“Early Bird” Session

REELING IN RECORD RETENTION REQUIREMENTS
TIPS AND COMMON MISTAKES

 Phillip A. Kilgore (Moderator) – Ogletree Deakins (Greenville)

 Bonnie L. Martin – Ogletree Deakins (Indianapolis)

 Marc L. Zaken – Ogletree Deakins (Stamford)
The management of recorded information has become a major burden for corporate America. This is particularly true when the recorded information takes the form of email, which seems to proliferate at exponential rates, and is a favorite target of both discovery and the attendant spoliation claims that threaten to take center stage in modern litigation. Given the potentially harsh sanctions which may be levied upon successful prosecution of a spoliation claim, there is just cause for concern.

However, forewarned is forearmed. Understanding the law of spoliation with regard to email can lead to the design of effective strategies that control risk.

I. The Law of Spoliation

The concept of spoliation is rooted in common law. It is the withholding, loss, alteration, or destruction of evidence relevant to a proceeding. Spoliation may be said to occur even in the absence of deliberate wrongdoing. However, the consequences of spoliation are generally determined based on a combination of two factors: fault and prejudice to the non-producing party.

Prejudice is shown simply by minimal proof that the withheld evidence was relevant. However, where a party destroys evidence in bad faith or with gross negligence, that bad faith or gross negligence alone may be sufficient circumstantial evidence that the missing evidence was unfavorable to the destroying party. When the spoiling party is merely negligent, then the innocent party must prove both relevance and prejudice in order to justify the imposition of a sanction.

Fault is a far more imprecise factor. As one court put it:

We have recognized that spoliation of evidence occurs along a ‘continuum of fault,’ from innocence through the varying degrees of negligence to intentional destruction. Likewise, a host of penalties may accompany the types of behavior manifested through this continuum.

How fault and penalty are associated along the continuum referenced by the court may vary significantly from one jurisdiction to another. In Nuvasive, Inc. v. Madsen Med., Inc., the Southern District of California reversed an adverse inference ruling and denied imposing any sanctions when a plaintiff failed to prevent the destruction of text messages requested by defendants. The court found that while the plaintiff was at fault for failing to enforce a litigation hold, there was no finding that the plaintiff intentionally failed to preserve text messages. Comparatively, the Middle District of Georgia in Oberry v. Turner imposed an adverse inference on a party for the loss of ESI yet no direct evidence of intent existed.

What is clear is that sanctions for spoliation can take many forms. On the milder end of the spectrum, the consequences of proven spoliation are ordinarily additional discovery (e.g., an opportunity to inspect a computer system or re-depose a witness after previously withheld documents are belatedly produced). More serious sanctions include awards of attorney’s fees and costs associated with the protraction of discovery (e.g., if repeated trips to the court were needed in order to ultimately obtain certain evidence), substantial fines, or the preclusion of certain evidence. The worst civil sanctions involve either adverse inference instructions (i.e., that certain information under the control of a party was not produced, and that the jury should assume the information would have been detrimental to that party) or outright default judgment. The Zubulake series ended with the former outcome – leading to the then largest verdict in a
single plaintiff EEO case; while a default judgment was entered as a sanction for spoliation in the much talked about case of Coleman Holdings, Inc. v. Morgan Stanley & Co.\(^8\)

Thus, to say that the successful spoliation claim can result in adverse decisions in cases that might otherwise have been won is no overstatement. But this is not the sole adverse effect. Whether or not successful, spoliation claims certainly divert a court’s (and the company’s) attention from the merits of a case. The fear of such claims has caused some companies to undertake extreme preservation practices such as saving all back up tapes. Such practices result in substantial ongoing costs to purchase an endless supply of tape and ever increasing storage costs. Even more significantly, such practices increase the costs of discovery, because the continuously growing store of information is subject to search for potentially relevant evidence and attorney review for relevance and privilege.

Especially in the context of employment cases, where the majority of relevant information is necessarily in the hands of the employer, spoliation claims become a powerful weapon in the hands of plaintiff’s counsel. The costs of preservation and discovery on a massive scale, backed by a threat of a spoliation claim for any misstep, create a substantial impetus to early settlement. Plaintiff’s counsel may also be able to use allegations of failure to preserve or produce potential evidence as a basis for directly accessing the employer’s computer systems. Once there, fishing expeditions are made simple.

There is no magic solution that can alleviate these concerns. However, there are steps that a company can take to improve its strategic position.

II. Putting the Corporate House in Order

In order to reduce the likelihood of a successful spoliation claim, a company should undertake the development and implementation of a litigation preparedness program. Such a program includes (1) well defined and enforced email usage and storage policies; (2) a comprehensive record retention program that fully incorporates email based on content; (3) limitations on mailbox size and automatic deletion functions that are based on sound assessments of business and legal defense needs; (4) backup policies that truly embrace a disaster recovery purpose; and (5) a robust litigation hold process. Some companies also find an email archive to be useful, or necessary, depending on their circumstances, and others benefit from advanced data mapping.

A. Email Usage and Storage Policies

Many email preservation and spoliation issues arise from the simple fact that companies take little or no control over their employees’ email use and storage habits. As a result, email proliferates, and even though it often houses critical company records, it is stored on a variety of platforms and media, most of which are under the user’s sole control.

The proper uses of email should be defined. If email is to be used for purposes more serious than conversation or general correspondence, centralized storage capacity should be developed. Any email that contains information important to the company’s business or operational decisions should be stored on a server, not an individual hard drive or portable media. At a minimum, the individual custodian should be required to store business email in a preordained fashion using a systematic protocol even if it remains under the user’s control. These simple steps would alleviate issues such as inconsistency in archiving practices, exclusive reliance on the attentiveness of individual employees to a request for the preservation
or production of relevant email, and the need to search through numerous and often unknown or forgotten stockpiles of email. *See Peskoff v. Faber; In re Kmart Corp.*

**B. Comprehensive Record Retention Program**

A general confusion often exists between policies relating to automatic deletion of email from active email accounts or backup media and record retention policies. The latter are designed to identify the recorded information the company needs to keep to satisfy its regulatory obligations, in addition to the recorded information the company wants to keep to meet its business and legal defense needs (collectively, "official records"). Record retention policies also mandate (or at least encourage) employees to discard all the remaining recorded information they generate or receive in a timely fashion, i.e., immediately upon determining that (1) it is not an official record, (2) it has outlived its immediate purpose, and (3) it has no presently identifiable future use. Record retention policies focus on the content of recorded information in distinguishing between official records to be kept for a predetermined period of time and transient materials to be timely discarded.

A record retention policy, properly implemented, adds a further layer of discipline on to the often haphazard email storage practices of employees. A policy assists employees in separating the wheat from the chaff, and establishes protocols for the retention of that which is important to the business. A record retention policy also may serve as a defense against spoliation claims as it justifies the non-existence of certain types of information. It also helps reduce information clutter by requiring the regular discard of unnecessary information. Finally, it serves as the backbone for any remediation program designed to eliminate outdated caches of recorded information, including email.

**C. Size Limits and Automatic Deletion**

Many companies impose size limits on accounts and implement automated deletion of email in the account based on aging. Both techniques are effective means of limiting the amount of email on hand, and may force employees to be disciplined about the management of their accounts. However, these techniques also create some spoliation risk. Size limits create risk because employees may delete potentially relevant email simply to reactivate an account. Education and careful deployment of litigation holds tend to overcome this risk. Risks as a result of auto deletion increase with the aggressiveness of the aging schedule. As the retention cycle shortens, the rapidity of deactivation through a litigation hold process must escalate. The choice of retention cycle should thus take into account not only business needs, but also the company's ability to deploy litigation holds, the extent of its litigation obligations, and other processes it has created to preserve potentially important email.

**D. Disaster Recovery Backups**

Business entities often use backup tapes originally intended for disaster recovery as an unofficial archive. While such dual use may be tempting in the short term, it leads to problems in the litigation context. Such dual use often results in the retention of backup media for long periods of time, increasing the amount of information on hand when litigation strikes. Because backup technology is generally not intended for archival use, there are no efficient means of locating individualized items of information. Disaster restorations ordinarily occur on system levels, so backups focus on entire data sets, not individual custodians or individual items held by individual custodians. Especially when multiplexing is employed, locating an individual custodians’ entire email account may be a challenge. Restoration may also be costly, yet use
for purposes other than disaster recovery largely eliminates any argument that the backup media is inaccessible for discovery purposes.

Ideally, ordinary backups should be used solely for disaster recovery, and placed on a very short recycle schedule. If a firm wishes to implement a separate archival use, consideration should be given to segregating specified tape sets for this purpose, without affecting the rotation of other backups. Consideration should also be given to configuring backups of certain systems – e.g., email servers, so as to segregate the content of such servers from other, unrelated data.

E. Litigation Hold Process

A robust litigation hold process is critical to a company’s ability to avoid spoliation sanctions. At the core of such a process lies a written preservation policy that (1) defines the circumstances when litigation holds apply; (2) sets forth basic rules on what is expected of employees when a hold is in place, e.g., employees should not alter or destroy any potentially relevant evidence, whether official records or transient material, and employees should communicate their knowledge of the special circumstance to the legal department or an appropriate risk management liaison; and (3) provides guidance to help employees successfully meet those expectations.

For example, a litigation hold would ordinarily apply when there is notice of litigation, government investigation, or a subpoena or similar information request. It would also apply if any of the forgoing were reasonably anticipated. A preservation policy should assist employees in identifying factors that could give rise to a post hoc judicial determination that a claim “should have been reasonably anticipated,” thus triggering a preservation obligation: the filing of an administrative claim; receipt of a demand letter; and in some circumstances, an internal complaint.11

Similarly, the preservation policy, and any attendant forms for the issuance of a preservation notice by the legal department upon its receipt of notice that a special circumstance either exists or is reasonably anticipated, ordinarily provide recipients of preservation notices guidance regarding where to search for potentially relevant recorded information and communicate the types and forms of recorded information that may be subject to the duty to preserve. The preservation policy and implementing notices should also communicate acceptable methods of preservation (e.g., to keep metadata intact) and should address issues such as the dissemination of a preservation notice to subordinate employees; identification of additional personnel with relevant information; identification of systems and other centrally managed ESI that is potentially relevant; methods to obtain any still existing information generated by employees who are no longer part of the organization; and information regarding collection of the preserved recorded information.

Many companies incorporate an acknowledgment of receipt and/or compliance as an aspect of the litigation hold process. Such an acknowledgment enhances the ability to track compliance, may serve to further impress on the employee the need for compliance by creating individual accountability, and may serve as evidence of the company’s good faith effort to preserve potentially relevant evidence.

The litigation hold process must further provide for regular reminders to employees who hold information subject to a hold, and other activities to ensure that potentially relevant evidence is preserved. IT must audit systems under its control to ensure that auto delete
functions have been deactivated as needed, or that alternative measures have successfully been implemented to avoid the destruction of potentially relevant evidence in those cases where the automatic roll-off of information cannot be suspended. It may be advisable to initiate email journaling for select custodians, or to segregate select custodians to specific servers whose back-up tapes are then preserved. In short, the litigation hold process is active and requires regular interaction and intervention by legal, IT, and individual custodians.

Finally, for those companies that are subject to significant quantities of litigation or other circumstances giving rise to preservation obligations, or whose legal departments are segmented, it is advisable to implement a means of tracking all litigation holds in a systematic way. Such a system enhances coordination and uniformity; reduces duplication of effort; and helps avoid errors (e.g., notifying custodians that a hold is no longer in effect because one case settled, but another litigation to which the custodian’s recorded information may be relevant has been elsewhere initiated).

**F. Email Archive**

Companies that are subject to a regulatory requirement to maintain all communications (e.g., investment advisors) should consider, and companies that frequently find themselves in litigation may wish to consider, an email archive with journaling as a means of automated collection and preservation of email. An archive provides ready, centralized access and enhances searchability. An archive should de-duplicate, thus reducing the amount of storage space. The journaling feature eliminates any human intervention in the preservation of email, and thus provides for consistency and obviates any possibility of deliberate non-compliance with preservation obligations.

The selection and deployment of archives are expensive and time consuming propositions. However, the benefits may outweigh the costs for some firms.

**G. Data Mapping**

Data mapping identifies the repositories of information that exist within a corporate entity. For each repository of interest, a data map should identify the name, and technical characteristics of the repository (e.g., operating system, associated software, etc.). It should describe the nature of the information stored and its parameters (e.g., HR information for employees of ABC Subsidiary after January 1, 2019). Ideally, it would reflect whether the system incorporates information from predecessor systems, and if so, the extent to which such data was migrated from the prior systems. It should identify the date of deployment, and if, as often happens, deployment occurred over a period of time during which various portions of the enterprise moved onto the system, a description and time table of that deployment. (Conversely, when a system is retired, the data map ought to indicate the extent to which data is migrated, the system to which it was migrated, and the date of retirement.) Data maps are also most helpful when they reflect the names of employees responsible for the content (often described as the system “owner” or “gatekeeper”), who designed the system, and/or who maintain the system (usually someone within IT, often coupled with a vendor). This provides quick access to the system’s experts, who are an invaluable resource in both preservation and production of database and system information. Finally, the perfect data map would provide a description of retention, system limits on size or duration of retention, backup methods, and automated “janitor” features that “clean” the system on a regular pre-set basis. (In the world of personal computers, examples of typical janitor functions are periodic defragmentation of the
computer’s memory or sweeps of recycle bins.) Such information could quickly alert the legal department if intervention was needed to ensure preservation of potentially relevant information.

While a data map may not be an absolute necessity in the garden variety litigation (or administrative proceeding, like an EEOC charge) that requires only limited and well-defined categories of information with which the legal department is already familiar, data maps are very important in complex organizations (geographically diverse operations, frequent acquisitions and divestments, decentralized management) or in the context of complex litigation (novel issues, class (or systemic) claims, or topics involving non-traditional sources of information). For example, any wage/hour claim that involves alleged “off-the-clock work” will likely involve information sources wholly unrelated to human resources. By definition, the activities at issue are not reflected in an employer’s time-keeping system. Rather, clues to employee activities while not “on the clock” are often found in business systems housing customer service accounts, work orders, point-of-sale information and similar sources. Identifying such systems, and reaching out to personnel who know whether they contain the sought after information is substantially facilitated by the existence of data maps. (Data maps also have non-litigation related uses. Such uses include identification and elimination of unnecessary, redundant systems and integration of systems.)

Armed with a data map, the legal department can easily identify the repositories of interest to any particular administrative matter or to any litigation. However, some entities find it useful to go a step further with data dictionaries for at least those systems commonly at issue in litigation.

Although data dictionaries come in infinite varieties, the most complete data dictionaries lay out the system’s architecture, identify the specific fields of information included within the repository, provide the location within the repository for the particular fields identified, and provide translations for codes. If one thinks of a data map as a form of Atlas, the data dictionary is like a detailed blueprint. Needless to say, creating a data dictionary for a complex system already in existence may require a significant investment of resources. On the other hand, creating a data dictionary in conjunction with system design is more in the nature of documenting the work itself and involves only incremental cost.

If a data dictionary exists, it provides the key to responding to interrogatories and similar requests for information about the systems that house relevant data. But data dictionaries also have more positive, beneficial uses. For example, data dictionaries provide an expert retained by the employer to help develop the defense of a claim with rapid insight into the specific data available for the expert’s consideration. Outside the context of litigation, they can help both administrative professionals (like HR) and IT in fine-tuning systems to make them more efficient or useful. They are also a valuable resource in designing new systems and deciding what data ought to be migrated.

The theme, of course, that runs through both data maps and data dictionaries is that advance planning and the knowledge that comes as a result can be critical in addressing information demands in administrative proceedings. Similar benefits inure in the context of formal litigation. In all federal jurisdictions (where much, if not most, employment litigation is pursued) and in a growing number of states, the parties are required by court rules to meet very early in the case to share information regarding potential sources of information that will be relevant to the litigation. Having data maps and dictionaries gives the employer’s counsel key information and allows the company’s attorney to pro-actively determine the direction of discovery. Simultaneously, investing in the development of data maps and dictionaries can
have business bonuses unrelated to the demands of litigation. These diverse benefits may incentivize the administrative professional – and his or her liaisons in IT – and improve the company’s ability to meet the obligations forced upon it in today’s litigation environment.

H. Cloud Storage

One of the most vexing problems for global companies and their lawyers is how to identify, collect and use electronically stored information in e-discovery without violating local restrictions and facing significant fines. With the advent of cloud computing\textsuperscript{12}, these problems are no longer reserved for global companies.

While it is easy to move data to the cloud, legally protecting that data and assuring its availability for business and litigation purposes is complicated. To help mitigate that risk, the cloud service contract must be carefully reviewed by in-house counsel, the CIO and CTO, and even outside counsel. The contract should fully memorialize the company’s expectations and requirements of its cloud providers in terms of preservation, retention, and disposal of data. With regard to discovery of ESI, companies should consider including in the contract how certain data and metadata will be retained, including the ability to search on the basis of content, sender, recipient, and other metadata. The cloud provider agreement should explicitly discuss the roles and responsibilities of the cloud provider and the company, including (but not limited to):

1. ownership of data and permissible uses
2. encryption and transmission standards
3. data breach liability, including notification procedures, data security standards, and other technical security measures
4. backups
5. confidentiality provisions
6. auditing rights, logs, and other related responsibilities
7. the cloud company’s business continuity plan/disaster recovery procedures
8. provisions in the event of a dispute with the cloud company (so that data cannot be held)
9. hostage
10. onward transfer agreements (in the event that the business migrates cloud providers)

The use of the cloud does not change a company’s responsibility to preserve and produce data. A court is not likely to be sympathetic to a proffered cloud-caused discovery excuse. Responding effectively to e-discovery issues requires that a variety of concerns be fully considered and resolved prior to selection of the cloud provider and data migration. The obligation to preserve and produce ESI extends to material that is not in the company’s “possession” or “custody” but nonetheless is within its “control.” E-discovery obligations cannot be avoided simply by contracting with a third-party provider to store business data or host a business application. A host of judicial holdings provide clear guidance for employers:

1. Finding that party had control over content posted on website even if website was maintained on a third-party server\textsuperscript{13}
2. Holding that party had control over text messages held by third-party service provider\textsuperscript{14}
3. Holding that party had control over electronic data maintained by third party human resources firm and that party could not delegate its recordkeeping duties under ERISA\textsuperscript{15}
4. Requiring defendant to provide the plaintiff’s counsel with full access to his third party servers

5. Finding that if a company has access to documents to conduct business, [then] it has possession, custody and control of the documents for purpose of discovery.

III. Maintaining Order

While litigation preparedness is critical to the successful defense of spoliation challenges, it is only half the battle. In addition to the pre-litigation actions outlined above, companies must take several steps once they receive notice of a claim, or reasonably anticipate the filing of a claim, to win the day. These steps focus on effective implementation of the tools created through a litigation preparedness program.

Several leading cases find fault not with the employer’s preservation policies, but rather, with the employer’s or counsel’s efforts to effectuate preservation notices and discovery strategies. Zubulake plainly found fault with the former; Qualcomm with the latter.

As the court cautioned in Zubulake, counsel must take a number of steps to ensure successful preservation and production of email. Counsel must:

1. “make certain that all sources of potentially relevant information are identified,” a task that requires counsel to “become fully familiar with her client’s document retention policies, as well as the client’s data retention architecture” which in turn requires not only the interview of IT personnel but also every key player to fully explore their personal document/data storage practices;
2. Periodically re-issue the litigation hold;
3. Personally remind key players of their duty to preserve evidence;
4. Instruct all employees to give counsel electronic copies of their relevant files; and
5. Either arrange for the identification and safe storage of all backup media which must be retained or take physical custody of such media.

As the outcomes in both Qualcomm and Coleman Holdings, Inc. demonstrate, the mere preservation of relevant evidence is insufficient. In both cases, the spoliation claim did not focus on the destruction of relevant evidence, but rather, on the responding parties’ inadequate production of such evidence. In Coleman Holdings, Inc., batches of backup tapes were belatedly identified by counsel on more than one occasion, and even more foot-dragging occurred before the relevant evidence from such tapes was produced. In Qualcomm, the responding company directed its counsel to limit the choices of email search terms so that large quantities of relevant evidence were essentially suppressed.

The lessons to be learned from these cases are relatively straightforward. A business must understand what information it possesses and where it is stored – record retention policies, proper use of backup tapes, and solid litigation hold process, should assist the employer in meeting these goals. Once the pool of potentially relevant information is identified, litigants must act in good faith in deploying technology tools to sort through that pool of information.
PAPER vs. ELECTRONIC EMPLOYMENT RECORDS

Maintaining only electronic copies of personnel files complies with federal and state law, although some statutes specify certain requirements for how the documents must be stored. Most employment laws that require record retention do not require a specific format or medium for maintaining the record. Federal regulations for other statutes explicitly provide that electronic scans of an original comply with record retention requirements, as long as minimum requirements are met, described below.

Of all employment-related forms, I-9s require the most precautions before shredding the original, as explained below. However, the requirements for converting I-9s to electronic form are not onerous. DOL regulations also establish minimum requirements for electronically storing documents that must be retained under ERISA, but those requirements are not onerous either. (In fact, you’ve probably already taken the required steps anyway in the ordinary course of business).

I. Storing I-9 Forms Electronically

Immigration and Customs Enforcement (“ICE”) issued a rule permitting employers to complete, sign, and store I-9 forms electronically if certain performance standards are met. See 8 C.F.R. §274a.2(b). The rule also permits employers to electronically scan and store existing I-9 forms. See 8 C.F.R. §274a.2(b)(2)(i). The rule is product and technology neutral, which allows employers flexibility to keep records in a manner consistent with other business processes and to adopt new technology in the future, as long as the selected electronic storage system meets minimum performance standards.

The ICE rule creates a set of minimum standards that must be met by employers electing to complete and/or retain I-9 forms electronically. See 8 CFR 274a.2(e)(1). The standards are designed both to enable employers to streamline their recordkeeping and to provide Department of Homeland Security (“DHS”) investigators with a framework for inspecting the records and assessing their trustworthiness. The key points of the rule are:

Standards for Electronic Retention: Any electronic generation or storage system used to store I-9 forms must include:

- Reasonable controls to ensure its integrity, accuracy, and reliability;
- Reasonable controls designed to prevent and detect any unauthorized or accidental creation of, addition to, alteration of, deletion of, or deterioration of an electronically completed and stored I-9, including the electronic signature if used;
- An inspection and quality assurance program evidenced by regular evaluations of the electronic generation or storage system, including periodic checks of the electronically stored Form I–9, including the electronic signature if used;
- A retrieval system that includes a searchable indexing system; and
- The ability to reproduce legible hard copies.

See 8 C.F.R. §274a.2(e)(1). The regulation defines “legibility” to mean “the observer must be able to identify all letters and numerals positively and quickly, to the exclusion of all other letters or numerals.” The regulation defines “readability” to mean “that the observer must be able to recognize any group of letters or numerals that form words or numbers as those words or complete numbers.” The regulation also provides more details about what constitutes an
acceptable indexing system and that an employer retaining completed I-9 forms electronically may use reasonable data compression or formatting technologies.

**Documentation:** Employers choosing to complete and/or retain I-9 forms electronically must maintain and make available to any U.S. agency, upon request, documentation of the business processes that:

- Create the retained I-9 forms;
- Modify and maintain the retained forms; and
- Establish the authenticity and integrity of the forms.

**Security:** Employers electing to complete or retain I-9 forms electronically must implement an effective records security program that:

- Ensures that only authorized personnel have access to electronic records;
- Provides for backup and recovery of records to protect against information loss due to reasons such as power interruptions;
- Ensure employees are trained to minimize the risk of unauthorized or accidental alteration or erasure of electronic records; and
- Ensure that whenever the electronic record is created, accessed, viewed, updated, or corrected, a secure and permanent record is created that established the date of access, the identity of the individual who accessed the record, and the particular action taken.

**Electronic Signatures for Employee and Employer:** If a Form I-9 is completed electronically, the attestations must be completed using a system for capturing an electronic signature that includes a method to acknowledge the signatory has read the attestation. Specific requirements also exist for creating and preserving a record verifying the identity of an employee producing an electronic signature, and providing printed confirmation of the transaction when it occurs.

**II. Occupational Safety and Health Act (OSHA)**

Documents required by OSHA (such as OSHA 300 Logs) may be maintained electronically, as long as the employer can produce a copy of the log within four (4) hours if OSHA asks for a copy. See 29 C.F.R. §1904.40(a). However, employers still have a duty to post a paper copy of the annual summary of injuries and illnesses recorded on the OSHA 300 Log for the previous year from February 1 to April 30. See 29 C.F.R. §1904.32. A log and summary of all recordable occupational injuries and illnesses for each establishment (OSHA Forms 300 and 300A) and a supplementary record (OSHA Form 301) must be kept for five years following the end of the calendar year that these records cover. See 29 C.F.R. § 1904.33.

**III. Employee Retirement Income Security Act (ERISA)**

ERISA requires plan sponsors to retain certain documents for a fixed period of time. DOL regulations specifically provide that electronic media may be used for complying with the record retention requirements provided certain requirements are met:

1. The electronic recordkeeping system must have reasonable controls to ensure the integrity, accuracy, authenticity and reliability of the records;
(2) the electronic records are maintained in reasonable order, in a safe and accessible place, and in such manner as they may be readily inspected or examined (for example, the recordkeeping system should be capable of indexing, retaining, preserving, retrieving, and reproducing the electronic records);

(3) electronic records must be readily convertible into legible and readable paper copies;

(4) the electronic recordkeeping system is not subject to any agreement or restriction that would, directly or indirectly, compromise or limit a person’s ability to comply with any reporting and disclosure requirement or any other obligation under Title I of ERISA; and

(5) adequate records management practices are established and implemented.

See 29 C.F.R. §2520.107-1(b). Regarding requirement (3), the DOL’s definitions of “legibility” and “readability” are substantively the same as the definitions of these terms as applied to I-9 forms. See 29 C.F.R. §2520.107-1(c). Regarding requirement (5), the regulations give the following examples of “adequate records management practices”:

- following procedures for labeling of electronically maintained or retained records
- providing a secure storage environment
- creating back-up electronic copies and selecting an off-site storage location
- observing a quality assurance program evidenced by regular evaluations of the electronic recordkeeping system including periodic checks of electronically maintained or retained records
- retaining paper copies of records that cannot be clearly, accurately, or completely transferred to an electronic recordkeeping system

The regulation states that the original paper records may be discarded as soon as they are converted to electronic format, “[unless] the electronic record would not constitute a duplicate or substitute record under the terms of the plan and applicable federal or state law.” See 29 CFR § 2520.107-1(d). Also note that certain original documents should not be discarded if they have legal significance or inherent value in their original form (e.g., notarized documents, insurance contracts, stock certificates, and documents executed under seal).

IV. Discrimination Laws and Retention of Documents

The various discrimination laws (Title VII, Age Discrimination in Employment Act (ADEA), Americans with Disabilities Act (ADA), Executive Order 11246 (EEO-1 Reports), Family and Medical Leave Act (FMLA)) and the Fair Labor Standards Act (FLSA) mandate certain retention periods for documents and certain forms of retention. However, none of these laws prohibit storing documents electronically. The Equal Employment Opportunity Commission (“EEOC”) has stated in an informal discussion letter that an electronic recordkeeping system could meet the requirements of the statute. See Title VII/ADA/ADEA: Recordkeeping, Jan. 19, 2006 (EEOC). Although the informal discussion letter is not an official, binding opinion, it is a good indication that maintaining electronic records would not be a per se violation of the above statutes.

The above laws do require that the required records be readily available for inspection upon request. Therefore, you may electronically store any documents required by these laws if you can access the documents within a reasonably short period of time.
PERSONNEL RECORD RETENTION REQUIREMENTS

Employers must ensure that their record keeping practices adhere to all of the numerous statutes and regulations dictating (1) what types of records must be retained and (2) the corresponding periods of retention. Below is a listing of record retention requirements of specific interest to those dealing in human resources. The chart considers the records involved, the period of retention, and in some instances, the statutory foundation for these requirements.

When different federal or state laws specify different record retention periods for the same records, employers should adhere to the longer period.

<table>
<thead>
<tr>
<th>TABLE VI, ADA and GINA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Employers with 15 or more employees in each of 20 consecutive calendar weeks of the current or preceding year.</strong></td>
</tr>
<tr>
<td>Any personnel or employment records, including application forms, which an employer makes or keeps, and records related to hirings, promotions, demotions, transfers, layoffs, terminations, rates of pay, selections to training programs, etc.</td>
</tr>
<tr>
<td>All personnel records relevant to a charge filed with or actions brought by the EEOC. Including, for example, records relating to charging party and to all other employees holding similar positions, application, or test papers completed by unsuccessful applicants and by all other applicants applying for same position.</td>
</tr>
<tr>
<td>Personnel records of terminated individuals.</td>
</tr>
<tr>
<td>EEO-1 report filed with the EEOC. (Only applicable if have 100 or more employees)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AGE DISCRIMINATION IN EMPLOYMENT ACT (ADEA)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Employers with 20 or more employees for each working day in each of 20 or more calendar weeks in the current or preceding calendar year.</strong></td>
</tr>
<tr>
<td>Payroll records containing each employee’s name, address, date of birth, occupation, rate of pay, and compensation earned each week.</td>
</tr>
</tbody>
</table>
### AGE DISCRIMINATION IN EMPLOYMENT ACT (ADEA)

<table>
<thead>
<tr>
<th>Records</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any personnel records which an employer makes and which are related to (i) job applications and inquiries; (ii) promotions, demotions, transfers, selections for training, layoffs, recalls, discharges; (iii) job orders submitted to employment agencies or unions for the recruitment of employees; (iv) test papers; (v) results of physical exams; (vi) any advertisements or notices of job opportunities.</td>
<td>1 year. 29 C.F.R. § 1627.3</td>
</tr>
<tr>
<td>Employee benefit plans, seniority, and merit system.</td>
<td>While plan is in effect and 1 year after termination of plan. 29 C.F.R. § 1627.3</td>
</tr>
</tbody>
</table>

### EQUAL PAY ACT

**Employers with at least 1 employee.**

<table>
<thead>
<tr>
<th>Records</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any records which an employer makes which relates to the payment of wages, evaluations, job wage rates, job descriptions, merit systems, seniority, collective bargaining agreements, description of practices or other matters which explain the basis for payment of a wage differential to employees of the opposite sex.</td>
<td>2 years. 29 C.F.R. § 1620.32</td>
</tr>
<tr>
<td>All records required to be kept by the FLSA.</td>
<td>See FLSA (below). 29 C.F.R. § 1620.32</td>
</tr>
</tbody>
</table>

### FAMILY AND MEDICAL LEAVE ACT (FMLA)

**Employers with 50 or more employees during 20 or more calendar work weeks in either the current or preceding calendar year.**

<table>
<thead>
<tr>
<th>Records</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll records for each employee, including full name, identification number, home address, date of birth if under the age of 19, sex, occupation, day and time work week begins, hours worked each day and week, total daily or weekly earnings, overtime compensation, basis of overtime computation, total additions to or deductions from wages, total wages for each pay period, date of payment, and the pay period covered by the payment.</td>
<td>3 years from last date of entry. 29 C.F.R. § 825.500</td>
</tr>
</tbody>
</table>
## FAIR LABOR STANDARDS ACT (WAGE & HOUR)

*Employers with at least 1 employee.*

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Retention Time</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll records for each employee, including full name, identification number, home address, date of birth if under the age of 19, sex, occupation, day and time work week begins, hours worked each day and week, total daily or weekly earnings, overtime compensation, basis of overtime computation, total additions to or deductions from wages, total wages for each pay period, date of payment, and the pay period covered by the payment.</td>
<td>3 years from last date of entry.</td>
<td>29 C.F.R. § 516.5</td>
</tr>
<tr>
<td>Individual employment contracts, collective bargaining agreements, plans, trusts, certificates, and required notices.</td>
<td>3 years from last effective date.</td>
<td>29 C.F.R. § 516.5</td>
</tr>
<tr>
<td>Sales and purchase records, by total dollar volume, weekly, monthly, or quarterly.</td>
<td>3 years.</td>
<td>29 C.F.R. § 516.5</td>
</tr>
<tr>
<td>Supplementary basic records including work sheets showing daily starting and stopping time of employees, wage rate schedules, and work time schedules.</td>
<td>2 years.</td>
<td>29 C.F.R. § 516.6</td>
</tr>
<tr>
<td>Order, shipping, and billing records.</td>
<td>2 years.</td>
<td>29 C.F.R. § 516.6</td>
</tr>
<tr>
<td>Records of additions to and deductions from each individual employee’s wages; all employee purchase orders; all records used in determining amount and computation of addition or reduction.</td>
<td>2 years.</td>
<td>29 C.F.R. § 516.6</td>
</tr>
<tr>
<td>Any Certificates of Age (if applicable). Employer may be required to keep different or additional wage and hour records on employees in certain specialized occupations and on employees who may be otherwise exempt from FLSA.</td>
<td>Until termination of employment.</td>
<td>29 C.F.R. § 570.6</td>
</tr>
</tbody>
</table>
### OCCUPATIONAL SAFETY AND HEALTH ACT (OSHA)

**Applies to employers with at least 10 employees.**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Duration</th>
<th>Rule Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>A log and summary of all recordable occupational injuries and illnesses for each establishment (OSHA Forms 300 and 300A) and a supplementary record (OSHA Form 301).</td>
<td>5 years.</td>
<td>29 C.F.R. § 1904.33</td>
</tr>
<tr>
<td>Employee exposure records on toxic substances and harmful physical agents (including environmental and biological monitoring information and material safety data sheets).</td>
<td>30 years.</td>
<td>29 C.F.R. § 1910.1020</td>
</tr>
<tr>
<td>Employee medical records (including medical histories, examinations and test results, medical opinions and diagnoses, description of treatment and prescriptions, and employee complaints). There are some exceptions.</td>
<td>Duration of employment, plus 30 years.</td>
<td>29 C.F.R. § 1910.1020</td>
</tr>
</tbody>
</table>

### IMMIGRATION REFORM AND CONTROL ACT OF 1986

**Employers employing persons to perform labor or services in return for wages or other pay.**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Duration</th>
<th>Rule Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form I-9</td>
<td>3 years after the date of hire; or 1 year after date the employment is terminated, whichever is later.</td>
<td>8 C.F.R. § 274a.2</td>
</tr>
</tbody>
</table>

### FEDERAL EMPLOYMENT SECURITY LAW (UNEMPLOYMENT BENEFITS)

**Employers with at least 1 employee in each of 20 different calendar weeks in either the current or preceding year.**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>For each pay period, the beginning and ending dates and the largest number of workers employed during each calendar week of that pay period. For each individual employee, his/her name and social security number, number of hours worked each weeks (if less than full-time), money wages paid, reasonable cash value of remuneration paid in other than cash, the date he/she was hired, rehired, or returned to work after temporary layoff, and the date or reason he was separated from employment. Regarding eligibility for partial benefits for each employee, the wages earned by weeks, whether any week was less than full-time, and time lost due to the employee’s unavailability for work.</td>
<td>5 years.</td>
</tr>
</tbody>
</table>
### FEDERAL WITHHOLDING AND SOCIAL SECURITY TAXES

**All Employers.**

<table>
<thead>
<tr>
<th>Information</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employer identification number (EIN); Amounts and dates of all wage, annuity, and pension payments</td>
<td>4 years following end of applicable tax year</td>
</tr>
<tr>
<td>Amounts of tips reported; Records of allocated tips; Fair market value of in-kind wages paid; Employee names, addresses, social security numbers, occupations of employees and recipients; All employee copies of Forms W-2 and W-2c that were returned as undeliverable; Dates of employment; periods for which employees and recipients were paid while absent due to sickness or injury, and the amount of weekly rate of payments made to them by the employer or a third-party payers; Copies of employees’ and recipients’ income tax withholding allowance certificates (Forms W-4, W-4P, W-4S, and W-4V); Dates and amounts of tax deposits made and acknowledgment numbers for deposits made by EFTPS; Copies of returns filed, including Form 941 TeleFile Tax Records and confirmation numbers; Documentation for allocated tips; Records of fringe benefits provided, including substantiation</td>
<td>4 years following end of applicable tax year</td>
</tr>
</tbody>
</table>

### HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (“HIPAA”) PRIVACY RULES

**Applies to covered entities, including group health plans, health care providers, and health care clearing houses.**

<table>
<thead>
<tr>
<th>Information</th>
<th>Retention Period</th>
</tr>
</thead>
</table>
| Privacy policy and procedures Implementation specifications and requirements: Plan amendments Business associate agreements Designation of privacy officer and contact person | Later of 6 years from:  
  - Date of creation; or  
  - Date last in effect  
  45 C.F.R. § 164.105  
  45 C.F.R. § 164.306  
  45 C.F.R. § 164.530 |
Required Communications:
- Privacy notices
- Authorizations
- Complaints
- Accountings
- Requests for access/copies

Actions, activity or designation required by the Privacy Rule to be documented:
- Records of privacy training
- Disposition of complaints
- Accountings
- Dispositions for requests to access/copies
- Confidential disclosures
- Restricted disclosures
- Sanctions for violations of policy (i.e., disciplinary actions)

### CONSOLIDATED OMNIBUS BUDGET RECONCILIATION ACT OF 1985 (“COBRA”)
Applies to group health plans sponsored by employers who normally employ 20 or more employees on 50% of the typical business days during the calendar year preceding the qualifying event, determined on a controlled group basis.

### EMPLOYEE RETIREMENT INCOME SECURITY ACT OF 1974 (“ERISA”)
Applies to all employee benefit plans.

<table>
<thead>
<tr>
<th>Summary annual reports</th>
<th>A minimum of 6 years from the date of the filing of the Form 5500 Annual Report (or date such Form 5500 would have to be filed if the plan did not qualify for an exception or simplified reporting format). Recommend that such records be held for at least 7 years following the end of the applicable plan year for which record applies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary of material modifications</td>
<td></td>
</tr>
<tr>
<td>Contracts and/or agreements (TPA, brokers, etc.)</td>
<td></td>
</tr>
<tr>
<td>Correspondence with Third party administrators, brokers, service providers, participants, etc.</td>
<td></td>
</tr>
<tr>
<td>Investment policies</td>
<td></td>
</tr>
<tr>
<td>Board/committee meeting minutes discussing benefit plan issues</td>
<td></td>
</tr>
<tr>
<td>Collective bargaining agreements</td>
<td></td>
</tr>
<tr>
<td>Administrative policies, procedures or guidelines</td>
<td></td>
</tr>
<tr>
<td>Vouchers, worksheets, receipts</td>
<td></td>
</tr>
<tr>
<td>Claim records</td>
<td></td>
</tr>
<tr>
<td>Qualified medical child support orders</td>
<td></td>
</tr>
<tr>
<td>Qualified domestic relations orders</td>
<td></td>
</tr>
<tr>
<td>Legal opinions</td>
<td></td>
</tr>
<tr>
<td>Journals, registers, ledgers, etc.</td>
<td></td>
</tr>
<tr>
<td>Checks, invoices, bank statements, etc.</td>
<td></td>
</tr>
<tr>
<td>Payrolls</td>
<td>Recommend retaining permanently.</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Form 5500’s and related schedules</td>
<td></td>
</tr>
<tr>
<td>Insurance policies, contracts, certificates of insurance</td>
<td></td>
</tr>
<tr>
<td>Employee enrollment and election forms</td>
<td></td>
</tr>
<tr>
<td>Beneficiary designation forms</td>
<td></td>
</tr>
<tr>
<td>Premium schedules, communication materials, etc.</td>
<td></td>
</tr>
<tr>
<td>Lists of covered employees</td>
<td></td>
</tr>
<tr>
<td>Evidence of compliance with bonding requirements; fiduciary liability insurance, etc.</td>
<td></td>
</tr>
<tr>
<td>Documentation regarding the selection, monitoring, replacement of Third party administrators, record keepers, trustees, investment options, etc.</td>
<td></td>
</tr>
<tr>
<td>Flexible spending accounts records and claims</td>
<td></td>
</tr>
<tr>
<td>Records relating to decisions to retire employees</td>
<td></td>
</tr>
<tr>
<td>Incentive plan records (if benefits are paid after term)</td>
<td></td>
</tr>
<tr>
<td>Plan documents</td>
<td></td>
</tr>
<tr>
<td>Plan amendments</td>
<td></td>
</tr>
<tr>
<td>Summary plan descriptions</td>
<td></td>
</tr>
<tr>
<td>Trust agreements</td>
<td></td>
</tr>
<tr>
<td>Applicable resolutions</td>
<td></td>
</tr>
<tr>
<td>Determination letter packages</td>
<td></td>
</tr>
<tr>
<td>IRS determination letters</td>
<td></td>
</tr>
<tr>
<td>401(k) retirement records and pension plans, including enrollment, contributions, summary reports, statements, correspondence, and work papers</td>
<td></td>
</tr>
<tr>
<td>Pension/401(k)/403(b)/457(b_/457(f) retirement plan vesting files; Records detailing employee eligibility and benefits under the disability insurance plan; Benefit reports (Report 5500) Transfer records Pay scales Salary surveys Promotion records (for company-wide promotions)</td>
<td></td>
</tr>
</tbody>
</table>
### FTC DISPOSAL RULE

<table>
<thead>
<tr>
<th>Applies to any business or individual who maintains or otherwise possesses consumer information for a business purpose.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer information must be properly disposed of by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.</td>
</tr>
<tr>
<td>“‘Consumer information’ means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report . . . [or] a compilation of such records.”</td>
</tr>
<tr>
<td>“Reasonable measures” include implementing and monitoring compliance with policies and procedures that require shredding papers containing consumer information and destruction or erasure of electronic media containing consumer information.</td>
</tr>
<tr>
<td>The rule does not provide a specific time requirement for disposing of records. 16 C.F.R. § 682 et seq.</td>
</tr>
</tbody>
</table>
ENDNOTES

1 In re Pfizer Inc. Securities Litigation, 288 F.R.D. 297, 319 (S.D.N.Y. 2013)

2 Id.

3 Welsh v. United States, 844 F.2d 1239, 1245-1247 (6th Cir. 1988).


5 O’Berry v. Turner No. 7:15-CV-00064, 2016 WL 1700403 (M.D. Ga., April 27, 2016) (inferring intent because “all of these facts, when considered together, lead the Court to conclude that the loss of the at-issue ESI was beyond the result of mere negligence”).


7 Goodman v. Praxair Services, Inc. 632, F. Supp. 2d 494, 506 (2009) (noting that “if spoliation has occurred, then a court may impose a variety of sanctions, ranging from dismissal or judgment by default, preclusion of evidence, imposition of an adverse inference, or assessment of attorney’s fees and costs”).

8 Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y 2004) (failure to identify one person with relevant emails and failure to sufficiently follow up on previously issued preservation notices to other custodians of relevant email leads to adverse inference instruction); Coleman Holdings, Inc. v. Morgan Stanley & Co., Inc. 2005 WL 674885 (Fla. Cir. Ct. 2005) reversed on other grounds 955 So.2d 1124 (Fla. 4th DCA 2007) (substantial delay and repeated misrepresentations to the court concerning the existence of back-up tapes containing relevant email leads to default judgment). See also In re Telxon Corporation Securities Litigation, 2004 WL 3192729 (N.D. Ohio 7/16/2004) (recommending default judgment against third party defendant PricewaterhouseCooper, LLP for a failure to timely produce various electronic documents and databases after repeated representations that its production was complete).

9 Peskoff v. Faber, 240 F.R.D. 26 (D.D.C. 2007) (requiring defendant to search plaintiff’s email account; email accounts of other employees; computer hard-drives of employees, including forensic analysis of “slack space;” backup tapes; and any other depository of company email); In re Kmart Corp., 371 B R. 823 (Bankr. Ct. N.D.Ill. 2007) (commenting on the multiple locations where email might be stored, requiring further searches by Kmart for responsive email, and awarding costs).

10 See Broccoli v. Echostar Communications Corp., 229 F.R.D. 506, 511 (D. Md. 2005) wherein the court criticized the employer’s failure to deactivate its autodelete functions that limited email retention to 30 days. A similar aging schedule had been implemented in Connor v. Sun Trust Bank, 2008 WL 623027 (N.D.Ga. 3/5/2008). While in Connor, the court did not criticize the schedule, it did find preservation efforts inadequate. In both cases, adverse inference instructions were granted.

11 In Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 217-218 (S.D.N.Y. 2003), the court held that the duty to preserve evidence would arise prior to the filing of an EEOC charge if there were “a uniform belief” by “key players” that litigation would ensue. In Broccoli v. Echostar Communications Corp., 229 F.R.D. 506, 511 (D. Md. 2005) the court concluded that litigation should have been anticipated at the time of an initial informal complaint of mistreatment to the plaintiff’s immediate supervisors without regard to whether those supervisors formed a belief as to the likelihood of litigation.

12 The “cloud” is often an overused but undefined term. The National Institute of Standards and Technology defines the cloud as having five characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion and measured service. Simply put, cloud
computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.


18 Qualcomm Inc. v. Broadcom Corp., No. 05-cv-1958-RMB, 2008 WL 638108 (S. D. Cal. Mar 5, 2008) is one of several important decisions in the Qualcomm series.

Reeling in Record Retention Requirements: Tips and Common Mistakes

Presenters
Bonnie L. Martin (Indianapolis) and Marc L. Zaken (Stamford)

Moderator
Phillip A. Kilgore (Greenville)

Today’s Topics

- Defining spoliation and how it is being used as a weapon in litigation
- Limiting exposure through effective record retention programs
- Creating a record retention program in 10 “easy” steps
What is “Spoliation”? 

- Common law concept
  - Negligent or intentional
  - Withholding or destruction of evidence
  - Prejudice to the opposing party

What is “Spoliation”? 

- Gained notoriety in the last decade
  - Zubulake
- Classic examples
  - Arthur Andersen/Enron
  - Broccoli v. Echostar
- Post-SOX criminal penalties
“Spoliation” as a Weapon

- Diverts focus from the merits
- Improves settlement posture
  - Stakes can be high
  - Cost escalation
- Accesses inner workings and enables fishing expeditions

Role of Records Retention Programs

- Litigation Preparedness
  - Helps in the spoliation battle
  - Helps reduce ongoing litigation costs
    - Defensible mechanism for eliminating unused information
    - Less information = lower discovery costs
Role of Records Retention Programs

- Business Needs
  - Necessary information is preserved
  - Reduces costs of undisciplined storage

- Regulatory Requirements
  - DOL: FLSA and FMLA
  - EEO
  - OSHA/MSHA
  - IRCA
  - ERISA
  - COBRA
  - HIPAA
  - IRS
  - SEC
Features of a Records Retention Program

- Written record retention policy
- Record retention schedule
- Record management procedures
- Periodic review and “housecleaning”
- Litigation hold process

10 “EASY” STEPS

- Step 1: The Fact Finding Mission
  - Identifying “Recorded Information”
    - What is it?
    - Who owns it?
    - How is it used?
    - How long is it kept?
    - Where is it kept?
  - Identifying external standards
  - Understanding the infrastructure
10 “EASY” STEPS

- **Step 2: Analysis**
  - Separating the wheat from the chaff
  - Identifying infrastructure improvements
  - Assessing the appetite for change

- **Step 3: Decisions**
  - Format
  - Comprehensiveness
  - Record management functions
  - Extent of remediation
  - Record Retention Schedule
    - Approaches
    - Retention periods
    - Triggers
10 “EASY” STEPS

Step 4: Drafting
- Scope
- Responsibilities and obligations
- Special circumstances (aka litigation...)
- Other exceptions
- Periodic review
- Resources
- Effective date
- Records retention schedule

10 “EASY” STEPS

Step 5: Review and Refinement
- User involvement is critical
- Goals
  - Acceptable
  - Workable
  - Accurate
10 “EASY” STEPS

- **Step 6: Mechanics of Implementation**
  - How to prepare records for storage
  - Where to store records
  - How to index
  - Process for discarding records
  - Methods for discarding records and transient materials
    - Secure destruction process for confidential information

- **Step 7: Litigation Hold Process**
  - Written “Preservation Policy”
    - Defines when applicable
    - Sets forth basic rules
    - Provides guidance
  - System for issuing, managing, and tracking holds
10 “EASY” STEPS

- **Step 8: Roll-out**
  - Implement infrastructure improvements
  - PR campaign
  - Focus groups
  - Training
  - Ongoing resources

- **Step 9: Remediation**
  - Identify stores of legacy information
  - Test accuracy of inventories
  - Apply retention schedules and litigation holds
  - Discard unnecessary recorded information
10 “EASY” STEPS

- Step 10: “Audit” and Corrective Action
  - Periodic review of compliance
    - Record retention
    - Discard of transient material
  - Prompt corrective action
  - Critical to maximize effectiveness

Questions?
Reeling in Record Retention Requirements: Tips and Common Mistakes

Presenters
Bonnie L. Martin (Indianapolis) and Marc L. Zaken (Stamford)

Moderator
Phillip A. Kilgore (Greenville)