
How to educate your workforce on the new federal rules regulating electronic discovery

The amendments to the Federal Rules of Civil Procedure regulating electronic discovery (e-discovery) have gone into effect as of December 1, 2006. These are some of the most profound changes to the federal rules in decades and directly focus on “electronically stored information” (ESI) and its discoverability in all federal lawsuits.¹ Some states have already enacted similar procedural rules, and it is expected that many other states will do so over the next year.

The federal rules were adopted because of the change from an analog to a digital world. The rulemakers understood that digital data is different from paper-based data in that it is dynamic and easily stored, even in great volume, and that it can also be easily destroyed or become “not reasonably accessible.”

Generally, the federal rules have not imposed *new* legal obligations on organizations but have codified case law and existing practices into formal rules. However, this codification requires rapid adoption of e-discovery policies and procedures by companies to ensure their compliance. These changes will significantly impact your business in practical terms. Failure to adapt to these changes can result in severe sanctions imposed by the courts on businesses.

Five key issues are important to understand about how these rules impact records management, controls and policies in companies. Suggested actions are provided to help ensure that your organization properly educates employees about the rules in order to remain in compliance with them.

What constitutes ESI

Rules 26 (a)(1), 33(d), 34(a), and 34(b) reference “electronically stored information” and broadly define it. As long as the information is “electronic” and “stored,” it is subject to discovery if relevant. Therefore, word processing documents, e-mails, spreadsheets, databases, instant messaging and voice

mail are considered ESI. Note also that “metadata” – embedded digital information that may store, among other things, files and their size, name, origin, history, and location in the computer system – are potential evidence in addition to files themselves and are thus considered ESI.

Duty to identify and preserve ESI

Organizations always have had the obligation to preserve relevant ESI when “litigation is pending, imminent, might occur or reasonably foreseeable.”² This legal obligation has existed for decades in the world of paper records but has been reaffirmed in the rules for electronic records. Therefore, a company is at great risk if relevant electronic information is deleted or altered, either intentionally or inadvertently, such as by recycling relevant backup tapes or taking any other actions that destroy data. The new rules do not address precisely how long data actually must be stored, and this issue remains to be addressed by the courts and by individual laws and regulations. Applicable times will vary based on a company’s industry, historical experience and potential litigation

For example, assume your employees use “instant messaging” that is subsequently stored to communicate about a particular business transaction and the organization assumes that litigation is “reasonably anticipated” regarding this transaction. In this scenario, the instant messaging information must be preserved for disclosure. Failure to do so could lead to significant court sanctions.

Though this issue seems easy and straightforward, a 2005 survey found that half of the organizations were either not at all confident or only slightly confident that their organization could actually demonstrate the accuracy of electronic records management systems for identification and preservation purposes.³ Companies must therefore make greater efforts to identify, preserve and segregate the storage media of

relevant electronic information when a lawsuit is reasonably anticipated.

Responsibility of corporate counsel

The new rules effectively impose important duties on organizations to ensure that their outside counsel are educated and prepared to discuss ESI issues at early attorney conferences and subsequent court hearings. This requires organizations to prepare a “blueprint” of what relevant ESI is available and to support their counsel at the pretrial “meet and confer” hearing. Identification of this ESI is also necessary for disclosure under the “initial disclosures” of Rule 26(a)(1)(B).

Judges will become impatient with counsel and companies that are not fully “up to speed” on these matters. Specifically, the new rules require the parties to confer early in a case to “discuss any issues relating to preserving discoverable information . . . any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced . . . any issues relating to claims of privilege or of protection as trial-preparation material, including – if the parties agree on a procedure to assert such claims after production – whether to ask the court to include their agreement in an order . . .”

One step therefore recommended is that companies set up a “rapid response e-discovery unit” to ensure the preservation of data and provide support to outside counsel in response to litigation.

Sanctions for failure to identify and preserve ESI

New Rule 37(f) provides that “[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide

electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”

At first glance, this rule seems to protect organizations that fail to preserve relevant information in a timely manner. However, this is not the case. The Committee Note to this rule explains that “[g]ood faith may require that a party intervene to modify or suspend certain features of the routine operation of a computer system to prevent the loss of information, if that information is subject to a preservation obligation.” This is commonly referred to as a “litigation hold.”

However, as described above, given that the organization may have had a “duty to preserve” specific evidence, the failure to do so may not provide protection under Rule 37. The precise contours of a valid litigation hold are outside the scope of this article but could typically include obligations to interview key witnesses, suspend document destruction policies, and many other obligations as set forth in federal case law. Companies must therefore have litigation hold policies and procedures in place to respond immediately in the event of a litigation trigger or notification to ensure that sanctions will not be imposed if data is lost.

Distinction between “accessible” and “not reasonably accessible” ESI

New Rule 26(b)(2) provides that “[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.” This rule embodies the principles set forth in the *Zubulake* decisions and protects companies that have preserved data in legacy systems,

backup tapes, etc. and where production would impose an undue burden or cost upon the organization.

However, companies will be required to provide evidence in the form of affidavits or other evidence from qualified IT/forensics specialists or experts that the data in question is “not reasonably accessible”

because of the cost or burden of translating or restoring the data. As a result, companies must better understand what data is stored where and be able to identify whether information is truly reasonably inaccessible.

*Written by Michael R. Arkfeld, Esq.,
an expert on e-discovery.*

1. In addition to the rules set forth here, there is the new Rule 45 that applies to non-parties to a lawsuit. This rule was expanded to provide for the discovery of electronically stored information from non-parties with provisions generally parallel to Rules 26 and 34.
2. Michael R. Arkfeld, *Electronic Discovery and Evidence*, § 7.9(d), *Duty to Preserve* (2006).
3. Cohasset and Associates 2005 Survey.

Implications for compliance education

These rules will be applied in all cases in federal court, and comparable rules soon will apply to many state court cases. It is important to follow them in order to avoid penalties and sanctions. Always remember that electronic data is as important as a paper document in terms of evidence in a case and must be treated accordingly.

Note that the rules on ESI need not be seen as a burden. In many situations, a litigant with detailed and accurate records will be at an advantage in either defending or pursuing claims. In evaluating record retention policies, one should not assume that preserving records necessarily results in an adverse outcome. Thus, the new rules, if followed, can have a positive value for organizations.

It is therefore recommended that companies establish clear policies that take into account the legal framework and the nature of their business (product, industry) and the company’s specific history in terms of litigation, government investigations and regulatory requirements. The resulting policies they establish regarding ESI must then be communicated in an effective manner to all responsible levels within the company, including managers and employees.

This means employees must be educated about the new regulations and about the importance of ESI in today’s legal environment. In particular, employees need to understand that seemingly casual acts of deleting or altering any type of ESI can have severe repercussions if a duty to preserve is present. Clearly employees are entitled to rely on their managers for guidance, but at the minimum, every

individual must realize that when a manager orders a litigation hold, evidence is to be preserved accordingly.

In addition, keep in mind that just because a company has established a policy and informed its employees, it cannot assume the policy will self-execute. The federal courts will expect reasonable monitoring to ensure effectiveness of the policy by testing it regularly and periodically refreshing employee education on ESI. Companies that are at high risk for litigation should run “fire drills” to make sure their preservation and retrieval processes work.



LRN Headquarters
1100 Glendon Avenue
Los Angeles, CA 90024-3503

New York Office
One East 52nd Street, Third Floor
New York, New York 10022

For more LRN papers, perspectives and research, please visit:

www.lrn.com

Or to learn how LRN can help create an effective ethics and compliance program,
contact us at: **800-529-6366** Toll-free **+1-310-209-5400** International