Pre-Litigation Risk Management: Record Retention

Stephanie A. "Tess" Blair
Morgan, Lewis & Bockius LLP

Introduction

Record management in a perfect world

- An organization will retain 3 buckets of records:
  - Legal Requirements (statutes, regs)
  - Business Need
  - Legal Hold
- Memorialized in a Retention Policy and Schedule
- Policy addresses electronically stored information
- Appropriate technology has been deployed to manage data retention
- Program includes compliance audits
Record management in a perfect world

- Record/Data Policies include:
  - Record retention policy and schedule
  - Legal Hold Policy
  - Data Storage Policy
  - Acceptable Use Policy
  - Disaster Recovery Policy
  - Information Security Policy

Reality is not so perfect

- Close to half of all US companies surveyed do not have a record retention policy
- Those that do report that the policy does not address electronically stored information
  - Source: 2007 Cohasset ARMA AIIIM Electronic Records Management Survey
- Estimates suggest that 95% of the information stored by US companies is junk

Yet...

- When failure to produce records in litigation is result of comprehensive and consistently enforced record retention program, program becomes a defense to claims of spoliation
  - United States v. Arthur Andersen, 125 S. Ct. 2129 (2005)
  - Park v. City of Chicago, 297 F.3d 606 (7th Cir. 2002)
  - Lewy v. Remington Arms Co., Inc., 836 F.2d 1104 (8th Cir. 1988)
  - Cf. Testa v. Wal-Mart Stores, Inc., 144 F.3d 173 (1st Cir. 1998)
<table>
<thead>
<tr>
<th>But...</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Failure to have a retention policy can provide evidence of spoliation</td>
</tr>
</tbody>
</table>


- "An organization should have reasonable policies and procedures for managing its information and records... The absence of a coherent document retention policy is a pertinent factor to consider when evaluating sanctions... Information management policies are not a dark or novel art. Numerous authoritative organizations have long promulgated policy guidelines for document retention and destruction."

### Proactive Record Management

### Lifecycle of a Record

- Creation
- Retention
- Destruction
**Creation**

- Employee Training is Key
- Training program should include:
  - Litigation Primer
  - Best Practices
  - Record Retention Program Implementation

---

**Creation**

- Litigation Primer
- Employees should know:
  - Litigants are generally entitled to all non-privileged potentially relevant records of the other party
  - Records include email and other electronically stored information
  - Organizations are obligated to produce records within the company's "possession, custody or control"
  - Such records include all records received, created or stored by employees including personal communications from corporate computers and corporate communications from personal computers
  - Note to Multinationals: the above is only. EU Data Protection law requires distinct policies for non-US operations
### Creation

**Best Practices Training Highlights:**
- Be scrupulously accurate
- Create documents that memorialize resolution of issues rather than debate or argue points
- Always include context for communication
- Limit preparation of critical evaluations to employees with responsibility for the function being evaluated
- Avoid editorial comment, rhetoric, conjecture, speculation, gratuitous characterizations
- Do not distribute documents indiscriminately
- Treat email as you would treat any other medium of business communication
- Do not use email for privileged or confidential communications

<table>
<thead>
<tr>
<th>Record Retention Program Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees should know:</td>
</tr>
<tr>
<td>- Importance of program</td>
</tr>
<tr>
<td>- Distinction between &quot;business records&quot; and &quot;records of transitory value&quot;</td>
</tr>
<tr>
<td>- How to store and discard business records in accordance with program</td>
</tr>
<tr>
<td>- Consequences of failure to properly retain records</td>
</tr>
<tr>
<td>- Sarbanes-Oxley Act of 2002</td>
</tr>
<tr>
<td>- Title 18 Obstruction of Justice</td>
</tr>
<tr>
<td>- Civil Penalties including adverse inference</td>
</tr>
</tbody>
</table>
### Retention

- All retention should be policy driven
- Policy should be designed to meet business needs and legal obligations
- Policy should be comprehensive, yet simple
  - Must address both electronic data and paper
  - Clearly state rationale for policy
  - Include retention/destruction schedules
  - Include an exception for litigation hold

<table>
<thead>
<tr>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Best Practices</td>
</tr>
<tr>
<td>- Create Taxonomy of “Records”</td>
</tr>
<tr>
<td>- Organize by functional area</td>
</tr>
<tr>
<td>- Tax, HR, Finance</td>
</tr>
<tr>
<td>- Interview representatives of each functional area</td>
</tr>
<tr>
<td>- Current business practices</td>
</tr>
<tr>
<td>- Nomenclature</td>
</tr>
<tr>
<td>- Rational deviations from statutory/legal minimum retention periods</td>
</tr>
</tbody>
</table>
| - Memorialize in Schedule

<table>
<thead>
<tr>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Best Practices</td>
</tr>
<tr>
<td>- Research laws and regulations applicable to each record type</td>
</tr>
<tr>
<td>- Develop retention/destruction schedules for each type</td>
</tr>
<tr>
<td>- Describe retention method</td>
</tr>
</tbody>
</table>
| • Beware of “off the shelf” policies and schedules
Retention

Caution:
- Do not use format to determine retention period
  - I.e. Delete all email after 45 days
- A policy ignored is worse than no policy at all
  - Develop a mechanism for auditing and compliance

Ensure regulatory compliance
- Records laws change slowly
- It is more likely that business practices will change
- Complete review of business lines
  - New lines of business have new requirements
  - Older lines of business may be beyond retention periods
### Destruction

- Documents must be destroyed "in the ordinary course of business" to be legally defensible
- One time destruction should be avoided
- **Destruction must be suspended for anticipated or pending litigation or investigation**

### Destruction

- Destruction Methods should minimize risk of:
  - Loss of confidential/trade secret information
  - HIPAA violations
  - Consumer protection/privacy violations
  - Identity Theft

### Hard Copy:

- Sensitive business and HR records should be destroyed by professionals
- Destruction should be certified
- Day to day destruction of business records should be done with shredders

### Electronic Records:

- Recycling and reformatting is preferred method for tapes and drives
- But it is virtually impossible to guarantee destruction
### Suspend Retention Policy

- Reasonable anticipation of litigation
  - Credible threat
  - More likely than not
- Release the hold and apply retention schedule
  - Certain that dispute is resolved
### Disparate data types

- Paper
- Email
- Loose Files (Office)
- Databases
- Instant Messaging
- Voicemail
- Website/Intranet
- Wikis, blogs, Web 2.0 content

### Questions

- Is it a Capital "R" Record?
  - Who decides?
  - Who owns it?
- If not, purge within prescribed timeframe
  - 60 days? 180 days? 2 years?
- If so, what is the prescribed retention period?
- Where is the Record to be stored?
- How can we find it again?
- How do we dispose of it when it expires?

### Current Array of Options

- Single retention period for all
  - Massive overretention
- Retention period by functional area
  - Difficult to implement without robust archiving capability and active management
- No retention (by definition)
  - Dangerous
- Auto-categorization
  - A dream in the making
Pre-Litigation Risk Management: Record Retention

Stephanie A. "Tess" Blair
Morgan, Lewis & Bockius LLP