INFORMATION REQUIREMENTS CLEARINGHOUSE

Legal Requirements for Records and Information Management Programs – Questions & Answers

February 23, 2016

Donald S. Skupsky, JD, CRM, FAI, MIT
President and CEO
303-721-7500
dskupsky@irch.com

Questions

- Electronic Imaging (7)
- Retention – Accounting (5)
- The Three-Year Presumption (2)
- Retention Program Implementation & Compliance (14)
- Privacy v. Record Retention (2)
- Litigation Protection (2)
- Information Governance v. Records and Information Management (2)

Electronic Imaging & Reproductions

- Will courts accept electronic images?
- When are paper records required or preferred?
- When can you destroy paper after reproduction?
- Have there been any changes to ESIGN?

Court Acceptance of Electronic Imaging

- Electronic images are 100% admissible in United States courts. No exception.
- Original records can be destroyed after reproduction . . . and quality control.
- If the original records exists, the other party can request them.
- Reproduction may continue after litigation begins; but relevant originals cannot be destroyed.
- No court has ruled electronic imaging not OK; courts have ruled reproductions OK w/o mentioning imaging

The Basis for Legal Acceptance of Electronic Imaging

- Uniform Photographic Copies of Business and Public Records as Evidence Act (UPA)
  - Uniform Business Records Act – US Federal Govt.
- Uniform Rules of Evidence (URE)
- Uniform Electronic Transaction Act (UETA)
  - ESIGN – US Federal Government
- Uniform Records Retention Act – 8 states
- Other state laws and court rulings on reproductions

Retention of Original Paper After Reproduction

- Original records required by law
- Records with intrinsic value: stock certificates, bonds, cash, negotiable instruments
- Documents for which the original signature or handwriting may be significant -- e.g., wills
- Promissory notes including federal mortgages, HUD loans. Not student loans. Check specific requirements.
- Optional: Documents of high value – e.g., contracts over $10 million

ESIGN – Electronic Signatures in Global Networks

- Adopted 1999 by US Federal Government and many other countries
- Similar to UETA except related to electronic signatures and documents in international commence
- Would allow electronic imaging; electronic records
- Would defer to UETA provisions if conflicts

Applying Retention to Accounting Records

- How long should accounting records be kept?
- How should we handled records of net operating losses (NOL)?
- How should we apply tax holds?

Retention Requirements for Accounting/Tax Records

- 5 states: 6-year legal requirement from end of fiscal year
- IRS/States: Limitation of assessment from tax return due date or filing
  - General: 3 years
  - Understate gross income by 25% or more: 6 years
  - Fraud/willful tax evasion: forever
- IRS/States: capital gains, loss, depreciation. ACT+?: while tax event current + normal tax period

Net Operating Loss (NOL)

- How create NOL
  - Organization has loss from business activity
  - Loss not fully offset by profits/gains in tax year
  - Carry loss forward and write off in future years until full amount written off
- Recordkeeping implications
  - IRS can audit the tax year when the original loss incurred, if you recognize a loss carry forward in a year still subject to audit
  - IRS can only change loss carry forward during audit (3 years) but can re-determine the original loss amount
  - Need ALL records of tax year of original loss until loss carried forward is written off plus normal retention period

Accounting Retention Summary

- 6 years: General Accounting – payables, receivables, payroll
- ACT+6: Capital Accounting – property, investments
  - ACT: Keep capital records until property sold, scraped, depreciation ends, etc.
- Net Operation Loss.
  1. ACT+3 or 6: keep ALL records of year loss originated until loss carry forward no longer claimed, OR
  2. Place audit hold on loss tax year until loss written off
- MAX3: Accounting Management Reports

The Three-Year Presumption – An Update

- Records that are required by law to be kept
  - No retention requirement period exists
  - Records can safely be destroyed after three years
- Basis:
  - Uniform Preservation of Private Business Records Act / Uniform Records Retention Act: CO, GA, IL, MD, ND, NH, OK, TX

Unless express provision is made by law for the period during which they must be preserved or for the condition upon which they may be destroyed, business records which persons by the laws of this state are required to keep or preserve may be destroyed after the expiration of three years from the making of such records without constituting an offense under such laws.

The Three-Year Presumption – An Update

- US Federal Paperwork Reduction Act: 5 CFR 1320.5(d)(2)(iv). [Note: Citation change]
- A US Federal regulation with a retention period of more than three years is not enforceable unless the retention period ("collection of information") is approved by OMB
- When an agency develops a regulation but does not state a retention period, OMB does not approve and not enforceable

> (d) * * *
>
> (2) Unless the agency is able to demonstrate, in its submission for OMB clearance, that such characteristic of the collection of information is necessary to satisfy statutory requirements or other substantial need, OMB will not approve a collection of information-
>
> * * * * *
>
> (iv) Requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records, for more than three years;

- Otherwise, keep records for a "reasonable period"

Records Retention Program

- How often should we review and update program?
- How can we stay informed of changes in the law?
- What is needed in the retention program to withstand a legal challenge?

Retention Program Implementation & Compliance

- How can we get people to comply?
- How should custodians throw away records?
- How should we set up the records retention audit?
- How can we apply retention to records in the cloud?

Records Retention – Compliance and Legal Challenge Protection

- Program must be systematically developed
  - Comprehensive legal research
  - Full coverage of records of organization
  - Program reviewed/updated at least annually
- Program must be systematically implemented
  - Destruction performed under retention program
  - Audit to confirm compliance
  - “Coercion” to force compliance
- Program and implementation documented

Legal / Audit Holds

- Legal holds operate independently of the retention program
- Identify records / documents subject to pending or imminent litigation, government investigation and audit.
- Place "holds" to prevent destruction (even under Retention Schedule)
- Manage "holds" – creation, update, removal
- Permit destruction when "holds" removed

Approval of Destruction

- Authorization of Destruction
  - Not recommended
  - Require specific approval
- Notice of Destruction
  - Provide listing of records for destruction
  - Request exceptions – rarely approved
  - Records being held not candidates for destruction
- No Notice or Approval
  - Recommended when hold system in place
  - Results is most consistent retention

Privacy v. Records Retention

- Definition (rough)
  - Privacy: Protection of personal and personally identifiable information (PII)
  - Records Retention: The period of time for keeping records
- Impact of Privacy on Records:
  - Privacy laws may limit the period to keep records
  - Retention laws set the minimum you must keep records
  - May sometimes be incompatible

Applying Records Retention in the Cloud

- First apply records retention on earth
- Retention program should apply to records wherever they reside, regardless of form
- Implement retention program in your cloud application . . . or don't put them in the cloud!
- Service provider must provide retention capabilities that you can apply to your records
- Check service provider destruction/backup practices. When you destroy they must destroy!

Litigation Protection & Rule 26. Federal Rules of Civil Procedure

- Manage records and information
  - Know what records/information you have
  - Know where it is stored
- Develop and implement a legally-defensible retention program
  - Know what you don't have
  - Know that you destroyed records/information properly
  - Can demonstrate compliance with program - audit

Information Governance v. Records and Information Management

- Definitions (rough): Wikipedia
  - Information Governance: the set of multi-disciplinary structures, policies, procedures, processes and controls, implemented to manage information at an enterprise level
  - Records and Information Management: the professional practice of managing the records of an organization throughout their life cycle, from the time they are created to their eventual disposal.

Information Governance v. Records and Information Management

- Both seek to manage the information of the organization
- IG includes more people, all systems, all information, all data -- entire organization
- RIM includes some records, little or no data, few systems, and the program is through the records management group, probably legal, and some cooperative parts of the organization.

Information Governance v. Records and Information Management

- RIM fully implemented would be a lot like IG today
- But:
  - RIM rarely got the full support of upper management and IT
  - RIM rarely controlled all information for the enterprise
  - RIM successfully managed some records, leaving many gaps; IG strives to manage all information
- Information Governance strives to encompass the entire organization and all its information

Thank You

INFORMATION REQUIREMENTS CLEARINGHOUSE

For more information:

Andre Cabral

Director of Sales & Marketing

303-721-7500

andre@IRCH.com