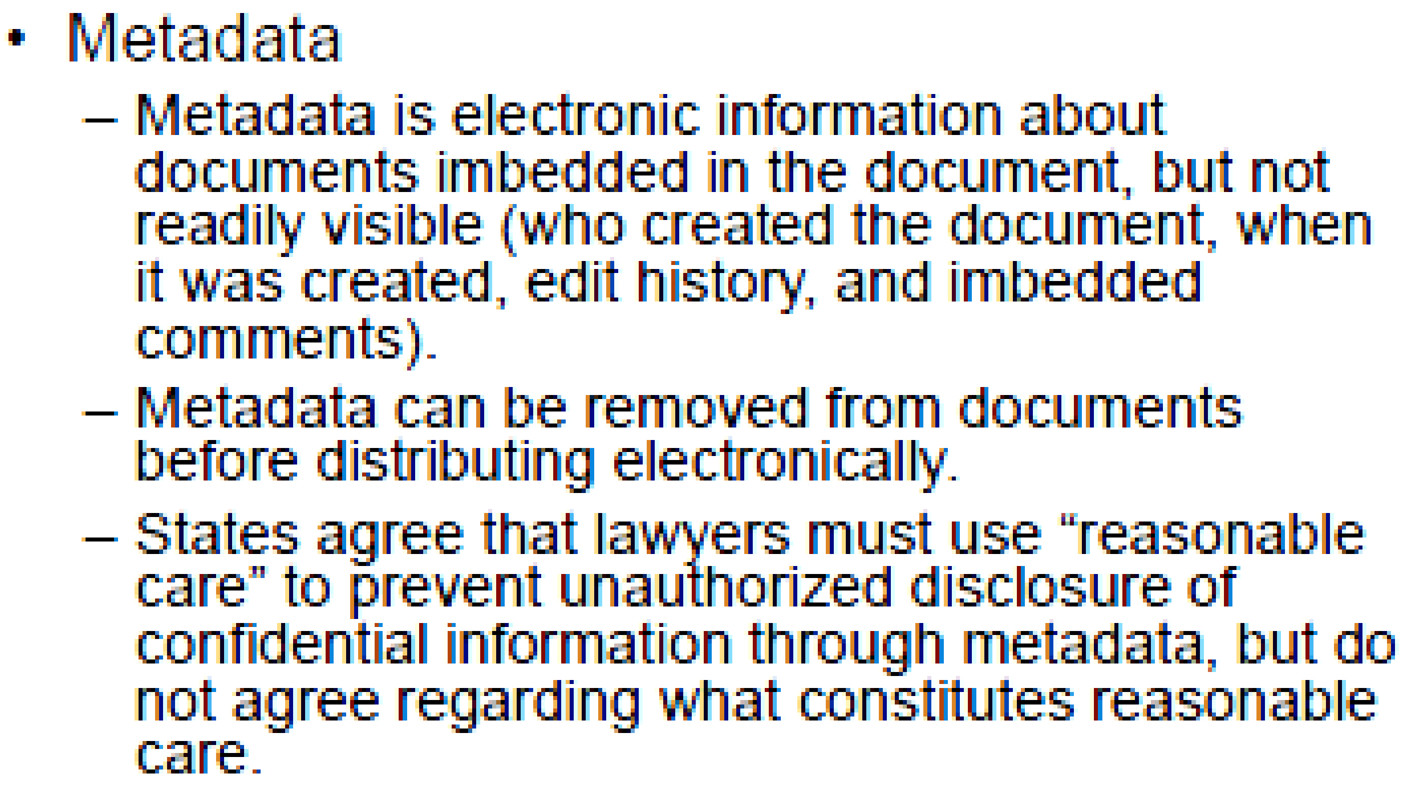
Considering the conclusions of the various cloud-computing ethics opinions, it seems that the current levels of risks dictate that best practices would require firms to ensure that cloud-based data is encrypted before delivered to a provider and that the encryption keys are held securely by the firm or by a reliable third party escrow.

- Various cloud providers are now offering services sufficient to ensure privacy and security for law firm cloud backup.
  - Many of these firms have implemented administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of law firm data.
  - For instance, Carbonite states that is compliant with stringent Massachusetts data security regulations and the SOC2 protection standards. See, e.g., http://www.carbonite.com/in-action/cloud-backup/legal. Mozy also offers a similar product. http://mozy.com/decho-more-than-doubles-number-of-mozy-legal-customers.
- In addition, many companies offering practice management software, such as Abacus, Rocket Matter, Clio and HoudiniEsq, either offer full-cloud based solutions or offer cloud backup solutions. Many of these companies will have standardized cloud backup provisions that meet or exceed law firm ethical confidentiality requirements for cloud-based retention of data.

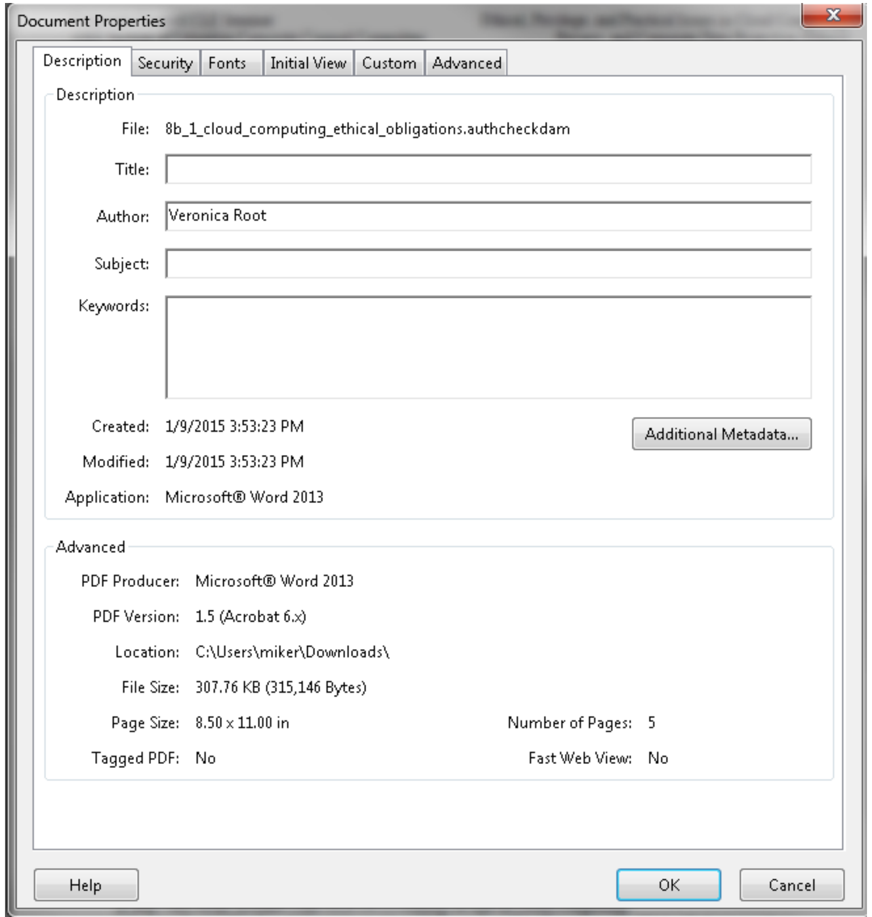
Before engaging a backup provider, law firms should ask these basic questions:

- Who is the vendor, how long has it been around, and will if meet my needs now and in the future?
- Where and how will my data be stored?
- Who can access my data?
- Is my data still mine after I store it on the vendor’s cloud server?
- What are my terms of service and will the vendor agree to provisions that protect my data?

9. Metadata



- Metadata
  - Metadata is electronic information about documents imbedded in the document, but not readily visible (who created the document, when it was created, edit history, and imbedded comments).
  - Metadata can be removed from documents before distributing electronically.
  - States agree that lawyers must use "reasonable care" to prevent unauthorized disclosure of confidential information through metadata, but do not agree regarding what constitutes reasonable care.



Description

File: 8b_1_cloud_computing_ethical_obligations.authcheckdam

Title:

Author: Veronica Root

Subject:

Keywords:

Created: 1/9/2015 3:53:23 PM

Modified: 1/9/2015 3:53:23 PM

Application: Microsoft® Word 2013

Advanced

PDF Producer: Microsoft® Word 2013

PDF Version: 1.5 (Acrobat 6.x)

Location: C:\Users\miker\Downloads\

File Size: 307.76 KB (315,146 Bytes)

Page Size: 8.50 x 11.00 in

Number of Pages: 5

Tagged PDF: No

Fast Web View: No

File Names, Indexes, and Keyword Searches

Indexes

- "Indexing" refers to searches of data and metadata (data about data) about a file that is used to identify its contents or categorization.

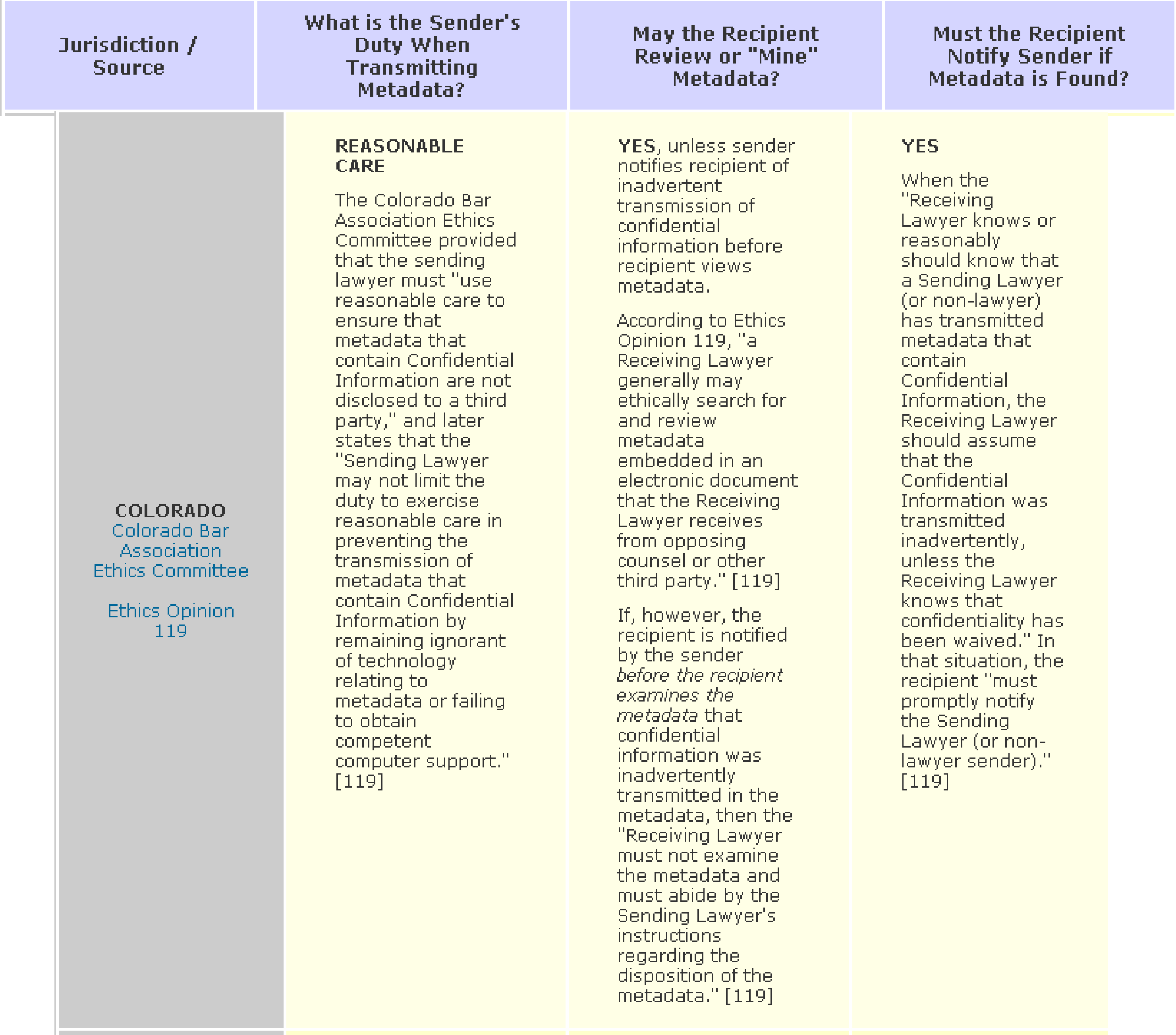
- Two different types:
  - Full-text
  - Field-based

File Names, Indexes, and Keyword Searches

Indexes

- Full-text indexing searches identify files by their actual contents.
  - E.g., the text of a file itself.

- Field-based indexing searches identify specific metadata about a file.



Jurisdiction / Source	What is the Sender's Duty When Transmitting Metadata?	May the Recipient Review or "Mine" Metadata?	Must the Recipient Notify Sender if Metadata is Found?
COLORADO Colorado Bar Association Ethics Committee Ethics Opinion 119	**REASONABLE CARE** The Colorado Bar Association Ethics Committee provided that the sending lawyer must "use reasonable care to ensure that metadata that contain Confidential Information are not disclosed to a third party," and later states that the "Sending Lawyer may not limit the duty to exercise reasonable care in preventing the transmission of metadata that contain Confidential Information by remaining ignorant of technology relating to metadata or failing to obtain competent computer support." [119]	**YES**, unless sender notifies recipient of inadvertent transmission of confidential information before recipient views metadata. According to Ethics Opinion 119, "a Receiving Lawyer generally may ethically search for and review metadata embedded in an electronic document that the Receiving Lawyer receives from opposing counsel or other third party." [119] If, however, the recipient is notified by the sender *before the recipient examines the metadata* that confidential information was inadvertently transmitted in the metadata, then the "Receiving Lawyer must not examine the metadata and must abide by the Sending Lawyer's instructions regarding the disposition of the metadata." [119]	**YES** When the "Receiving Lawyer knows or reasonably should know that a Sending Lawyer (or non-lawyer) has transmitted metadata that contain Confidential Information, the Receiving Lawyer should assume that the Confidential Information was transmitted inadvertently, unless the Receiving Lawyer knows that confidentiality has been waived." In that situation, the recipient "must promptly notify the Sending Lawyer (or non-lawyer sender)." [119]

Paperless Estate Planning Office Resource Materials

- ABA Legal Technology Resource Center, at http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/paperless.html. This resource includes various articles and practice resources. The Tech Overview and Charts page is at http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis.html.
- Paperless in One Hour for Lawyers, ABA Law Practice (book) (2014)
- ABA, Paperless for Lawyers, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/paperless.html
- Paperless in 12 Steps (2012), Adriana Linares, http://www.lawtechnologytoday.org/2012/06/paperless-in-12-steps/ (good paper on paradigm shifting in your office)
- How to Save Money Now by Going Paperless, Molly DiBiana, at http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/may11/how_to_save_money_now_by_going_paperless.html
- Corporate Compliance Series: Designing An Effective Records Retention Compliance Program, J. Edwin Dietel (2014)
- Joe the Lawyer Goes Green, Kathryn Smith, Chicago Bar Association Record, 23 APR CBA Rec. 46 (2009)
- The Practical Paperless Office, Jan. 2008 Colo. Lawyer at 55
- Can You Set Up a Practice on a $1000? Going Solo Without Breaking the Bank, Nerion Petro, 87 Nov Wis. Law 55 (2014)
- The Lawyers Guide to Adobe Acrobat (3d Ed.) 2012, ABA, David Masters
- Metadata opinions: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html
- Cloud ethics opinions: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html
  - Also see article at http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2015_corporate_counselcleseminar/Materials/8b_1_cloud_computing_ethical_obligations.authcheckdam.pdf

For further information, contact us:

Michael W. Reagor, Esq.
Dymond • Reagor • Colville, LLP
The Edward Building, Suite 1040
Greenwood Village, CO 80111-2922
mreagor@drc-law.com