

## **The Importance of Appropriate Record Retention Policies**

*Copyright © 2003 by Document Technologies, Inc.  
David Shub, Discovery and Records Management Director<sup>1</sup>*

With HIPAA, Sarbanes-Oxley, and various high-profile corporate fraud cases involving record destruction, national concern with record management and retention has reached new levels. In the resulting legal and business environment, it is more important than ever for firms and companies to develop and implement appropriate record retention policies. A sound policy ensures that records that serve important business or legal interests are maintained and remain relatively easy to access, while other records are not maintained longer than necessary and do not unnecessarily increase the difficulty and expense of record storage and access.

This article is the third of a three part series: the first article described potential document production obligations for attorneys; the second discussed steps in responding to electronic document requests; and this article involves an examination of the importance of record retention policies. Eight basic steps can guide an organization in developing a sound record retention policy:

1. Evaluate statutory requirements, litigation obligations, and business needs;
2. Classify types of records;
3. Determine retention periods and destruction practices;
4. Draft and justify record retention policy;
5. Train staff;
6. Audit retention and destruction practices;
7. Periodically review policy; and
8. Document policy, implementation, training, and audits.

### **Statutory Requirements, Litigation Obligations, and Business Needs**

State and federal laws and regulations impose many retention requirements. Among the many requirements are those of the Internal Revenue Service for tax-related records, the Securities and Exchange Commission for brokerage and accounting records, the Food and Drug Administration for pharmaceutical research records, and the Department of Health and Human Services for health care and health insurance records. Any particular law firm client may be subject to one or more of these or other agencies' record retention regulations. Other legal requirements apply more directly to personnel

departments of both law firms and their clients. An article in the August 2002 issue of the Law Office Management & Administration Report lists employment record retention requirements under nine laws that would apply to most firms and clients' personnel records.<sup>2</sup>

Other record retention obligations arise in the context of litigation. Besides a litigant's obligation to provide relevant documents to opposing parties' upon their appropriate request, every litigant must ensure that relevant documents are not purposefully or incidentally destroyed. In fact, that obligation arises as soon as litigation is anticipated, even if it has not yet begun.<sup>3</sup> A party must be especially careful if it routinely engages in rotation or erasure backup tapes or other storage media — it must interrupt its cyclical erasure procedure if there is reason to believe that responsive electronic records exist on those backups. This obligation applies even if erasure would otherwise be proper in the normal course of business. The penalty for failing to retain responsive documents may be as severe as “death penalty” civil sanctions — negative disposition of a material claim<sup>4</sup> or default judgment.<sup>5</sup> Less severe sanctions of adverse inferences, fines, costs, and fees may also be imposed.<sup>6</sup>

Finally, an organization must consider business reasons for maintaining records. Even when there is no legal obligation to retain a record, an organization may have a need for particular records, whether they are contracts, order forms, research memoranda, or important correspondence. Only by consulting with organization officers and department heads can a policy drafter ensure that records can be classified appropriately for storage and retention and scheduled appropriately for destruction.

### **Classification of Records**

An organization likely will decide that it needs to retain a large variety of records. To enable the organization to access the records when needed (and eventually when needed for destruction), the organization must classify the records into helpful categories. In addition to classifying for business use, an organization should consider the potential need for certain types of records in relation to future litigation.

When an organization enters litigation as either a plaintiff or a defendant, it will be called on to produce a variety of records. When the requested records include

electronic records, whether e-mail, word processing documents, or anything else stored electronically, the cost of complying with the record request can be dramatic, especially when servers are backed up to electronic tapes without regard to storing potentially relevant records in a grouped fashion.

Paper records should be stored through a centralized system that organizes records through folders, files, and subfiles in a manner chosen to best locate records when needed for retrieval, whether for use or destruction. Consider also that a single record may fit into multiple subfiles and there may be cases where an organization may be best served by storing copies of certain records in more than one place.

Electronic records present an equally complex issue. Certain electronic records may fit into similar categories as paper records, but certain types of electronic records, such as e-mails, web sites, and voicemails, may require additional categories. Specific record management software may help an organization to develop and implement classification categories for electronic records, and it may be easiest to follow those categories with regard to storage of any paper records.

### **Retention Periods and Destruction Practices**

As discussed above, certain records are legally required to be retained for given time periods. An organization may choose to retain those records just as long as required and then destroy them, or it may determine, for business reasons, that such records should be retained for some longer period. In any event, if the records are relevant to some anticipated or ongoing litigation, they may not be destroyed.

Those same considerations exist for all records. If there is no legal obligation to retain a record, the organization is free to choose the length of time it wishes to retain a record, except that no record may be destroyed if it is relevant for anticipated or ongoing litigation.

For every type of record, an organization must, in consultation with appropriate officers and department heads, determine the appropriate retention period. Certain records may have an infinite retention period, such as an organization's articles of incorporation. Others may be appropriate to destroy immediately, such as junk mail or e-mail.

An organization must not destroy records lightly or haphazardly. Ad-hoc or indiscriminate destruction of records will weaken the legal usefulness of a retention policy. Unless an organization can establish that it followed a documented retention policy faithfully, the record destructions are likely to be viewed as fraudulent efforts to destroy harmful evidence, subjecting the organization to sanctions discussed earlier.

Generally, individuals should not be permitted to destroy records. It may make sense to have one person responsible for all record destruction, or to have different people responsible for destruction for each category of records. It may be appropriate to have each individual who receives personal mail or junk mail to discard such records without other review. However, an organization should consider whether allowing such exceptions might lead to the inadvertent or otherwise improper destruction of an important record that could jeopardize the organization's business or legal interests.

Finally, an organization must be careful and thorough in destroying records. All copies of paper and electronic records must be located and destroyed. For paper documents stored in multiple files or subfiles, maintaining an index or cross-reference table would be helpful. For electronic documents, periodic cleansing of employee hard drives may be required to ensure that electronic copies of unwanted documents do not continue to linger, hidden until a forensic specialist uncovers them in the course of litigation discovery.

### **Drafting and Justifying the Policy**

With the guidelines established by the above steps, the organization should then draft its record retention policy, outlining the classification of records, retention and destruction schedules, parties responsible for retention and destruction, and procedures to be used for destruction. In addition to record management procedures and rules, the policy should include an explicit justification for those procedures and rules.

The justification should set out the sound business rationale for keeping certain records and destroying others. Among other appropriate grounds, the rationale may reference the business interests of: organizing records in a fashion that makes them easier to access, limiting the records retained to as few as possible to make searching for records as quick and inexpensive as possible, limiting the records retained to save on storage

expense (whether on-site or off-site storage of paper or electronic records), and limiting records retained to lessen the burden of keeping backup copies as protection against catastrophic loss. Failing to appropriately document an organization's rationale for keeping certain records and destroying others could subject an organization to the potentially extreme sanctions in the context of litigation discussed above.

### **Training Staff**

Staff training must be part of retention policy implementation. Every employee must be taught the importance of retaining records in accordance with the policy. The organization should stress that every record of the business, whether it is created or received in the office, while traveling, at home, or anywhere else, is subject to the policy. Equally important is the notion that individual employees should not destroy any record (except any which the policy specifically permits employees to destroy). Employees should know, with respect to e-mails and other electronic records, that for two reasons "deleting" a record does not destroy it – first, the record may exist elsewhere, such as on the employer's server; and second, a skilled computer forensic specialist will be able to recover many "deleted" electronic records from a computer's hard drive.

An organization should train employees as soon as the record retention policy is adopted and should train every new employee as part of the employee's initial training. Furthermore, the policy should set a schedule for continuing refresher training to ensure that employees remain vigilant with respect to their record retention obligations.

### **Audit Compliance**

An organization should conduct periodic audits to ensure that records are being retained and destroyed appropriately. Paper files and electronic storage media should be checked to ensure that records are not retained past their scheduled destruction dates. Conversely, hard drives may be spot-checked to ensure that improper efforts have not been made to "delete" records. The particular process used to audit compliance depends on the types of records that an organization generates and the storage methods used.

### **Periodic Review**

A record retention policy should not be entirely static. An organization's business need for different types of records may evolve. New laws or regulations governing record retention may apply to the organization. Laws or regulations may be altered or repealed. Feedback from organization employees or officers may show that records need to be categorized differently or that other alterations would be beneficial. Changes in the policy should be accompanied by appropriate training, whether of all employees or of those responsible for retention and destruction decisions, depending on the nature of a particular change.

### **Documentation**

Finally, it is crucial that an organization document all aspects of record retention policy implementation. Obviously, the policy itself must be written. Furthermore, the policy should be accompanied by a log that shows all training efforts, auditing processes and results, and record destruction schedules and actions. Every effort must be made to make the retention and destruction process as transparent as possible to prevent any suggestion of fraudulent or haphazard record destruction.

### **In Conclusion**

Record retention policies are vital to ensuring the preservation of necessary records and the limitation of unnecessary storage, retrieval, and litigation expense. Careful construction and implementation of such policies are necessary to protect against accusations of fraudulent destruction of records, but it is well worth taking that care to ensure that records are available when needed and not accessible once they are no longer needed.

---

<sup>1</sup> Formerly law clerk for the United States Court of Appeals for the Federal Circuit and securities litigation and banking attorney at the law firms of Wilmer, Cutler & Pickering in Washington, D.C., and Brooks, Pierce, McLendon, Humphrey & Leonard in Greensboro, N.C.

<sup>2</sup> "Records Retention Policies: Now More Important than Ever," Law Office Management & Administration Report, at 7 (August 2002) (describing record retention periods under the Fair Labor Standards Act, the Employee Retirement Income Security Act, the Family and Medical Leave Act, Title VII of the 1964 Civil Rights Act, the Americans with Disabilities Act, the Age Discrimination in

---

Employment Act, the Consolidated Omnibus Budget Reconciliation Act of 1985, the Immigration Reform and Control Act, and the Employee Polygraph Protection Act).

<sup>3</sup> See ABC Home Health Servs. v. IBM Corp., 158 F.R.D. 180 (S.D. Ga. 1994) (court finds that jury instruction that could give rise to an adverse inference would be appropriate where defendant erased computer's hard drive before complaint filed or discovery request served but where defendant actually anticipated litigation).

<sup>4</sup> See Residential Funding Corp. v. DeGeorge Financial Corp., 306 F.3d 99 (2<sup>nd</sup> Cir. 2002).

<sup>5</sup> Cabnetware, Inc. v. Sullivan, 1991 U.S. Dist. LEXIS 20329, at \*3-\*6 (E.D. Cal. July 15, 1991) (default judgment) Computer Assocs. Int'l, Inc. v. American Fundware, Inc., 133 F.R.D. 166 (D. Colo. 1990) (same).

<sup>6</sup> In re Prudential Ins. Co. Sale Practices Litig., 169 F.R.D. 598 (D.N.J. 1997); RKI, Inc. v. Grimes, 177 F. Supp. 2d 859 (N.D. Ill. 2001); Linnen v. A.H. Robins Co., 1999 Mass. Super. LEXIS 240 (June 16, 1999); see also Danis v. USN Communications, 2000 U.S. Dist. LEXIS 16900 (N.D. Ill. 2000).

