

EmailXtender and the U.S. Federal Rules of Civil Procedure

Get your e-mail house in order to comply with the Federal Rules of Civil Procedure

THE BIG PICTURE

- Prepare your company for litigation and align with the Federal Rules of Civil Procedure (FRCP) amendments
- Enforce e-mail retention policies and consistent, defensible processes for retention and litigation holds
- Reduce the complexity and number of sources of messaging information by eliminating unmanaged copies of messages, contacts, calendar items, and tasks
- Eliminate sources of inaccessible messaging data by managing the storage of historical e-mail
- Manage e-mail as a corporate record
- Store messages in native formats and preserve all message metadata, ensuring messages have evidentiary weight

Litigators often target e-mail for electronic discovery because, in many organizations, the e-mail system is a vast collection of potential business records. According to a survey by the Enterprise Strategy Group, 80 percent of discovery events involve e-mail, making it the most common source of electronic evidence (source: ESG Research Report, *Electronic Discovery Requirements Escalate*, November 2007). Companies that secure e-mail in a searchable archive, managed according to corporate retention rules, reduce both costs and risks associated with legal discovery. EMC® EmailXtender®, along with EMC's recommended best practices for addressing eDiscovery and compliance challenges,¹ can help your organization become litigation ready.

An overview of the Federal Rules of Civil Procedure

The U.S. Federal Rules of Civil Procedure (FRCP) specifies that “electronically stored information” is a formal category of discoverable information. These rules require an early conference to discuss any issues relating to discoverable information, including an inventory of information sources. Additionally, the FRCP requires that litigants be prepared to collect and maintain discoverable data in its native format.

Identification of sources

Prior to a request from a plaintiff, parties must either produce all relevant electronically stored information or provide a description and location of all such information (Rule 26(a)(1)(B)). A party also must provide a list of all sources that it is not searching due to inaccessibility (Rule 26(b)(2)(B)). Thus, parties must be armed, early in the litigation, with a comprehensive list of their sources of data in preparation for responding to these obligations.

Protection from sanctions

Rule 37(f) provides a limited “safe harbor” from sanctions when a party has acted in good faith, but potentially relevant information is still deleted by “routine, good-faith operations.” This rule is meant to cover circumstances where information is disposed of as part of normal business practices, such as during the scheduled recycling of backup tapes, dynamic updates of databases, automatic overwriting of deleted information, and the automatic deletion of e-mail.

Inaccessible data

A party does not have an initial obligation to produce electronic information that is “not reasonably accessible because of undue burden or cost,” but the party must identify the sources of data (see above) and be prepared to provide facts supporting the claim of undue burden or cost. Inaccessible sources might include backup tapes, “unintelligible” legacy data, deleted data, and nonstandard database output.

¹ *A Practical Enterprise Methodology for Addressing the Compliance Challenges of eDiscovery, eRetention Management and Defensible Disposition*, Andrew M. Cohen, Esq., EMC Corporation.

E-Discovery Amendments can be found on the website of the Administrative Office of the United States Courts. U.S. Courts, Federal Rulemaking:
www.uscourts.gov/rules/EDiscovery_w_Notes.pdf

Format of data

Rule 34(b) states that electronic information must be produced in the form in which it is ordinarily maintained or some other reasonably useable form. The requesting party may specify the form of production (for example, hard copy, .gif files, native format), and the responding party may object or specify the form in which it intends to produce data if the requesting party does not indicate a preference. This rule is designed to identify and efficiently resolve potential disputes before production occurs.

Early conference

Parties are required to confer before the scheduling conference to discuss any issues relating to the preservation of discoverable information. This could become a battleground in some cases as the parties maneuver to maximize the amount of data that the other side must preserve—with the significant risk of facing spoliation sanctions if they do not and the court rules against them.

How you can prepare for FRCP

To prepare for litigation, organizations need to establish e-mail retention policies, as well as consistent, defensible processes for retention and litigation hold. EmailXtender enforces these business policies and helps you adhere to the new rules by:

- Reducing the number of sources of messaging information
- Ensuring messaging information is accessible
- Disposing of messaging information when it no longer has business value
- Storing messages in their native format with all relevant metadata to meet requirements concerning format of data

Reduce sources of messaging information

A comprehensive e-mail archiving policy and implementation eliminates the complexity and sheer number of sources of messaging information. By ensuring all messaging information is in a secure EmailXtender archive, you can eliminate unmanaged copies of e-mail, instant messages, contacts, calendar items, and tasks in both personal archives and public folders. Additionally, an integrated backup, recovery, and archive strategy reduces the information saved on backup tapes.

Ensure messaging information is accessible

Your cross-functional discovery team should understand the different sources of information assets, the cost of accessing this information, and the likelihood that they contain responsive information. EmailXtender helps eliminate sources of inaccessible messaging data by managing the storage of historical e-mail. Access to all messages is through the archive versus convenience copies that can appear throughout the organization.

Manage e-mail as corporate records

Creating clear policies for message retention and disposition and enforcing these policies consistently with EmailXtender establishes routine, good-faith practices, and allows you to dispose of expired information safely. EmailXtender also helps ensure that a company does not have unmanaged convenience copies in sources such as PST files or Notes local archives.

Store messages in native format

EmailXtender stores messages in their native format with no changes in fidelity such that they can be retrieved and displayed accurately within any e-mail client. EmailXtender preserves all message metadata, which may be relevant to a discovery request, such as the time at which a message was sent and the recipients of a message.



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com

Take the next step

To find out more about how EMC can help you archive e-mail to align with the Federal Rules of Civil Procedure and assess litigation readiness for all your eCommunications, visit www.EMC.com or call **800.607.9546** (outside the U.S.: +1.925.600.5802).