If you found out you had a data breach would you know what had been information had been accessed and if it triggered a statutory requirement for notification? Do you know what records in your firm need to be kept, which need to be destroyed? The only way to enforce policies on record retention, security, business continuity, incident response and plan for succession is to first understand what data you have, what format is it in, where is it stored, and who should have access to it. We will walk through the concept of information governance and how to start mapping your firms data as an essential step in truly managing and protecting the firm and its clients.

Mapping Your Data for Retention, Succession and Security

Catherine Sanders Reach, Director
Law Practice Management and Technology
The Chicago Bar Association

DOWNEY LAW GROUP LLC

Originally printed in the July 2016 *St. Louis Lawyer*

Eleven Tips for Managing and Protecting Client Records

By Michael Downey

Two recent developments in legal ethics may impact how lawyers handle client-related information. First, the Missouri Supreme Court adopted amendments effective July 1, 2016, to the Missouri Rules of Professional Conduct that regulate lawyers' handling of client-related and trust-account records, Rules 4-1.15 and 4-1.22.

Second, the Missouri Office of Chief Disciplinary Counsel and other states' bar counsel have warned lawyers that certain emails appearing to come from disciplinary counsel in fact do not, but may instead contain Cryptolocker-type computer viruses or malware.

In light of these recent developments, I offer eleven tips relating to the handling of client records.

1. The client still owns the entire file. Missouri law has long recognized that the client owns the client file – including attorney work product "from cover to cover." *In re Cupples*, 952 S.W.2d 226, 234 (Mo. banc 1997). The new amendments to Rules 4-1.15 and 4-1.22 do not alter this basic principle.

2. The client decides what lawyer gets the original file. Missouri law provides that, upon request, a lawyer must give a client the client's original file. The lawyer generally may keep a copy, but must do so at the lawyer's own expense. The sole recognized exception is materials for which the lawyer has paid a third party (such as court transcripts, investigative or expert reports, and the like), and for which the client has not yet reimbursed the lawyer.

3. Trust-account related records must be kept six years. Rule 4-1.15(f) creates a similar six-year retention requirement for trust account-related records. The six-year period, a one-year year increase from the prior trust account record retention period, runs from the later of "termination of the representation" or the "date of the last disbursement of funds."

Rule 4-1.15(f) contains detailed specifications of the records that must be kept for a minimum of six years. These records include at minimum: (1) receipt and disbursement journals; (2) client-specific ledgers; (3) fee agreements and similar documents; (4) accounting statements showing disbursements made; (5) bills and expenses sent to clients; (6) disbursement records; (7) check-book registers and bank statements or the equivalents; (8) electronic transfer records; (9) account reconciliations; and (10) credit-card transaction information.

The six-year period for maintaining trust-account related records may not be shortened by an agreement with a client.

4. Other client-related records must be kept six years, unless the client agrees to a shorter period. The July 2016 amendment to Rule 4-1.22 establishes that client-related records must be held for a six-year period, for client files closed after July 1, 2016. Unlike the six-year period for preserving trust-account related records,

however, this six-year period may be shortened by agreement.

Rule 4-1.22(a) states that, for client engagements that end after July 1, 2016, client files must be retained "six years after completion or termination of the representation absent other agreement between the lawyer and client through informed consent confirmed in writing." "If the client does not request the file within six years after completion or termination of the representation, the file shall be deemed abandoned by the client and may be destroyed." *Id.*

Client files from engagements that terminate prior to July 1, 2016, must – consistent with the prior version of Rule 4-1.22 – be kept 10 years, unless the client had agreed otherwise. *Id.*

5. To shorten the period for retaining client records, the lawyer must obtain "informed consent confirmed in writing." Rule 4-1.22(a) provides that an "agreement to diverge from this default six-year requirement may be made" for retention of client-related records. To exercise this option for shorter retention, Rule 4-1.22(a) instructs, the lawyer must obtain "informed consent confirmed in writing." This consent may be obtained "at any point during the six years after completion or termination of the representation." Also, the writing memorializing consent to destruction must be kept for six years after the representation ends.

6. Records may be kept in electronic format. This six-year period for both trust-account and client-related records may be satisfied by keeping the client file – except items of intrinsic value – in an electronic format, as long as electronic record is "readily accessible" to the lawyer. Rule 4-1.22 requires items of "intrinsic value" to be properly preserved, as explained in more detail in Tip #7 below.

Likewise, Rule 4-1.15(f) permits lawyers to keep trust-account related files by electronic means. "Client trust account records may be maintained by electronic, photographic, or other media provided that they otherwise comply with Rules 4-1.145 to 4-1.155 and that printed copies can be produced. These records shall be readily accessible to the lawyer."

Preserving client information electronically is also addressed in Missouri Formal Opinion 127 (2009).

7. Items with intrinsic value should be preserved. Rule 4-1.22 states that items of "intrinsic value" shall not be destroyed. They shall be preserved, or as appropriate turned over to the state as lost property.

The Missouri Bar has previously identified original promissory notes, stock certificates, personal property, and valid wills as examples of items with intrinsic value.

8. Pending litigation or an investigation prevents record destruction. Rule 4-1.22(a)-(d) states that a lawyer shall not destroy a client file if the lawyer knows or should know there is a pending malpractice claim, lawyer discipline or criminal investigation, or other litigation related to the file. Rule 4-1.15 lacks a similar warning, but a prudent lawyer would likely hold onto any records relating to a file under investigation or embroiled in litigation, until that investigation or litigation ends.

9. Back up files frequently. Lawyers should also back up client- and trust account-related records frequently, through an easily accessible backup system. This tip may seem out of place, but frequent backups are often (along with user education) among the best means for avoiding costly ransoms associated with Cryptolocker-type computer viruses. If

a lawyer has a recent back-up, the lawyer may use this backup instead of paying a ransom or otherwise trying to unencrypt files encrypted by operation of a Cryptolocker-type virus.

10. Maintain confidentiality when destroying records. Missouri has not yet adopted a version of ABA Model Rule 1.6(c), which requires lawyers to protect client-related information from inadvertent disclosure. Nevertheless, lawyers should take steps to ensure they maintain confidentiality when they are storing and destroying client-related information.

Failure to protect confidentiality at any point, including preservation and destruction, may constitute a violation of fiduciary responsibilities, even if such conduct does not (yet) violate an express requirement in Missouri's legal ethics rules.

11. Dissolving firms should account for client records. Rule 4-1.15(f) directs lawyers to consider preservation of trust account-related records when dissolving a law practice. Rule 4-1.15(f) states:

> Upon dissolution of a law firm or of any legal professional corporation, the partners shall make reasonable arrangements for the maintenance of client trust account records. Upon the sale of a law practice, the seller shall make reasonable arrangements for the maintenance of client trust account records.

Rule 4-1.22 lacks a similar mandate regarding the handling of client files when a lawyer firm dissolves. Nevertheless, experience teaches that lawyers should consider establishing resources to address client files should a law firm dissolve or close unexpectedly.

Michael Downey is a legal ethics lawyer at Downey Law Group LLC. He has taught legal ethics at Washington University and St. Louis University, chaired the ABA Law Practice Division, and testified as an expert witness in proceedings pending in Missouri, Illinois, and Kansas. Reach Michael at 314-961-6644 or mdowney@DowneyLawGroup.com.

Chicago Bar Association &
Chicago-Kent College of Law
present

Document Management and Retention Policies for Clients and Law Firms

February 15, 2008

Lawyer As Manager

- Protect the firm/business from liability/risk
  - Ensure the law firm adheres to ethical obligations
- Protect firm/business intellectual assets
- Educate partners and employees
- Ensure productive business processes
- Manage cost
- Manage firm resources effectively

Lawyer As Manager Must Manage IT Resources

- Size does matter
  - Small Firm – May be able to do it yourself
  - 1-15 – Utilize professional services company
  - 15+ - Staff and/or Outsource
- Land Line Phones, Computers, Printers, Firewalls, Anti-virus/spam, Cell Phones, E-mail, Document Production (DMS?), Legal Research, Accounting, Paperless, Forensics, and more

Major Distinction Between Client And Lawyer Records Obligations

- Client owns its records
  - Can make policy and business decisions without considering outside interests
- Lawyer has obligations to the law firm AND the client
  - Law firm records management program must
    - Protect the firm and manage firm resources
    - Support the lawyer's ethical obligations to clients

Model Rules Used As Ethical Basis For Law Firm Records Management

- 1.1 Competence
- 1.4 Communication
- 1.6 Confidentiality
- 1.15 Safekeeping Property
- 1.16 Declining or Terminating Representation
- 5.1 Resp. of Partner or Supv. Attorney
- 5.3 Resp. Regarding Nonlawyer Assistants

- American Bar Association, *Model Rules of Professional Conduct, 2007 ed.*

Categories of Records (94-13)

	Category	Duty
1	Documents and other materials supplied by the client	Return upon reasonable request (1.15b)
2	Correspondence between lawyer and client	Provide on an ongoing basis (1.4)
3	Correspondence between lawyer and third parties	Provide on an ongoing basis (1.4)
4	Copies of pleadings, briefs, applications prepared by the lawyer and filed with courts or other agencies on the client's behalf	Provide on an ongoing basis (1.4)
5	Intrinsically valuable documents	Provide on an ongoing basis (1.4)
6	Firm administrative materials (conflicts checks, time records, credit checks	No duty to provide access under the rules. Not client property
7	Lawyer work product – notes, drafts, internal memoranda	Significant controversy, but believes materials are property of lawyer.

Client Notice of Retention Policies

- Engagement Letter:
  - Language re the firm's records management and retention policies
  - Client must keep attorney aware of location
  - Electronic records may be kept in lieu of printed records
  - Return of client's property at the end of the matter
  - Client's right to request other portions of the file
- Should the firm send additional notice:
  - At the end of the matter (when the retention period is assigned?)
  - At the end of the retention period, when the records are eligible for disposition?

Core Requirements for Compliant Records Management

- Good Policies and Procedures
- Executive-Level Program Responsibility
- Proper Delegation of Program Roles and Components
- Program Communication and Training
- Auditing and Monitoring to Measure Program Compliance
- Effective and Consistent Program Enforcement
- Continuous Program Improvement

From: Information Nation: Seven Keys to Information Management Compliance by Randolph Kahn and Barclay Blair

In Addition also consider…

- Legal Holds process
- Tax Holds notification

Good Policies and Procedures

- Over-riding policy (i.e. has consequences) statement
- Definitions
- Process documentation
- Records retention schedules

What is a Record?

- **Record -** A “record” is any recorded information that has value to the company for conducting its business or meeting its legal obligations. This includes information created or received in any form, including e-mails, paper documents, electronic documents, database or application information, and other electronic or photographic media.

Critical Definition Elements

- Must be media-agnostic
- May delineate between client and firm records
- May extend to outsourcer records
- Inclusive of all employees, agents, contractors

Proper Delegation of Program Roles and Components

- Records officer / records manager
- Records management council / committee
- Records champions
- Records coordinators
- Records staff
  - Analysts, divisional records managers, records center staff, etc.

Strategy / Design Layer

- Generally, the Records Manager or Records Officer
- Will make policy, determine program outcomes
- Has accountability for program compliance and success
- Generally should not be outsourced
- Also includes Records Management Committee

ARMA RIM Core Competencies Level 4

Process / Build Layer

- Generally, a Records Analyst
- Can also be the Records Operations Manager
- May include the “Records Champions”
- Can be outsourced
- Designs, communicates processes to manage records in the organization
- Provides operational direction

ARMA RIM Core Competencies Levels 2 / 3

Delivery / Run Layer

- Records staff
  - Can include departmental designates who manage records (“Records Coordinators”)
  - Can include full-time records center staff
- Often outsourced
- Primary tasks are managing physical records, indexing, storing and retrieving

ARMA RIM Core Competencies Level 1

Program Communication and Training

- Generally, all lawyers, employees and contractors should be required to have some sort of records management training
- At minimum, this should be training on the policy and basic responsibilities
- Communications should be regular and planned

Communications

- Timing is everything

"Mike -- It might be useful to consider reminding the engagement team of our documentation and retention policy."

-- Nancy Temple to Michael Odom, October 12, 2001

Auditing and Monitoring to Measure Program Compliance

- Develop an approach to ensure that employees, agents and contractors are following the records management policy
- This can be made part of process audits
- You can require annual compliance certification – and then spot check

Effective and Consistent Program Enforcement

- As with any policy, it needs to be enforced consistently
- If non-compliance can result in employee discipline, then that action must be taken
- BUT, ensure that employees have the correct tools to comply

Continuous Program Improvement

- Measure progress
- Find bottlenecks
- Look for opportunities to reduce cost or improve cycle time
- Add technology where it makes sense
- Legal Review

Legal Holds

- A critical element of the program must be a process that ensures notification all employees, agents, and contractors whose records may be subject to litigation
- People must be held accountable for destruction of records on legal hold
- Give consideration to creating hard drive images very early in the hold process and securing those drive images

Tax / Audit Holds

- Similarly, ensure that employees are aware of the need to retain records for tax or financial audits that are ongoing beyond the normal retention period

Holds

- For all holds, ensure that you have a mechanism to “flag” records on hold that are stored offsite.
- Ensure that the holds are released when no longer required

Example From Foley File Plan

	Category	Filing Rule	Alternative
1	AFFIDAVIT	A sworn statement, in writing, sometimes signed by a notary. Any signed Affidavit.	
2	AGREEMENTS	Any signed agreement between one or more parties.	Could also file into a Contracts insert.
3	AMENDMENTS	Amendments to agreements or contracts	
4	ASSIGNMENTS	Examples: Assignment Agreement, Assignment of Rents, Collateral Assignments, etc.	
5	ATTORNEY NOTES	Notes taken by the attorney or legal assistant during the matter.	
6	ATTORNEY SPEECHES, ARTICLES, CLASSES	Any materials generated during professional activities such as speaking, writing, teaching or taking classes	
7	AUDIT REQUEST	Materials generated re response to an audit letter request.	

Retention Schedules

- Define the various types of records scheduled
  - Official, convenience, non-record
  - Short term retention for non-official records
- Define active (onsite) and inactive (offsite) retention periods
- Define conditions for starting the retention period (after creation, after termination, after litigation closed, etc.)
- Define disposition (return to client, destroy, make available to historical archives, etc.)
  - Electronic records
  - Printed records

Retention Research

- Consider:
  - Laws and regulations
    - Professional guidelines
  - Fiscal / tax / audit requirements
  - Operational or business requirements
  - Historical value
- Tools: Subscription services, records management consultants, some law firms
- There is no “magic” solution. Competent legal and / or records professionals within the organization need to review and approve the retention schedules.

Retention Exceptions

- Holds (legal and tax / audit) may require records to be maintained longer than retention period
- Shortened Retention
  - Non-disclosure agreements
  - Confidentiality
  - Court Orders
- Lengthened retention periods
  - What other scenarios justify keeping records longer than the schedules define?

Retention and Disposition Periods

- How are the periods applied to different types of records?
- Law firms use different methods:
  - Apply a default period to all files
  - Apply a default period to all files, with certain exceptions
  - Define different periods for areas of law
  - Define different periods for different document types
- Non law firms apply retention periods to *records series*
  - Examples: Accounts receivable, lab notebooks, quality assurance records

Sample From Foley Schedule – Representation Records

- Files are scheduled for disposition at the end of a matter
- The default retention period is 10 years
- Exceptions
  - Certain areas of law are kept longer
  - Files that contain specific document types are kept longer
  - Retention periods can only be shortened with a court order to destroy or an obligation to comply with confidentiality agreement
  - Other than the scheduled periods, the only reason to extend a retention period is if the records are under a hold
  - If there is a document hold in place, the schedule keeps running, but destruction activities are suspended

Sample From Foley Administrative Schedule – Similar to Client Schedule

MATTER TYPE (AREA OF LAW)	DESCRIPTION OF RECORDS ASSOCIATED WITH THIS MATTER TYPE	TRIGGER EVENT	LEGAL RETENTION REQUIREMENT	TOTAL RECOMMENDED RETENTION
ACCOUNTING/ TRUSTS	Check copies, trust receipts, disbursement records of funds received or owed to the firm,	Fiscal year end	7 Fiscal Years **26 USC 6501**	7 Fiscal Years
ACCOUNTS PAYABLE	Invoices for goods and services purchased by the firm; includes authorization for payment and documentation that payment was made. Includes expenses requiring special approval (travel and entertainment)	Fiscal year end	7 Fiscal Years **26 USC 6501**	7 Fiscal Years
ACCOUNTS RECEIVABLE	Documentation of funds receivable including, notated pro formas and documents that support billing to clients; honorariums, refunds, employee personal charges, and lists	Fiscal year end	7 Fiscal Years **26 USC 6501**	7 Fiscal Years
ANNUAL REPORTS (REVIEWED)	Annual reports created and certified by an outside auditing authority	Fiscal year end	7 Fiscal Years **26 USC 6501**	7 Fiscal Years

Disposition

- If records are to be destroyed, ensure that they are completely destroyed in all forms – don't just let employees drop the documents in the waste basket
- Document the disposition
  - A form or other documentation should indicate:
    - Who approved and performed the disposition?
    - When were the records disposed of?
    - What records were disposed of?
    - How much material and what time range was disposed of?

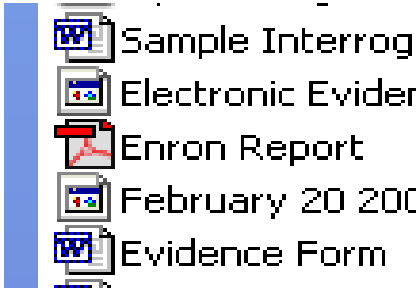
Technology

- Take backup systems into account
  - Are backup systems
    - Records repositories
    - Disaster recovery systems
  - How long does information live on backup before it is overwritten
    - Limit the number of backups created and the length of time information is stored

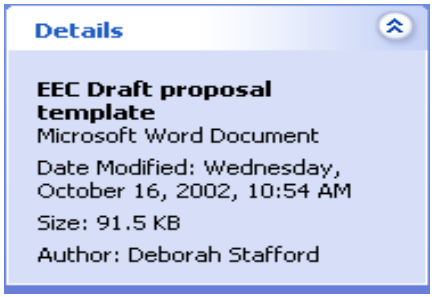
Accessible vs. Inaccessible Data?

Active Data

Inactive Data



Files in Use



Meta-data

Deleted Files

Back-Up Tapes

Other Considerations

- Attorney Mobility
  - Incoming
    - Records moved into approved repositories
  - Departing
    - Classification for work they take with them (Emails, documents, shared drives, etc.)
- Employee Departures
  - Emails, documents
- Telecommuting and Home Offices
  - What should / shouldn’t be maintained outside the office
  - What happens if records are maintained on personally-owned resources

Outsourcing Impacts

- IT – motivations to keep or dispose
- HR and Benefits – who owns the records?
- Real Estate and Facilities – who manages the records?
- Accounting – who owns the records?
- Records Management – who has accountability and liability?

A Word on Email…

- Email is a medium of storage
- Retention of email should be based upon content; clearly, email that has no record value need not be retained
- You would set a retention period for “email”, no more than you would set a retention period for “paper”

* The exception to this would be broker-dealers where all forms of communications of “business as such” are explicitly required (under SEC and NASD rules) to be retained for at least three years.

Beware Technologists Bearing Cheap Storage

- Many technology folks are touting an approach of “retain everything – storage is cheap”
- Very often, keeping records too long is as damaging as keeping records for too short a period of time
- And with increased storage volume comes increased e-discovery costs
- In addition, if electronic records are maintained “forever”, the disposition of hard copy records may be questioned in court
- And how will you access those records in the future – who will ensure that the information migrates to current software?

Compliance Considerations

- Law firms must comply with:
  - Rules of Professional Conduct
  - Court rules and procedures
  - Evidentiary rules
  - Statutes
  - Fiduciary duties
  - Case law and other authorities
  - Client needs
    - Don’t keep records past retention period as it may jeopardize client interests

The Next Steps

- Separate document management function
- Document retention program, not just policy
- Manpower
- Training
- Audits

Technology

- Document Management System (DMS)
  - Stores work in progress documents in native format
  - Allows team collaboration on documents
  - Requires metadata profiling
    - Client = records series, document type, and title
    - Law Firm = client/matter number, document type, and title
- Records Management System (RMS)
  - Stores the file plan and retention schedules
  - Catalogs physical records holdings
    - Index of file folders for a file

Technology

- Concept – Records Repository
  - A single location for all records for a file
  - Allows easy retreivability
  - Allows easy application of retention period
- Both DMS and RMS systems can function as repository for e-records
- There is a trend to see DMS vendors purchase RMS vendors to combine distinct functionality into a single application

Litigation Preparedness & ESI Considerations

- Scope of Request
  - We recommend getting a forensically sound copy of the entire hard drive. Data can be searched for part numbers, accounting information etc.
  - Use of Document Review Technology (LAW)
- Use of Specialized Software to get Data
  - Encase, Parabin, Access Data
  - Search e-mail? Search Documents? Search Accounting Records?
- Use of 3rd party to do investigative work
  - RGL Forensic Accountants
- Expensive!!!
  - Minimum acquisition costs of $3-$5,000
  - Accounting Review of MFG (25 million gross) company $50,000
  - Search Review $5,000 - $15,000 for keywords

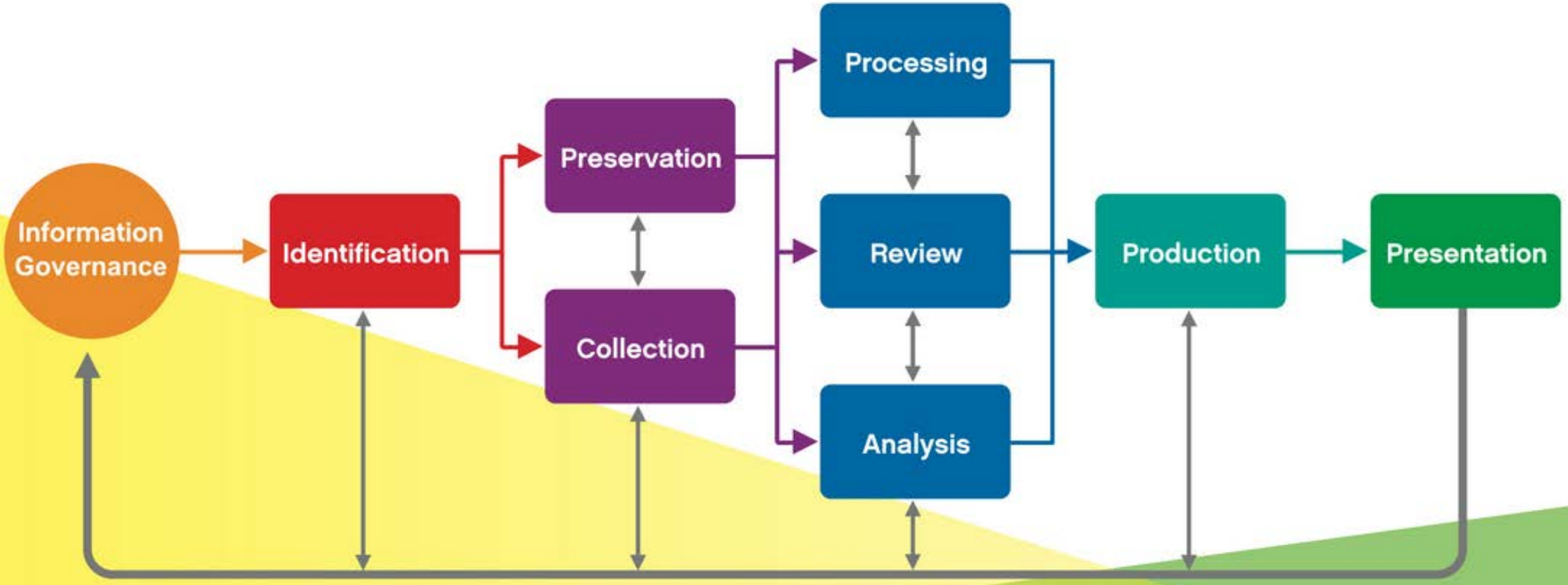
Technology Obsolescence

- Software/hardware
- You must keep an old version (or even an old computer) in order to run the software for old records. Example – if you have a Wordstar file, you may need to keep an old version of Wordstar. If you have an old accounting system, you may need to keep an old accounting computer until enough time passes for your retention policy to get rid of the information.
- Backup Tape Software – This is an expensive problem if you don't have the hardware and software to recover files from an old tape backup system.
- If you change from Windows to MAC anything not converted over to the new system may need to be kept on one or two computers (accounting systems are usually specific to the operating system)

QUESTIONS?

Document Retention in Law Firms

Electronic Discovery Reference Model



VOLUME

RELEVANCE

Electronic Discovery Reference Model / © 2014 / v3.0 / edrm.net

Information Governance

- Records Management
- Document Retention Policies
- Relevant governing laws

Where is the data?

- Desktops/Laptops
  - Company issued vs personal
- Email
  - Company issued vs personal
  - Corporate emails or 3rd party hosted
- Chat or Messaging system
- File Servers
- File Cabinets/Desks/Drawers/Briefcases
- External Drives/Shared Drives/Jump Drives
- Cell Phones/Tablets
- Back-up systems
- Industry specific documents
- Company specific documents

Implement a Process

- Set Up a Defensible Process
  - Locate the data
  - Decipher the types of data
  - Document how long each type of data will be retained
  - Implement the documented retention plan

Once you have Implemented a Process…

- Ensure Compliance
- Be prepared for exceptions (Legal Hold, Internal Issues)
- Amend Automated Document Retention when needed
- Revisit annually to check for necessary updates

What I am doing is working, why change?

- Data Privacy
  - You have an obligation to protect your client's files. The longer you keep them, the higher the risk of breach.
  - Traditionally, law firms do not have state-of-the-art security. They can be an easy target for hackers.
  - Breaches lead to expensive remediation and upset clients.
- Cost
  - Storage
    - Physical and electronic
  - Litigation
    - Similar to corporate litigation, the more data you keep, the more expensive it is.

DLA Piper v. Adam Victor

- DLA sued Victor when he did not pay his bill ($675,000).
- Victor filed a counterclaim saying that he was billed too much.
- Victor was able to discover emails supporting his allegation.
  - “I hear we are already 200k over our estimate—that’s Team DLA Piper”
  - “churn that bill, baby!”

See: http://www.abajournal.com/news/article/sued_by_dla_piper_for_675k_ex-client_discovers_lighthearted_churn_that_bill/

Scott Martin v. Andrews Kurth LLP

- Martin was involved in a business dispute and hired Andrews Kurth.
- Andrews Kurth drafted a settlement agreement and sued for enforcement of the agreement.
- The settle agreement was held to be unenforceable on appeal.
- Martin brought suit for breach of fiduciary duty (and other counts).
- Martin used several internal emails from the firm as evidence.
- Jury awarded $167M in compensatory damages and $29M in attorney fees.

See: http://www.texaslawyer.com/id=1202742916570/Andrews-Kurth-Hit-With-Nearly-200M-Verdict?mcode=0&curindex=0&curpage=ALL

Changes to the FRCP

- Rule 37(e) – Failure to Preserve
  - ESI that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery
  - The Court can:
    - Upon finding of prejudice, may order measures no greater than necessary to cure the prejudice; or
    - Upon finding intent to deprive, may:
      - Presume the lost information was unfavorable to the party;
      - Instruct the jury that it may or must presume the information was unfavorable; or
      - Dismiss the action or enter default judgment

Additional Resources:

Elements of a Good Document Retention Policy
http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_WP_ElementsOfAGoodDocRetentionPolicy.pdf

Records Retention in the Private Legal Environment: Annotated Bibliography and Program Implementation Tools
http://www.aallnet.org/mm/Publications/llj/LLJ-Archives/Vol-93/pub_llj_v93n01/2001-01.pdf

Record Retention Obligations: Acing The Audit
https://www.isbamutual.com/liability-minute/record-retention-obligations-acing-the-audit