Controlling E-Discovery

Drafting an Effective Records-Management Policy

By John J. Jablonski
and Phillip J. Duffy

Even small steps to ensure compliance can go a long way toward protecting a company in the long run.

Having a solid records-management policy and records-management program is critically important for companies of all shapes and sizes. As courts continue to issue lengthy judicial opinions sanctioning litigants for failing to preserve potentially relevant documents and data, companies have become cognizant of the importance of issuing and complying with carefully tailored records management policies. Having a systematic, well documented, and thoughtful business approach to retaining, managing, and ultimately destroying expired, obsolete, or temporary records is often the best defense to allegations of spoliation when an opponent seeks sanctions for missing documents or electronically stored information (ESI).

Records-Management Policies Are Important

A records-management policy supports the good-faith efforts of a company to retain and dispose of records in a documented, systematic manner. A records-management policy guides a company by identifying the "official" records of the company, who custodians of official records are, and the company's policy toward all other records, often called "unofficial" records or "non-records." A records-management policy defines retention periods for records needed for various legitimate business purposes such as (1) keeping records as long as necessary to comply with legal and regulatory requirements, (2) keeping records used by a company to conduct business, (3) minimizing the volume of duplicate copies of records, (4) reducing storage and maintenance costs, (5) ensuring the timely disposal of information copies and other nonessential records, (6) creating procedures to dispose of expired or obsolete records systematically that no longer reflect a company's current business practices, (7) helping employees comply with the policy, and (8) implementing effective legal holds and preserving records when required because of a lawsuit or investigation.

With increasing frequency, clients ask attorneys to assist them to develop and

■ John J. Jablonski is the chair of Goldberg Segalla's E-Discovery Practice Group and concentrates his practice on commercial and business litigation, developing records management and legal hold policies and procedures, counseling companies on defensible preservation practices, and supporting trial teams on e-discovery issues. He is currently the vice chair of DRI's Electronic Discovery Committee. Phillip J. Duffy is a director in the Products Liability Department at Gibbons P.C. in Newark, New Jersey. He is a founding member of the firm's Electronic Discovery Task Force and an active member of DRI's Electronic Discovery Committee.

implement these policies. So it is particularly important for attorneys to understand the importance of good records management, the benefits of having a defensible policy, and to learn some of the key provisions that go into a well-crafted records-management policy.

For one thing, a records-management policy can control e-discovery. Gaining control of company data is critical, and this is best accomplished by developing and implementing a written records-management policy. A comprehensive records-management policy is an effective step toward ensuring compliance with future e-discovery obligations. In fact, a well-crafted policy not only will help ensure that a company meets its preservation obligations, but it may insulate a company from sanctions. Federal Rule of Civil Procedure 37(f) provides a limited "safe harbor" prohibiting the imposition of sanctions under the rules absent exceptional circumstances if a party loses ESI as a result of the "routine, good faith operation" of an electronic information system. Courts will more likely than not deem an electronic system as operating in good faith when a well-constructed records-management policy undergirds the system's operation. Moreover, in addition to thwarting spoliation sanctions, having an effective records-management policy is rapidly transforming from a best practice to a required one. Indeed, the Internal Revenue Service (IRS) recently revised Form 990, the annual information return filed by most publicly supported exempt organizations, to include several questions regarding corporate governance, board structure, and organizational policies, one of which specifically asks an exempt organization whether it has a written document retention policy in place. For all of these reasons, it is important for companies to develop written records-management policies.

Creating an Effective Records-Management Policy

To create an effective records-management policy the creators need to understand the principles of records management and generally accepted record-keeping principles. Luckily professional organizations offer reputable resources that an attorney or a company can refer to begin to develop this essential knowledge. First, however, we need to define "records" preliminarily.

Defining "Records"

The Federal Records Act, 44 U.S. Code 3301, although not strictly speaking applicable, provides a useful definition of records. It defines U.S. government records as

> all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by [an agency] in connection with the transaction of public business and preserved or appropriate for preservation by [the agency] as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them.

Principles of Records Management

While many recent spoliation cases provide detailed guidance on legally defensible document preservation methods, little case law exists that defines acceptable record-keeping practices. Lawyers are nevertheless called upon more and more to offer legal opinions related to records-management policies and records-retention schedules. The principles associated with good record-keeping practices are derived from a number of sources.

The goals of a properly constructed records-management policy are multifaceted. First, the policy should address all five stages of the information life cycle—creation, identification, retention, retrieval, and ultimate disposition—for both electronic and hard copy records. Second, a policy should account for existing regulatory-based preservation obligations, as well as those dictated by a company's business needs and potential litigation risks. Third, a policy should contain well-defined procedures for suspending routine computer operations that might overwrite or destroy data when complying with preservation obligations related to a legal hold, such as those imposed by actual or reasonably anticipated litigation, governmental investigations or audits.

Creating a comprehensive records-management policy involves carefully assessing corporate electronic data and storage practices. An ideal policy should retain the records necessary for business purposes and to satisfy legal and regulatory obligations and discard the remainder. Accomplishing this is easier said than done and requires a company to reconcile the competing interests and the inevitable clash of mindsets. For example, it is certainly not uncommon for information technology professionals to want to keep multiple backup copies of data in case of a disaster and for other reasons, while legal counsel usually focus on retaining only those documents necessary to meet legal requirements. So the best document retention policies usually result from extensive collaboration among in-house counsel, business personnel, IT specialists, and outside counsel. It is also important that employees understand up front that a company's records-management policy has the support of the company board, C-level executives, or both.

The components of a successful program are the following. The policy should be clearly written and easily understandable by all employees. The policy should identify specific categories of documents and assign appropriate retention and destruction schedules. It should, to the extent possible, identify the personnel responsible for performing key retention and destruction-related tasks. Moreover, the policy should prescribe and define chains of reporting, documentation, and accountability.

Before finalizing a policy, it is important to circulate the policy among key players to obtain the kind of useful comments and suggestions that will allow a company to implement the policy successfully. Document retention policies are not one-size-fits-all exercises. Understanding corporate culture is paramount to drafting an appropriate and successful policy "individualized" to a company so that it will use terms that all employees understand. Feedback allows a drafter to make a policy more specific and tailor it to the needs of a company and generally contributes to the kind of overall "buy in" at all levels necessary to ensure successful implementation.

"Generally Accepted Recordkeeping Principles"

ARMA International released "Generally Accepted Recordkeeping Principles,"

(GARP), in 2009. *See* The Generally Accepted Recordkeeping Principles, http://www.arma.org/garp/. ARMA International is a nonprofit professional association and a recognized authority on managing records and information. GARP provides a useful framework for attorneys asked to assist clients with revising or preparing records-management policies. These principles were developed by leading industry experts and are similar but not as detailed as the "Generally Accepted Accounting Principles." The GARP principles are designed to provide a theoretical framework for the development, implementation, and audit of record-keeping programs around the world. The eight principles are comprehensive in scope but general in nature. They are not intended to serve as a legal rule. They outline the characteristics of an effective record-keeping program but they do it flexibly, recognizing an organization's unique circumstances due to size, sophistication, legal environment, or resources.

Courts will more likely than not deem an electronic system as operating in good faith when a well-constructed records-management policy undergirds the system's operation.

The GARP principles follow.

- Preamble
  Records and recordkeeping are inextricably linked with any organized activity. It is only through the information an organization records in the normal course of business that it can know what it has done and effectively plan what it will do in the future. As a key resource in the operation of any organization, records must be created, organized, secured, maintained, and used in a way that effectively supports the activity of that organization, including:
  - Facilitating and sustaining day-to-day operations
  - Supporting predictive activities such as budgeting and planning
  - Assisting in answering questions about past decisions and activities
  - Demonstrating and documenting compliance with applicable laws, regulations, and standards
- Principle of Accountability
  An organization shall assign a senior executive who will oversee a recordkeeping program and delegate program responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and ensure program auditability.
- Principle of Integrity
  A recordkeeping program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability.
- Principle of Protection
  A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity.
- Principle of Compliance
  The recordkeeping program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization's policies.
- Principle of Availability
  An organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.
- Principle of Retention
  An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements.
- Principle of Disposition
  An organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.
- Principle of Transparency
  The processes and activities of an organization's recordkeeping program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties.

ARMA International, Generally Accepted Recordkeeping Principles®, *available at* http://www.arma.org/garp/ (last visited Jan. 19, 2011).

ISO 15489-1 Information and Documentation—Records Management—General

Additional reputable guidance is available through the International Organization for Standardization (ISO), which provides guidance on various industry specific topics. With the help of ARMA International, ISO 15489-1 was published in 2001. International Standard ISO 15489-1, Information and documentation—Records management—General (2001) provides worldwide best practices guidance on records-management principles. Its implementing companion standard, ISO 15489-2, Information and documentation—Records management—Guidelines (2001), provides guidance on creating and implementing records-management programs. These standards and guidelines are internationally recognized as providing a responsible framework in which to manage an organization's records.

ISO 15489-1 defines "records" as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business." Specifically, the standard states that

> [r]ecords contain information that is a valuable resource and an important business asset. A systematic approach to the management of records is essential for organizations and society to protect and preserve records as evidence of actions. A records management system results in a source of information about business activities that can support subsequent activities and business decisions, as well as ensuring accountability to present and future stakeholders.

Legitimate Systematic Destruction of Records Is Legal

As the Supreme Court has noted, "[d]ocu-

ment 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. 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, 704 (2005) (internal citation and quotation marks omitted). As a result "a party can only be sanctioned for destroying evidence if it had a duty to preserve it." *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003). The tricks are to know when a company can legally destroy records and when it cannot and to craft a records-management policy and a document-retention policy that appropriately makes the distinction.

A Company Should Train Employees on and Ensure That They Comply with a Document-Retention Policy

Once a company has prepared, circulated, vetted, and implemented a document-retention policy, the company should republish it at regular intervals. A company should offer training to employees on how to implement the policy so that they clearly understand their document-management duties and responsibilities. A company should document that this training took place. Moreover, a company should periodically monitor employee compliance and document that monitoring took place. Every so often a company should revise and modify the policy as the company's needs or experiences dictate.

A company also should provide copies of the company's document-retention policy during training sessions for new hires and reissue it during refresher courses as necessary. A well-drafted policy complemented by consistent monitoring and enforcement, builds a culture of compliance that will serve a company well in the event of litigation.

Organizations Must Plan in Advance for Litigation Eventualities

E-discovery is here to stay. The sheer volume of ESI is staggering. A company must have "at the ready" an in-house or hired technology expert to help preserve, collect, and produce ESI. A company must plan in advance for the eventuality of litigation. Under the e-discovery amendments to the Federal Rules of Civil Procedure once a party files a lawsuit in a federal court the litigating parties must analyze the existence and relevance of ESI within 90 days. This offers litigants very little time to prepare for the mandatory meet and confer unless they have already considered that they might face litigation at some point. An organization ideally should have an adequate e-discovery plan in place before someone sues the organization. We recommend making this a number one priority.

Without a prelitigation e-discovery plan in place, an organization risks sanctions and other intangible losses when sued. For example, in one discovery dispute the court ordered the defendant to participate in depositions relating to the defendant's *entire* data storage system to help the plaintiff develop a search protocol for searching the defendant's electronic claim files. In *Zurich Am. Ins. Co. v. Ace Am. Reins. Co.*, No. 05 CIV 9170 RMB JCF, 2006 WL 3771090 (S.D.N.Y. Dec. 22, 2006), the defendant submitted an affidavit of the individual responsible for handling the defendant's claims, which included the claim involving the plaintiff. The affidavit stated that the defendant's computer system could not segregate claims by the amount of the claim, the type of claim, or the reason that the defendant may have denied the claim, although the defendant processed thousands of claims.

The court held that a "sophisticated [entity] that operates a multimillion dollar business is entitled to *little sympathy* for utilizing an opaque data storage system, particularly when, by the nature of its business, it can reasonably anticipate frequent litigation." The court recognized, however, that the volume of data rendered searching the entire database infeasible. The court ordered the parties to propose a protocol for sampling the relevant claim files. To facilitate the process, the plaintiff was permitted to depose the affiant mentioned above and other persons familiar with the defendant's data-storage system. The court ordered the defendant to support objections to the sampling proposal with "specific evidence of the cost and burden involved." If the defendant had considered litigation needs before litigation actually happened, the court may not have ordered depositions about the defendant's entire data-storage system and saved the defendant the costly e-discovery that certainly followed.

A Good Litigation Hold Policy Is Critical to Preservation Success

By now the courts have made it generally understood that parties must take reasonable and good-faith efforts to preserve electronic evidence and documents that may be relevant to pending or threatened litigation and that issuing a written legal hold directive is a critical first step in attempting to meet this obligation. Therefore, a good records-retention policy must clearly include and ensure that a company issues timely legal holds and educates employees about the importance and general mechanics of legal holds. Although a legal hold directive will vary with the circumstances, a successful legal hold policy has several standard components that a company should incorporate into or at least reference in the company document-retention policy to the extent possible.

A legal hold policy, also called a litigation hold, a records hold, or a hold order, is a necessary component of a records-management policy. A legal hold policy should include language that protects a company and limits the legal hold obligation to its appropriate circumstances. The policy should specify that the scope of a legal hold shall be reasonable considering the issues, actual or anticipated claims, defenses, and pertinent time periods. It should further specify that a company shall only distribute a legal hold notice to key custodians, meaning those employees, departments, other individuals, or entities which the company has identified as potentially having possession, custody, or control of documents or data that may fall within the scope of the hold as the company deems necessary.

All Employees Must Work from the Same Legal Hold Map

A company should advise the company employees through appropriate policy provisions that, at the company's discretion, the company may apply company policies and procedures to preserve documents and data for legal purposes when warranted. Employees should understand that a legal

hold simply means that they must preserve and must not destroy certain information. A company should direct company employees that the legal hold policy (1) shall apply to documents regardless of form or storage medium, and specifically includes electronically stored information as well as paper documents; (2) shall take priority over the company's document-retention policy any time the company issues a legal hold notice; (3) shall not impose any duty or obligations beyond those imposed by applicable law or regulations; and (4) may be reviewed or revised at any time by the company. A legal hold policy should also explain to employees the circumstances under which a company may issue a legal hold. To this end, a company should advise employees that the company shall suspend its document-retention policy and issue a legal hold notice when the company (1) learns of pending litigation, (2) is notified of a credible threat of litigation, or (3) learns of another legal duty to preserve documents or data.

Having an effective records-management policy is rapidly transforming from a best practice to a required one.

Recent Legal Hold Case Law

Recently, a number of courts have issued significant judicial opinions directly addressing legal holds. These cases detail steps that various courts around the country deem necessary to evidence preservation. A court may sanction a company if it does not take some basic steps to support issuing a legal hold when a company reasonably anticipates litigation.

Judge Shira Scheindlin, well known to litigation attorneys preserving evidence, issued a series of seminal opinions that defined a legal hold in the *Zubulake v. UBS Warburg* case in 2004 and 2005. Courts throughout the United States have widely cited the *Zubulake* opinions in other opinions. Scheindlin "revisited" the preservation standards articulated in the *Zubulake* cases in an 89-page comprehensive legal hold opinion in *The Pension Comm. v. Banc of America Sec.*, No. 05 Civ. 9016 (SAS), 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010), even subtitling the opinion "Zubulake: Six Years Later."

In the *Pension Committee* opinion, Scheindlin reiterated many of the concerns raised by the *Zubulake* case six years earlier. In the *Pension Committee* case tremendous legal resources were devoted to arguments over the shoddy legal hold efforts of a group of plaintiffs. The plaintiffs' failure to issue timely legal hold notices and to enforce the legal holds properly now seriously jeopardize their case. Scheindlin concluded that an organization's failure to issue written legal holds will inevitably result in the destruction of relevant evidence.

Shortly thereafter, Judge Lee Rosenthal also called into question legal hold practices in *Rimkus v. Cammarata*, No. 07-cv-00405 (S.D. Tex. Feb. 19, 2010). The opinion singled out the need for better preservation practices to maintain the integrity of the judicial process. "Spoliation allegations and sanctions motions distract from the merits of a case, add costs to discovery, and delay resolution," wrote Rosenthal, who chose not to impose monetary sanctions based on the facts of the case, instead opting to instruct the jury about the defendants' willful destruction of evidence.

Two more recent cases reaffirm Scheindlin's position that the lack of written legal holds will inevitably lead to the wrongful destruction of relevant evidence. In *Crown Castle USA, Inc. v. Nudd Corp.*, No. 05-CV-6163T, 2010 WL 1286366 (W.D.N.Y. Mar. 31, 2010), the plaintiff failed to issue a legal hold resulting in the "wholesale destruction" of responsive ESI. The court deemed the behavior grossly negligent and compelled the plaintiff to undertake extensive effort to recover the lost data to avoid even harsher monetary sanctions.

In late April 2010, U.S. District Judge Richard Sullivan issued severe sanctions for a party's failure to issue a written legal hold in *Merck Eprova v. Gnosis*, No. 07-CV-5898 (RJS) 2010 WL 1631519 (S.D.N.Y. Apr. 20, 2010). Making frequent references to Scheindlin's *Pension Committee* opinion, the court declared, "[t]here is no doubt that Defendants failed to issue a legal hold" and deemed "this failure… a clear case of gross negligence." In addition to requiring the defendants to pay the plaintiff's legal fees and costs, Sullivan fined the defendants $25,000 "both to deter future misconduct… and to instill… some modicum of respect for the judicial process."

The need to issue a legal hold policy in conjunction with a records-management policy was made clear in *Jones v. Bremen High School*, No. 08 C 3548 (N.D. Ill. May 25, 2010). In *Jones* an Illinois court expressed complete dismay with the defendant's lackadaisical approach to records management. In this discrimination case, the defendant's actions included failing to issue a legal hold, adhere to a published document-retention program, and suspend automatic deletion of relevant electronic files. During discovery, the IT manager at the suburban Chicago school district testified about certain record-keeping practices that were at odds with the organization's publicly available records-management policy. This dichotomy did not sit well with the judge. Sanctions included special jury instructions and additional discovery costs.

Implementing a Good Legal Hold Involves Taking Seven Steps

Although courts often declare that preservation perfection is not the goal, spoliation cases do require companies to take reasonable and good-faith steps to prevent spoliation. The necessary steps are best understood as a seven-step business process. *See* John J. Isaza and John J. Jablonski, *Seven Steps for Legal Holds of ESI and Other Documents* (ARMA International 2009) (discussing legal holds in detail). The seven steps are as follows.

First, identify the trigger event. Issuing a legal hold becomes necessary when an organization "reasonably anticipates" litigation or regulatory action. Once the duty to preserve is triggered, an organization must take steps to ensure that it preserves potentially relevant data. Examples of typical trigger events include the filing of a lawsuit, a notice or threat of an intent to file a lawsuit, the occurrence of an events that typically will result in legal action such as a significant monetary loss, a severe injury or

death, a breach of a contract, or a product defect, or the filing of an employment claim an agency such as the U.S. Equal Employment Opportunity Commission. An often overlooked "trigger event" occurs when an organization first contemplates taking a legal action as a plaintiff.

Second, analyze the duty to preserve. Once an organization has identified the duty to preserve, the organization must determine if it needs to implement a legal hold. An organization's general counsel, chief compliance executive, or an outside counsel typically does the analysis leading to the decision to implement a legal hold. It is important to keep in mind that a court judges an organization's knowledge on a "knew or should have known" standard if spoliation occurs. If people exchange e-mails that say, "We are going to be sued over this," it is reasonable to assume that a court will view the exchange as a trigger event. Lawyers can crucially resolve ambiguities or close calls.

Third, define the scope of the legal hold. If an organization decides that it must preserve ESI and physical documents, the organization must define the scope of information that it will preserve. Custodians, meaning those individuals who have custody, ownership, or control over the information, must receive guidance about what information they need to preserve. Merely asking someone to "look for things to keep" or to "preserve relevant information" is insufficient to meet preservation obligations. Often defining the scope starts by identifying key players with direct knowledge of the specific legal matter. This will be a small group, but the number of individuals receiving hold instructions can be very large. For example, in an antitrust case a large multinational company could compel thousands of employees to preserve relevant e-mails and business records.

Fourth, implement the legal hold. The implementation phase has been garnering the most scrutiny by the courts in recent court opinions. For this reason, the standards have become much more stringent, stemming directly from Scheindlin's landmark *Pension Committee* opinion. It is becoming clear that issuing a timely written legal hold whenever litigation is anticipated probably is the only way for litigants to demonstrate that they have discharged their preservation obligations properly in federal courts. In the words of the *Pension Committee* opinion, "The failure to issue a *written* legal hold constitutes gross negligence."

Fifth, enforce and examine the effectiveness of the legal hold. Ensuring the legal hold process is effective once it is under way requires diligence and follow up. As with any form of effective communication, an organization must take steps to ensure and track the receipt, understanding, and acceptance of the custodians of their duty to preserve.

Sixth, modify the legal hold. Issuing a legal hold is rarely a "one and done" deal. A duty to preserve evidence evolves as new facts come to light. At this stage, attorneys familiar with a case leading to a legal hold should interview the key players to ascertain their involvement. Reviewing initial evidence, often referred to as "early evidence assessment," can help an organization understand the types and quantity of data that it may need to collect. The scope of a legal hold or the instructions for preserving data often changes as an organization gathers more information. New custodians may be identified, while others can be released from the duty to preserve if the situation warrants it.

Seventh, monitor and remove the legal hold. It is also important to continue to monitor a legal hold over time. At a minimum, a court will expect an organization to send periodic and routine reminders to custodians to ensure their ongoing awareness of the need to preserve data. When an organization expects custodians to continue to preserve data diligently, sending occasional reminders is certainly warranted. Once the duty to preserve no longer exists—a case settles, regulators conclude an investigation, or a trial resolves a case—the obligation to preserve relevant documents and data also goes away. At this point, it is important to remove the legal hold. An organization should send a notice to custodians releasing them from the obligation to preserve information and stating that the routine retention policies of the organization can be resumed. Further, an organization at that point can destroy expired documents and records as long as they do not fall within the scope of a concurrently pending but separate legal hold.

Creating an Effective Legal Hold Policy Involves Four Steps

A comprehensive records-management policy requires creating, implementing, and adhering to a legal hold policy. Here are steps that companies can take to protect themselves in light of recent case law.

First, deploy a legal hold management process. Ensure a consistent and defensible process is in place to reliably issue legal hold notifications and track custodial compliance with the hold instructions—and apply those processes consistently. As with information governance, reinforce that a transparent and repeatable process, consistently applied regardless of venue or type of legal matter, becomes far easier to defend than the actions of individuals. Having a reliable and consistent audit trail can also help.

Without a prelitigation e-discovery plan in place, an organization risks sanctions and other intangible losses when sued.

Second, establish a legal hold oversight committee if an organization hasn't already done so. Responding to a preservation obligation is an interdisciplinary exercise that should involve representatives from the records management, legal, information technology, and human resources departments as well as compliance administrators. Needless to say, having these groups learn to collaborate in the midst of a high-stakes legal or regulatory response is not an optimal strategy for success. Rather, put these teams in place today and establish a repeatable, documented process for invoking the team as needed.

Third, reassess and update information governance and a records-retention plan. Knowing where data resides that may become relevant to litigation or a government investigation in the future is critical to data preservation efforts. Responding in

Records Mgmt., continued on page 69

Records Mgmt., from page 23
a timely manner requires proactively establishing a process for identifying the data that an organization needs to preserve, where it resides, and who has responsibility for the data. Furthermore, a data-mapping process can help focus and prioritize information governance initiatives to reduce and eliminate obsolete or redundant data before a duty to preserve it arises. An effective legal hold management process also allows an organization to identify data repositories and areas of the organization quickly that others will want from an organization most frequently during litigation discovery and that an organization has a duty to preserve.

Fourth, educate employees about and train them on legal holds. An effective legal hold process depends on the actions of custodians and data stewards to suspend routine destruction or alteration of relevant data. A well-crafted legal hold notice that clearly and concisely instructs employees how to act and a process to ensure that they receive and understand a legal hold notice are critical elements of reasonable and good faith preservation. Organizations that educate and train employees will reap the investment benefits by improving the efficiency and effectiveness of their efforts. Look for opportunities to incorporate such training into new employee orientations or annual ethics and compliance training sessions. Introduce employees to sample legal holds and walk them through what an organization expects from them in response. Consider including a reference to legal holds in the employee policy and procedures handbook.

Conclusion

The old adage "an ounce of prevention is worth a pound of cure" is the best way to understand the role that a records-management policy plays in evidence preservation and ultimately the e-discovery process. In managing where an organization stores records, how long the organization keeps them, and when the company will destroy them, a company can effectively minimize its exposure to spoliation risks as well as minimize the costs of e-discovery. As shown, taking small steps to make sure a company complies with an existing records-management policy or creating a new more effective policy will go a long way toward protecting a company in the long run. FD