FOLEY

FOLEY & LARDNER LLP

DO YOUR RECORDS STORAGE AND RETENTION PRACTICES COMPLY WITH APPLICABLE LAW?

A Checklist to Assist Legal Compliance

As a result of Sarbanes-Oxley and recent amendments to the Federal Rules of Civil Procedure regarding discovery of electronic records ("e-discovery"), federal regulators, courts and companies are focusing more and more attention on records retention policies and practices. The following is a checklist to assist in determining whether a company's records retention policies and practices are designed to maximize compliance with applicable law in a cost-effective manner.

1. Implement a Records Retention Policy that addresses the new and clarified obligations under the recently amended "e-discovery" Federal Rules of Civil Procedures.

The Federal Rules of Civil Procedure were amended effective December 2006, adding numerous rules and regulations relating to electronic records, or as referred to in the Rules, electronically stored information (ESI). Among other things, the Rules require early treatment of e-discovery issues, as well as full and accurate disclosure of the existence of relevant ESI. If not properly planned, managed and coordinated, locating and producing ESI can become very time consuming and expensive. Failure to comply with the discovery rules can result in court imposed sanctions, fines and adverse rulings. Accordingly, it is critical for companies to develop accurate documentation describing its ESI practices and policies on the "front end," rather than dealing with these issues on an ad hoc, case-by-case basis after litigation has commenced.

2. Ensure the Records Retention Policy contains an up to date and legally accurate Retention Schedule.

An essential component of every Records Retention Policy is the Retention Schedule that identifies all different types and categories of records, and the required retention periods. The retention periods may be based on a statute, regulation or other law that mandates the record be retained for at least a specified period of time, or in the absence thereof, operational requirements dictating that records should be available for at least a certain length of time. Failure to utilize an accurate Retention Schedule can lead to premature destruction of records, resulting in legal fines and sanctions, and loss of information needed for the ongoing operations of the business. The company's Records Retention Policy should have a Retention Schedule that accurately and concisely identifies all different categories and types of paper and electronic records retained by the company, and legally compliant retention periods for each category or type of record.

3. Reconcile and coordinate email destruction policies and practices with retention requirements under applicable law and for on-going business operations.

Email explosion is a problem faced by every company. Confronted with growing storage costs and system performance issues, companies are limiting the amount of email that employees can keep. Tape backups typically do not keep a complete record of all emails. While limiting email volume is legally appropriate, and in many cases advisable, the company must also ensure employees (or an automated system) do not delete emails that are required for on-going business

operations or legal compliance. Companies should implement polices and practices for ensuring required emails are not prematurely destroyed, for example, by migrating or archiving required email records to a document management system, or secure networked data servers.

4. Ensure records relating to potential or pending legal claims, investigations or proceedings are not prematurely destroyed.

Improper destruction of records, or spoliation, can result in fines, sanctions, adverse legal rulings and other undesirable consequences. Even inadvertent destruction of records can lead to adverse results, particularly where the company's Records Retention Policy does not adequately deal with "litigation holds." The obligation to preserve records can arise before a lawsuit is initiated or a demand letter received. The Records Retention Policy should properly address the retention of relevant records, including timely notice to employees, compilation and production of records, and suspension of normal records destruction with respect to relevant records.

5. Current or active electronic records should be readily accessible and stored only in company approved locations.

Electronic records can be stored in a variety of locations – network servers, local hard drives, home computers, laptops, handheld devices, CD-ROMs, flash storage devices, web-based e-mail applications, online backup sites, etc. Multiple locations add to the difficulty and cost of locating and producing records, and increases the likelihood that records will be lost, not produced when they should be, and/or improperly disclosed to third parties not entitled to access the records. When a company is required to locate and produce electronic records in litigation (as a party or a third-party witness), it must search all locations for potentially relevant records, and produce those records. Companies should require storage or records in locations and in manners that facilitate prompt and cost-effective location and production, and consider limiting locations where electronic records may be stored by employees.

6. Develop a Data Map of all electronic records locations.

As discussed above, electronic records should be stored only in company approved and controlled locations. The next step is to create a Data Map or inventory of where all electronic records and other ESI is stored (e.g., file servers, email servers, identified drives, storage networks, removable media, etc.). This is important to facilitate the company in locating electronic records when they are needed for litigation or other legal proceedings. The Data Map is also critical to complying with the e-discovery rules which require early and proactive disclosure of electronic records and information regarding their location and accessibility.

7. Store records with appropriate safeguards to protect the security of company records and to protect the privacy of personal information.

An important aspect of records retention is how the records are being stored during retention. Electronic records often contain sensitive information valuable to the company, such as trade secrets, financial data, business plans and other confidential business information. Similarly, with the increase of legislation regulating privacy of personal information, companies are under increasing obligations to maintain the privacy of such data. Accordingly, the company

should implement and enforce policies and practices that protect the confidentiality, integrity and security of important business information and adequately protect the privacy of personal information.

8. Take steps to ensure compliance by outsource vendors.

Many companies use independent contractors and outsource functions and operations of the business, resulting in third parties having primary responsibility for storing, retaining and disposing of company records. Outsourced functions include areas such as information technology, accounting, human resources or other business processes. In such instances, the company should require the outsourcer to comply with the company's records management policies through appropriate contract language, monitoring, reporting by the outsourcer and periodic auditing of the outsourcer.

9. Implement policies and practices to ensure destruction of records in accordance with the Records Retention Policy.

The corollary to retention is destruction. In order to obtain the benefits of having a Policy and avoiding liability for improper destruction of records, it is necessary to destroy records in accordance with the Policy. The records destroyed by Arthur Andersen in the Enron matter were subject to destruction and could have been destroyed earlier. However, the records were not timely destroyed, but instead destroyed after notice of the investigation. The company should regularly destroy records in accordance with its Policy, subject to suspension of destruction pursuant to a litigation hold.

10. Educate and train employees about the importance of its records management policies and procedures, and monitor compliance.

Putting the proper Policy in place is just the first step. In order to obtain legal compliance and cost effective operations, the company should properly implement the policy with adequate employee training, and enforce the policies through appropriate monitoring and auditing activities.

11. Routinely update and audit compliance with the Records Retention Policy.

Having a good Records Retention Policy in place is a substantial part of compliance, but appropriate compliance efforts do not end there. Failure to properly implement, comply with and update a Policy can result in adverse and unintended consequences as severe, if not more, than failing to have a Policy at all. The Records Retention Policy should contain provisions addressing implementation of the Policy, as well as routine audits to ensure compliance and that the Policy is kept current.