

SETTING THE CORNERSTONES FOR INFORMATION GOVERNANCE

Establishing an Information Governance Portal, Implementing a 2-Part Record Retention Policy, and Taking the “Reasonable Steps” for ESI Preservation

James S. Kurz and Rebecca Larson • Redmon, Peyton & Braswell, LLP

A growing body of literature encourages businesses to implement comprehensive Information Governance programs. While the advice is sound, companies understandably balk at the costs—both internal and external—of designing, implementing and following through with a full-blown, multi-part program. This paper proposes a scalable, cornerstone program designed for cost-conscious smaller and mid-sized businesses.

This White Paper arrives as the third in a series that addresses ESI Preservation and, most recently, proposed FRCP Rule 37(e). The initial paper, *A Trial Lawyer’s Wish List*, identifies the requirements and design for a defensible ESI preservation management solution. The second paper focuses on proposed Rule 37(e), with special attention to the rule-makers’ “reasonable steps” to navigate to a preservation safe harbor.

This third paper proposes a set of core steps that lay the cornerstones for an Information Governance program. The discussion in this paper distills to three points:

- ***Establish Information Governance Portal.*** A business’ Information Governance program, including the components discussed in this paper, should (with some exceptions) be

accessible and known across the company. A company’s Information Governance Portal accessed from the company’s website or from an internal site provides this access and provides later proof of the dissemination of the program information.

- ***Design and Implement a 2-Part Record Retention Policy.*** Every company should consider a 2-part Record Retention Policy. Part 1 identifies a business’ retention schedules, while Part 2 introduces a practice of routine deletion of some or all records not otherwise designated for retention.
- ***Navigate to the ‘Reasonable Steps’ ESI Safe Harbor.*** A practice of routine document deletion creates a tension with the duty to preserve relevant documents when a reasonable anticipation of litigation arises. The rule-makers’ solution is the ESI preservation safe harbor offered in proposed FRCP Rule 37(e). A business’ ESI preservation management solution should navigate to this safe harbor.

This paper tracks these three subjects.

1. THE INFORMATION GOVERNANCE PORTAL

As the starting point, appreciate that a Records Retention Policy imposes dissemination and record-keeping requirements. For a Policy to truly serve a

business, the business must keep sufficient records of (i) its Policy content, (ii) the dissemination of the Policy, and (iii) its compliance with the Policy. Simply put, if you're not able to reasonably prove these points in a court battle, then why bother?

Internal Publication of Policies/Record of Reviews

Employees should know where to find the company's Record Retention Policy. All too frequently, companies develop a Policy but fail either to publicize the Policy within the company and/or fall short of maintaining adequate records showing that employees have in fact been advised of the policies. A basic website accessed from the business' website or from a publicized internal site should solve both the publication and record-keeping concerns.

The graphic below shows an example of an internal website (or page on an internal website) that is a simple portal for the Record Retention Policy.

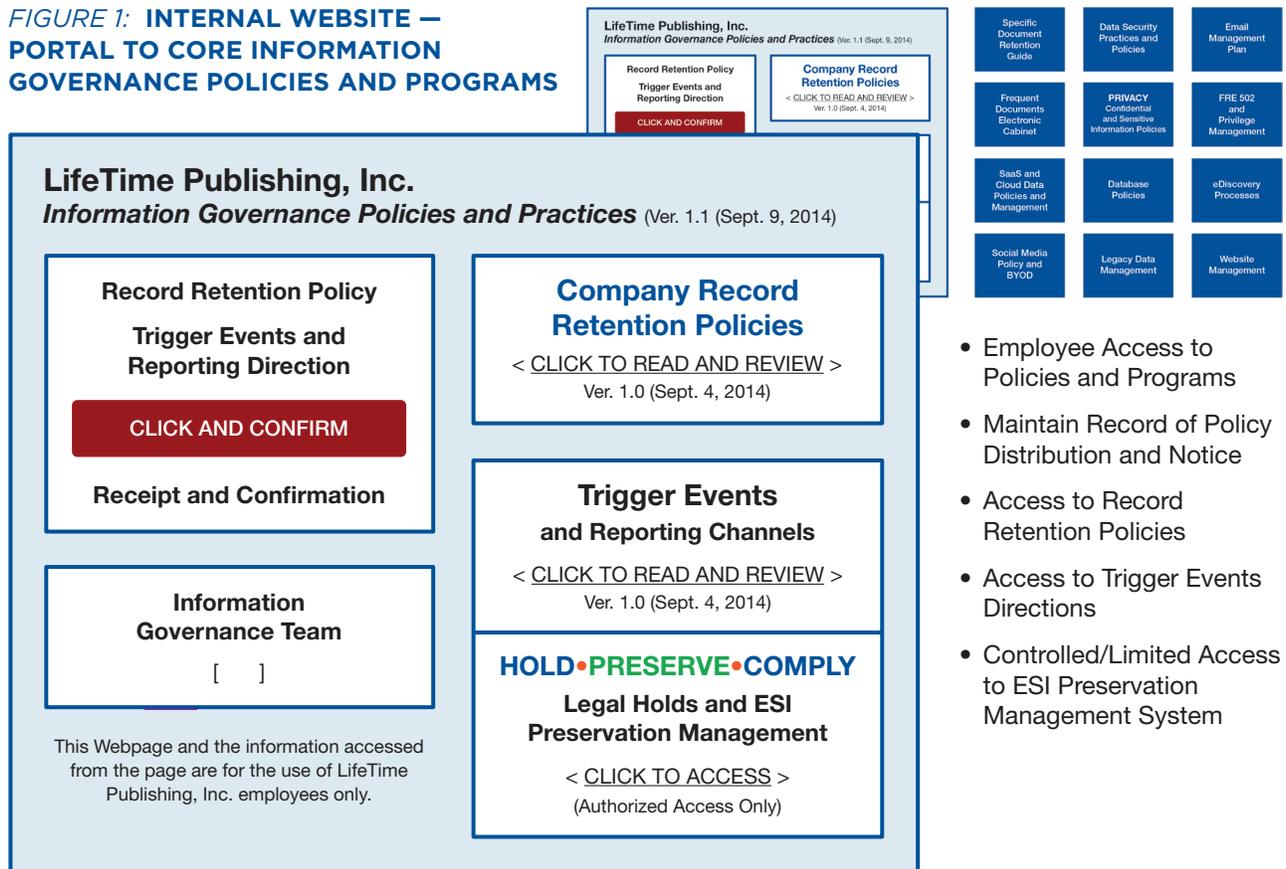
Employees are periodically directed to the site, and advised to review the Record Retention Policy and basic preservation Trigger Events.

Note that the portal website as shown includes a broader set of Information Governance components (the twelve blocks on the upper right-hand side of the graphic). For current consideration, these other components remain in the background and are not published to all employees. At the outset, the remaining parts of the portal may be empty or blank.

Record of Periodic Dissemination

An additional instruction directs employees to confirm through an online database that they reviewed the Policy. A simple login and checkmark confirms that an employee has visited the site at least represents that he or she read the Records Retention Policy including the Trigger Events. As a record-keeping method, this is both inexpensive and effective.

FIGURE 1: INTERNAL WEBSITE — PORTAL TO CORE INFORMATION GOVERNANCE POLICIES AND PROGRAMS



- Employee Access to Policies and Programs
- Maintain Record of Policy Distribution and Notice
- Access to Record Retention Policies
- Access to Trigger Events Directions
- Controlled/Limited Access to ESI Preservation Management System

2. THE RECORD RETENTION POLICY

Turning to the substantive side, every business should consider a 2-part Record Retention Policy. Part 1 includes the retention schedules for specific ESI and documents. Part 2 identifies a periodic record deletion practice for some or all of the ESI and documents that are not retained pursuant to the Record Retention Policy.

Record Retention Schedule

A business' Record Retention Schedule is a policy document that identifies the legal and compliance record maintenance requirements. The policy lists the types of records created and used by the company and identifies how long the records in each category should be retained. The schedule organizes the business' records in categories, which are often referred to as "record classes." A retention period or rule follows each record class—usually a rule is a set time period, but it may be stated as an event contingency (e.g., retain the records until a specific decision is reached or some action is taken).

Periodic ESI and Document Deletion

Part 2 of the Record Retention Policy is the practice of periodic deletion. Businesses understandably balk at implementing practices that delete large quantities of ESI and documents. They worry that they may be accused of destroying materials for nefarious reasons. But the United States Supreme Court has advised us that Record Retention Policies that include periodic ESI and document destruction are common, and that they are not wrongful. Justice Rehnquist's often quoted language is from this:

"Document retention policies," which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business. See generally Chase, To Shred or Not to Shred: Document Retention Policies and Federal Obstruction of Justice Statutes, 8 Ford. J. Corp. & Fin. L. 721 (2003). It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.

Arthur Andersen LLP v. United States,
544 U.S. 696, 04 (2005)

The *Arthur Anderson* case addressed record deletion proscribed by federal criminal statutes. The Court's holding, however, applies as well to purely civil matters where compliance with a Record Retention Policy provides a defense to spoliation accusations.

In sum, a reasonable Record Retention Policy that specifies periodic deletion of records not otherwise required to be preserved should provide a shield against spoliation accusations. A business, however, must be prepared to prove that its policy was in place at the time of claimed spoliation and that the policy was followed.

3. ESI PRESERVATION MANAGEMENT AND THE 'REASONABLE STEPS' SAFE HARBOR

A practice of routine deletion of ESI and documents remains defensible until a preservation requirement not included in the schedules arises. The rules then change. The recurring requirement that keeps corporate counsel awake late at night is the prospect of litigation, because a business has a duty to preserve relevant evidence whenever there is a "reasonable anticipation of litigation." This introduces the Legal Hold.

(a) The Challenge of Multiple Legal Holds.

The concept of a Legal Hold covers the processes a business should follow to satisfy its preservation obligations when litigation appears. The Sedona Conference's 2010 *Commentary on Legal Holds: The Trigger & the Process* summarizes the preservation obligation in this manner:

The duty to preserve requires a party to identify, locate, and maintain information and tangible evidence that is relevant to specific and identifiable litigation. It typically arises from the common law duty to avoid spoliation of relevant evidence for use at trial and is not explicitly defined in the Federal Rules of Civil Procedure. See, e.g., *Silvestri v. General Motors*, 271 F.3d 583 (4th Cir. 2001) (applying the "federal common law of spoliation"); *Chambers v. NASCO, Inc.*, 501 U.S. 32 (1991).

In *The Pension Committee of the University of Montreal Pension Plan. v. Banc of America Securities, LLC*, 685 F. Supp. 2d 456, (S.D.N.Y. 2010), Judge Scheindlin, a leading eDiscovery jurist, wrote:

The courts have a right to expect that litigants and counsel will take the necessary steps to ensure that relevant records are preserved when litigation is reasonably anticipated, and that such records are collected, reviewed and produced...

The judge continued,

By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records—paper or electronic—and to search in the right places for those records, will inevitably result in the spoliation of evidence.

There is no ambiguity in Judge Scheindlin’s directions nor in the Sedona *Commentary* summary: When there is reasonable anticipation of litigation, an appropriate Legal Hold must be implemented.

The preservation duty in a single matter can be generally satisfied when a party identifies the ESI and documents that are relevant to the claims either made or likely to be made, and protects these records from deletion. But there is a conflict between the routine, and most likely automated, deletion of business records and the continuing duty to preserve. Navigating around Legal Holds in the periodic deletion of ESI and documents becomes increasingly complex as the number of Legal Holds rises. It does not take much litigation before the routine practices are no longer routine—they become the exception.

Managing multiple Legal Holds therefore requires a process. Not only should a business establish and follow a set, legally-defensible process, but that process and the compliance with it should be well documented.

(b) Proposed Rule 37(e)’s “Reasonable Steps” Safe Harbor.

The obvious question is what are the requirements for a legally defensible process? The emerging answer is in proposed FRCP Rule 37(e), the rule that identifies the “reasonable steps” safe harbor. The surface reading of the proposed rule presents a uniform process and standard which will resolve the split among the circuits on the availability of the most serious ESI spoliation sanctions. A closer reading coupled with review of the Committee Note reveals the “reasonable steps” safe harbor and preservation proportionality.

The safe harbor works this way—if a business takes “reasonable steps” to preserve relevant ESI after the litigation flag goes up, then it may not be sanctioned for a records loss. The real-world requirement is that the company must prove that it took the reasonable steps.

Rule 37(e) is admittedly threadbare when it comes to the identification of the necessary proof, but there is guidance in the Committee Note and in the literature, most notably the Sedona Conference’s *Commentary on Legal Holds*. These sources point toward establishing an adequate process and maintaining records of compliance with the process. The *Commentary’s* Guidelines 8, 9, and 10 list process attributes, which, if incorporated into an overall ESI Preservation management solution, should satisfy Rule 37(e)’s “reasonable steps.” In other words, implementing and following the Guidelines will show that a party has taken the reasonable steps to navigate to the safe harbor described in the rule.

Rule 37(e) is now a proposed rule. It represents, however, more than four years of efforts by the Advisory Committee on Federal Rules of Civil Procedure. If the rule-making stays on course, the new Rule will be effective on December 1, 2015.

(c) The Trigger & the Process.

The *Sedona Commentary* writers split the Legal Hold process into the Trigger Events and the Preservation Process.

<p>Trigger Events and Reporting Channels</p> <p>< CLICK TO READ AND REVIEW ></p> <p>Ver. 1.0 (Sept. 4, 2014)</p>
<p>HOLD • PRESERVE • COMPLY</p> <p>Legal Holds and ESI Preservation Management</p> <p>< CLICK TO ACCESS ></p> <p>(Authorized Access Only)</p>

Returning to our Information Governance Portal, clicking on the Trigger Events opens a bullet point-list of the events that will cause the business to commence a Legal Hold.

This list is likely limited, and provides straight-forward directions for reporting an event to the person or persons responsible for implementing the Legal Hold. Where appropriate, the Trigger Events identifies bright line criteria. For example, if a business is served with the Complaint in a civil action, then a Legal Hold should be implemented; the same result might follow if the business receives a written threat of litigation from an opposing attorney. When the criteria are not so clear, the Trigger Events should at least identify a reporting process so that when there are close calls a Hold versus No Hold decision is made by the business legal department.

(d) ESI Preservation Management Solution.

The remaining component for the third cornerstone is an ESI Preservation Management solution. The requirements for this solution are detailed in J. Kurz, *A Trial Lawyer's Wish List: A Legal Hold and Data Preservation Management Solution* (accessed from the eDiscovery page on the Redmon, Peyton & Braswell website (www.RPB-law.com)).

The *Wish List* paper, which is in significant part based on the *Sedona Commentary's Guidelines*, is the blueprint for a proof-of-concept online SAAS system aptly named HOLD•PRESERVE•COMPLY. The system was built using Microsoft's Visual studio tool, and operates on SQL database. It is supported remotely by a third-party hosting vendor.

At the core of the HOLD•PRESERVE•COMPLY design is the Legal Hold, which is described above. The *Commentary* at Guideline 8(d) advises that a Hold Program is most effective when it . . . “[c]learly defines what information is to be preserved and how the preservation is to be undertaken.” Under HOLD•PRESERVE•COMPLY, each matter has a separate Hold Program, which includes the set of discrete tasks for plan implementation and then lifecycle management from inception through to eventual shutdown. A Hold Program is constructed and managed in stages. Part of the design is maintenance of comprehensive records of each Hold Program, an audit trail, and the availability of specially designed courtroom-ready reports.

HOLD•PRESERVE•COMPLY is a compliance tool intended to meet the “reasonable steps” requirement now embodied in proposed Rule 37(e). Its purpose is to provide the processes, supported by the necessary tools, for companies to (1) comply with the duty to preserve relevant records when litigation is at hand, when litigation is reasonably anticipated or when regulation or statute requires preservation, (2) be positioned for eDiscovery when matters cross into litigation, and (3) deliver courtroom-ready proof of the process itself and adherence to process.

SUMMARY

ESI preservation has moved to center stage in commercial litigation. The courts recognize a duty to preserve ESI, and we have a developed body of case law addressing ESI spoliation. With proposed FRCP Rule 37(e) on the horizon, businesses, both small and large, should be implementing Information Governance programs.

This White Paper identifies the cornerstones for an Information Governance program. These are first, the deployment of an Information Governance Portal. The second cornerstone component is a 2-part Record Retention Policy, a policy that includes a Record Retention Schedule and a disciplined ESI deletion practice. Based on the *Arthur Anderson* case and its progeny, an explicit and preferably written Record Retention Policy can be an effective shield against spoliation accusations.

The remaining cornerstone is the implementation of Trigger Events and an ESI preservation management solution that meets the “reasonable steps” criteria of proposed Rule 37(e). Once the duty to preserve arises because there is a reasonable anticipation of litigation, a business will rely on its ESI preservation management solution to invoke the Rule 37(e) protections against spoliation sanctions. While the “reasonable steps” criteria are only vaguely identified in the rule language, the Committee Note and the Sedona Conference's *Commentary on Legal Holds* provide guidelines for developing a legally-defensible solution.

ABOUT REDMON, PEYTON & BRASWELL LLP

Redmon, Peyton & Braswell LLP is, by design, a small law firm in Alexandria, Virginia, less than seven miles from the U.S. Capitol. Many of the Firm's attorneys practiced previously with AmLaw 100 firms. Our goal is to provide the same quality representation that clients expect from a large law firm but at substantially lower costs. We strive to solve our clients' problems in economically sensible ways.

Our lawyers are recognized as SuperLawyers and Rising Stars, listed among the Legal Elite and the Best Lawyers in America, and rated AV® Preeminent by their peers. We include among us a former U.S. Supreme Court law clerk and law professor, and federal Courts of Appeals and District Court law clerks. Attorneys from the Firm have served as presidents of the Alexandria Bar Association, the Federal Bar Association (Northern Virginia Chapter), and the Northern Virginia Bankruptcy Bar Association. Our lawyers practice across the Washington, D.C. metropolitan area, primarily in Northern Virginia.

The Firm's Commercial Litigation practice takes us into areas of eDiscovery, ESI Preservation and Information Governance. We advise our clients, including many smaller and mid-sized businesses, on compliance with ESI preservation duties. Our web-based ESI Preservation management solution,

HOLD•PRESERVE•COMPLY, provides a low-cost method to meet increasing preservation obligations in both federal and state court litigation. In the broader field of Information Governance, we counsel businesses regarding email and record retention policies, legacy and cloud data management, and social media and BYOD practices.

THE AUTHORS

James S. Kurz

James Kurz's law practice builds on his experience as a litigation partner with two AmLaw 100 firms, his time as a federal prosecutor, and his work as a federal government antitrust attorney. He has extensive courtroom experience (including more than 180 trials to verdict) that include computer, software and communications technologies cases. Central to his law practice today are the challenges of eDiscovery and the complexities of Information Governance.

Rebecca Larson

Rebecca Larson's law practice focuses on the areas of commercial litigation, eDiscovery, real estate and criminal defense. Ms. Larson clerked with the Cook County State's Attorney's Office in Markham, Illinois for three years during college and law school and with the Massachusetts Attorney General's Office in Boston.



REDMON, PEYTON & BRASWELL LLP

510 King Street • Suite 301 • Alexandria, VA 22314

(703) 684-2000 • www.rpb-law.com

Visit the EDVA Update Blog at www.rpb-law.com/EDVAUpdate