FOLEY

FOLEY & LARDNER LLP

COMPLYING WITH E-DISCOVERY RULES

A Checklist to Assist Legal Compliance

The Federal Rules of Civil Procedure were amended effective December 1, 2006 to more fully address the rights and obligations of parties (and non-party witnesses) relating to the discovery of electronic records, or as referred to in the rules, electronically stored information (ESI). As a result of these "e-discovery rules," companies should take steps to ensure their policies and practices comply with the e-discovery rules and provide for cost effective compliance with the rules. The rules do not contain specific requirements for retention of ESI, but rather clarify and amplify the parties' rights and obligations with respect to the handling of e-discovery issues. The following checklist is intended to provide assistance in complying with e-discovery obligations in a timely and cost-effective manner.

1. Ensure the company's Records Retention Policy is designed to ensure cost effective compliance with the e-discovery rules.

Every company should have a Records Retention Policy that sets forth the company's policies and procedures pertaining to the storage, retention and disposal of records – paper and electronic. The Records Retention Policy should contain a retention schedule which identifies all of the various types and categories of records retained by the company, with a corresponding retention period dictated by legal or regulatory requirements, and in the absence thereof, business and operational requirements. Companies operating in multiple countries or receiving foreign data will need to anticipate the special requirements applicable to trans-border data flows, privacy protection and data security that might be involved in the receipt, retention, use, and disclosure of such information, both for general business purposes and for litigation purposes. The Records Retention Policy should accurately address storage, retention and disposal of electronic records, including compliance with the e-discovery rules.

2. Designate appropriate individuals with primary responsibility and accountability for proper storage, retention, location and production of electronic records.

One of the primary factors contributing to companies not complying with e-discovery requirements is the lack of responsibility and accountability for driving compliance. If an individual, such as a Compliance / Risk Manager, is not primarily responsible for coordinating and directing these activities, responsibility is diluted and diffused throughout the organization. While the individual can have other responsibilities consistent with or related to e-discovery and records management, the individual should have sufficient time and resources available to manage compliance, as well as the appropriate relationship with senior management and sufficient authority within the organization to compel compliance. Additionally, the company will be required to identify one or more persons who are knowledgeable about the company's ESI retention and destruction practices who will testify about such matters on the company's behalf. When assigning responsibility for its records retention and e-discovery activities, the company should consider who will be a good and suitable witness when depositions or other testimony is required.

3. Create a Data Map of the IT infrastructure and location of electronic records.

One of the fundamental changes resulting from the new e-discovery rules is the requirement that companies and their counsel be knowledgeable of the nature and location of ESI, as well as "key

players" within the company's IT organization. The ESI may be maintained on legacy systems no longer in active use. Parties and their counsel are also required to make complete and accurate disclosure of ESI, including the sources thereof. Companies have typically dealt with e-discovery on a case by case ad-hoc basis, dealing with the location and production of e-mails or other ESI as the need arose in the context of a particular case or investigation. The e-discovery rules require early and proactive treatment of e-discovery issues. In order to timely and cost effectively comply with the rules, companies should create a Data Map documenting their electronic records systems and infrastructure, including historical and legacy systems, so as to avoid recreating the wheel, inaccurate or late discovery disclosures, and the unneeded expenditure of excessive time, money, or other resources on electronic discovery.

4. Document e-discovery policies, procedures and expectations for litigation counsel.

Whether handled in-house or with outside counsel, the company should adopt a coordinated and consistent approach to dealing with e-discovery rights and obligations. Among other things, the new rules address proactive handling of e-discovery issues at the initial 26(f) attorneys' meeting, the initial 16(b) scheduling order, discovery requests and responses, the form of production of ESI, inadvertent production of privileged records, production of ESI that is "not readily accessible," (ref. number 8), and conditions on the production of ESI. Rather than having different attorneys handle e-discovery in disparate, and perhaps even conflicting manners, companies should consider what standards or baselines they desire in these areas, and document them accordingly.

5. Consider limiting the permissible storage locations and sources of electronic records.

Electronic records can be stored in numerous locations – network servers/drives, local hard drives, laptops, PDAs, wireless devices, CD-ROMs, USB drives, flash memory, home PCs, web-based e-mail applications, tape and other backup media, etc. Storing records in locations other than secure network servers increases (a) the costs and difficulty of locating records, (b) the likelihood of incomplete disclosure to the adverse party and the court, and (c) the risk that confidential, proprietary and sensitive records will be accessed by or disclosed to unauthorized third parties or competitors. Companies should seriously consider limiting the authorized locations and sources for electronic records, for example, by limiting storage to network drives, or prohibiting archival onto CD-ROM or other removable media, using remote (rather than local) access to records for laptop users, and/or prohibiting or limiting home PC use for company e-mail and the storage of company records.

6. Implement and document a logical and consistent backup / archival process.

Many of the court sanctions relating to e-discovery result from improper or inconsistent management of backup routines, such as the improper destruction of e-mails due to the recycling of backup tapes. As discussed above, litigation counsel will need complete and accurate information regarding the company's backup procedures. In some instances (refer to the safe harbor discussion in number 11, below), it may be necessary to suspend all or a portion of the backup system to avoid the improper destruction of electronic records. The company's policy documentation should accurately and completely describe the company's archival and backup systems, including tape backup frequency and recycle schedules.

7. Coordinate records retention archival functions with disaster recovery data backup functions (and recognize the distinction between the two).

Many companies confuse records retentions and archival with its electronic data backup procedures. Data backups are typically for disaster recovery and are "snap shots" of electronic data on the company's servers. Backups may be performed daily, weekly and monthly. The tapes containing shorter term data sets such as the dailies are then recycled, resulting in the data being overwritten and destroyed. Thus, if an e-mail was received Tuesday, and deleted Thursday, it would not be contained on any of the weekly backups generated on Sunday. This backup tape procedure is sufficient for disaster recovery purposes, but not for e-discovery and retention of ESI. Thus, the company should not rely on disaster recovery backup functions to satisfy its records retention obligations.

8. Assess and document which electronic records are readily accessible and which are not readily accessible.

The e-discovery rules provide that a party need not provide ESI from sources that the party identifies as not reasonably accessible because of undue burden or cost. Rather than making ad hoc or case by case assertions with respect to accessibility, the company should document in a logical and well-reasoned manner, which records are not reasonably accessible, for example, e-mails and other electronic records stored on backup tapes, and electronic information stored on a historical or legacy system no longer in active use by the company. This will bolster the company's position that if discovery of inaccessible electronic records is required, the cost should be borne by the requesting party. The not readily accessible designation must, however, be well-founded, and cannot be used indiscriminately as a tool to avoid or limit discovery obligations.

9. Document and implement effective litigation hold procedures.

Every company should implement a litigation hold policy, which can be a part of the Records Retention Policy. The litigation hold policy establishes procedures to avoid the improper destruction of records which are or may be relevant to a pending or reasonably foreseeable litigation claim, proceeding or investigation. Improper destruction of records relevant to a claim (or reasonably foreseeable claim) constitutes "spoliation," and may result in monetary fines, adverse evidentiary rulings and other sanctions against the company. The litigation hold must be effectively communicated to the "key players" – the employees who will be material witnesses in the litigation, as well as the employees within the company's IT organization involved in implementing any IT department aspects of the litigation hold procedure. Under certain circumstances, hard drives controlled by "key players" may need to be removed and stored, or copied by replicating an image of the hard drive. The litigation hold policy should include requirements for periodic reminders of pending holds, as well as audits to compel and document compliance. An effective litigation hold procedure is important to maximize potential advantages under the e-discovery good faith safe harbor (see ¶ 11, below).

10. Coordinate litigation hold procedures with automatic or routine e-mail destruction policies and systems.

Faced with growing storage costs and system performance issues, many companies limit the amount of email that employees can keep. As noted above (¶ 7), 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 automated systems) do not delete emails subject to a litigation hold. The e-mails may reside in an employee's inbox or other e-mail folders, which can be promptly captured and archived by the company's IT department as part of the litigation hold procedure. In the event on-going retention is required for e-mails sent and received during the litigation, the company should consider utilizing software to journal or capture e-mails from "key players." Effective e-mail retention and archival in coordination with data backup policies (¶ 6) will enhance the company's compliance with the e-discovery rules, permit continued operation of the company's email destruction policy, and reduce potential sanctions due to improper destruction of backup tapes (¶ 11).

11. Maximize the potential benefits under the good faith safe harbor.

Rule 37(f) provides that absent exceptional circumstances, a court may not impose sanctions for failing to provide ESI lost as a result of the routine, good faith operation of an electronic information system. While there has been much commentary but little court guidance so far on this rule, companies should maximize the potential benefits under this safe harbor. The Advisory Committee comments indicate a party cannot "exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific information that it is required to preserve." Factors noted by the Committee relevant to good faith include steps the party took to comply with a court order or agreement of the parties to preserve ESI, and whether the party reasonably believed that information on sources not reasonably accessible was likely to be discoverable and not available from reasonably accessible sources. In other words, if the party reasonably believes the information is available from other reasonably accessible sources, the party is able to argue it acted in good faith in allowing the continued operation of its electronic information system, including automatic or routine deletion or destruction of e-mails or other ESI on backup tapes.

12. 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 electronic records policies through appropriate contract language, monitoring, reporting by the outsourcer and periodic auditing of the outsourcer.

13. Enforce and audit electronic records retention and e-discovery policies.

Putting the proper policies 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.