LJN'S
Product Liability
Law & Strategy®
LAW JOURNAL NEWSLETTERS
Volume 23, Number 6 • December 2004
ALM

# Ten Steps to an Effective Document Retention Program

**By Jennifer Smith Finnegan**

In the past, the implementation of a comprehensive document retention policy may have seemed a secondary concern at best; however, the primary importance to all companies of implementing such a policy was dramatically illustrated in 2002. That year brought the federal obstruction of justice conviction and ultimate demise of accounting firm Arthur Andersen for destruction of documents it knew were important to the SEC's investigation of the Enron scandal. It also brought the Sarbanes-Oxley Act of 2002, which significantly expanded the reach of federal obstruction statutes, increased the penalties for document destruction that hinders a federal investigation, and promulgated new record-keeping obligations. *See, e.g.* 18 U.S.C. 1519, 1520. Coupled with these developments are the ever-expanding obligations in connection with discovery of electronic information.

In this new legal climate, it is vital that every product design and manufacturing company take steps to implement and enforce a justifiable and uniform document retention policy that meets the company's business needs and also permits it to satisfy its legal obligations and minimize potential liability.

## What Not To Do: The Arthur Andersen Story

The Arthur Andersen story provides a template for what *not* to do with a document retention policy. In the face of investigations into Enron's improper accounting practices, one of Andersen's in-house attorneys reminded senior executives about the firm's document retention policy in an e-mail stating that it would be "helpful to make sure that we have complied with the policy." Four days later, Enron disclosed the $1.2 billion drop in previously reported equity of its shareholders, which was followed by commencement of an SEC investigation. At that point, Arthur Andersen executives ordered the immediate destruction of all Enron-related documents, purportedly in keeping with the document retention policy that, to date, had not been enforced. The hurried shredding of Enron documents did not stop until after Andersen received an SEC subpoena a few weeks later. This selective "compliance" with its document retention policy led to the firm's criminal conviction and demise. *See* Eichenwald, Kurt, *Andersen Misread Depths of the Government's Anger*, N.Y. Times, Mar. 18, 2002 at A1 and Johnson, Carrie and Peter Behr, *Andersen Guilty of Obstruction; Accounting Firm Will End Audit Work*, Wash. Post, Jun. 16, 2002 at A1.

If Andersen had consistently enforced a retention program, it is highly unlikely it would have been charged with obstruction, let alone convicted. As Judge Patrick E. Higginbotham wrote for the Fifth Circuit in June 2004 in affirming Andersen's conviction:

> There is nothing improper about following a document retention policy when there is no threat of an official investigation, even though one purpose of such a policy may be to withhold documents from unknown, future litigation. A company's sudden instruction to institute or energize a lazy document retention policy when it sees the investigators around the corner, on the other hand, is more easily viewed as improper. *United States v. Andersen*, __ F.3d __, 2004 U.S. App. LEXIS 11814, *41-42, 2004 WL 1344957, *12 (5th Cir. Jun. 16, 2004).

The lesson from the Andersen story, and many similar stories where companies have been sanctioned for document destruction in the context of litigation or government investigation, is that a comprehensive, consistently applied and enforced document retention policy is a must. This is particularly so for product design and manufacturing companies, which face myriad regulatory reporting and record-keeping requirements (depending upon their products) as well as the ever-present specter of product liability litigation or government inspection.

But why should a company have any document retention policy at all? If companies are exposed to ever-stricter criminal and civil liability for destroying documents that might someday be relevant to an investigation or litigation, why ever destroy any documents at all? The practical answer is that it would paralyze a business if it were required to maintain every record ever produced. The legal answer is in accord: The law does not require businesses to preserve every document ever created on the off chance it might someday be relevant to an investigation or litigation. *See Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003)

Instead, a company may institute and regularly enforce a document retention program that has a reasonable business purpose, such as promoting efficiency, reducing costs and assisting the business in its day-to-day operations, and it must

provide for the suspension of document destruction when the company knows or should know that the documents have become relevant to possible litigation or investigation. The following are 10 steps to developing and implementing an effective document retention policy:

1) Develop a written policy with schedules for document retention. A written policy should be developed that sets forth schedules for retention and destruction of records by defined categories. Employees from the business, legal and information technology departments should be consulted in developing and later implementing and enforcing the policy.

In defining the schedules, federal and state record-keeping statutes and regulations should be consulted first (*eg*, federal and state consumer product safety acts, occupational safety acts or other agency regulations), as should statutes of limitations and contractual obligations of the company to determine the minimum retention periods for categories of documents. Business necessity and industry norms then dictate any further retention periods beyond the legally defined minimums.

2) Identify company records. In connection with the first step, it is necessary to identify and locate the types and categories of records that the company has in order to determine what schedules should apply. Physical files should be located and identified throughout the company (with an eye toward eliminating unnecessary duplication of files). The company's IT department should be consulted to identify where and how electronic documents are stored. This task is not a small one, given the ever expanding amount of data that is generated and made accessible, as well as all the places that such data — particularly the ubiquitous e-mail — can "hide," *eg,* individual laptop or desktop hard drives, PDAs, floppy disks, backup tapes and employees' "personal" files.

While a companywide inventory may be particularly daunting, it is necessary to draft the document retention schedule comprehensively and then uniformly implement it. On the upside, the inventory has the added benefit of enabling the company to better harness its institutional knowledge for its day-to-day business operations.

***Not only should the files be categorized and maintained uniformly, but the security of the storage and filing systems of the company should be addressed as part of the policy.***

3) Take responsibility for document management. After the company's documents are identified and located, the company must ensure that they are maintained in a standardized manner so that they remain easily identifiable and locatable by subject matter, companywide. This is accomplished by providing a uniform protocol for filing and storing both paper and electronic files, thereby eliminating employee discretion as the basis for keeping track of company records.

4) Set up a secure storage system that preserves records. Not only should the files be categorized and maintained uniformly, but the security of the storage and filing systems of the company should be addressed as part of the policy. How would the company function if a fire destroyed the company's facilities overnight? The answer may be through offsite storage of physical and electronic files, *eg,* offsite computer servers or backup servers. The records kept at any offsite locations should be, of course, also subject to defined retention schedules.

5) Communicate the policy internally. Once the document retention policy is established, it must be communicated to all personnel, including to new employees as part of their orientation. It is a good idea to keep a running record of the distribution of the policy to each employee, as further proof of consistent and non-arbitrary enforcement of the policy companywide. Key employees responsible for product development or manufacturing guidelines also should be briefed on their specific responsibilities for maintaining the company's records regarding product design and manufacturing.

6) Establish rules for enforcement and training. A records retention policy that just sits on the shelf and is not routinely enforced is no policy at all. Indeed, a policy that is selective or enforced haphazardly may lead to enhanced liability. For example, in *In re Prudential Ins. Co. Sales Practices Litig.*, 169 F.R.D. 598, 613-17 (D.N.J. 1997), Prudential was fined more than $1 million when it destroyed documents due to a failure of its document retention policy, which the court found was not sufficiently implemented or enforced, particularly in the face of court orders requiring preservation and production of certain documents.

Because a records retention policy must be enforced and applied on a day-to-day basis by employees, regular employee training regarding records management is vital to the success and viability of the program. Equally vital is an enforcement mechanism to guarantee compliance. Employees can be sent routine destruction directives in keeping with the policy schedules and be required to respond that they have received, understood and complied with the directive. Enforcement policies should convey "zero-tolerance" of violations, including disciplinary action and possible termination if, for example, an employee hoards documents or destroys documents contrary to the retention schedule or a "hold" notice placed on destruction of documents.

7) Perform routine compliance audits. Routine audits by employees responsible for overseeing the

**Jennifer Smith Finnegan** practices in the litigation department of Herrick, Feinstein LLP in Princeton, NJ, and concentrates in product liability. Telephone: (609) 452-3800.

implementation of the policy are advisable. Not only do routine audits enable a company to monitor and enforce compliance with the program, they also provide a level of centralized control to ensure that the policy is being implemented consistently throughout the company.

8) Dispose of records as they become eligible. Of course, the final goal of the policy is to enable document disposal; accordingly documents *must* be routinely destroyed as soon as they become eligible. Lax enforcement or only periodic destruction of obsolete records can cause as much or more trouble than if there were no document retention policy at all.

9) Set up a "stop" or "hold" mechanism. Perhaps the most vital element of any document retention policy is a procedure for immediately suspending document destruction when the company learns or has reason to suspect that the documents may be relevant to possible or pending litigation or governmental proceeding. When such a situation arises, it is essential that a "hold" notice immediately be communicated to all employees advising them to preserve any records relating to the subject matter at issue and to cease any regularly scheduled document destruction for records relating thereto. If a company fails to stop destruction once it is or should be on notice of its duty to maintain and produce such records, it may be subject to monetary sanctions, an adverse inference jury instruction regarding the destruction or even a default judgment. *See Wm. T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984); *Carlucci v. PiperAircraft Corp.*, 102 F.R.D. 472, 486 (D. Fla. 1984), *aff'd* 775 F.2d 1440 (11th Cir. 1985).

In implementing an effective "hold" mechanism, procedures should be in place to ensure that the legal department is notified whenever there is a potential claim or investigation. Draft "hold" notice forms should be on file along with a regularly updated master list of contact information (e-mail addresses, telephone numbers and the like) for all employees to whom the "hold" notice should be addressed. Finally, the importance of "hold" notices and instructions on how to respond to one should be prominent in employee training.

***Lax enforcement or only periodic destruction of obsolete records can cause as much or more trouble than if there were no document retention policy at all.***

10) Regularly monitor and update the policy. Continual monitoring of the enforcement of the policy is necessary to make sure that the first nine steps are being followed consistently. The policy itself also should be periodically updated to account for changes in the law or the company's business needs. Constant vigilance is a must for establishing that the policy is, indeed, a good faith, business-related endeavor rather than a scheme to destroy "smoking guns" or conceal the truth. *See Lewy v. Remington Arms Co., Inc.*, 836 F.2d 1104, 1112 (8th Cir. 1988).

A comprehensive, consistently administered policy is not only a safeguard from legal liability for obstruction of justice, spoliation or violations of regulatory record-keeping requirements, but also is a tremendous benefit to the business side of the company. It will ultimately serve to reduce the cost of searching and storing documents as well as the cost of responding to investigations or requests for production. It will also improve and standardize internal knowledge management within the company. No company should be without one.

—❖—