

Regulation Overview

Federal Rules of Civil Procedure (FRCP)



FEDERAL RULES OF CIVIL PROCEDURE (FRCP)

The FRCP governs court procedures for civil lawsuits. Established in 1938, the FRCP has undergone multiple revisions over the years, with the most recent set of revisions made in December 2006. While the FRCP defines how parties should behave when participating in a lawsuit, the latest amendments provide practical changes in discovery rules for production of data. Specifically, the amendments detail what, how and when electronic data must be produced – including the new requirement of production as part of the pretrial process.

WHO IS AFFECTED BY THE FEDERAL RULES OF CIVIL PROCEDURE?

The FRCP is designed for the civil federal court system, with input from the U.S. Supreme Court, and approval by the U.S. Congress. Companies who are party to or may become party to lawsuits within the federal courts need to be prepared to meet the discovery requirements of FRCP. Further, while states make their own rules to apply within their own courts, many have adopted rules that are based on the FRCP. Therefore companies who become party to litigation within a given state court system may still be subject to the same discovery requirements as if they were in a federal court case.

WHAT ARE THE RELEVANT PORTIONS OF THE FRCP AMENDMENTS FOR eDISCOVERY?

The FRCP contains thirteen sections, broken into individual rules of conduct. Chapter V, Rules 26-37, covers the bulk of amendments and detailed procedures for eDiscovery and carries the most concern for companies because they require a detailed understanding within the organization of record retention policies and procedures, the knowledge of what data exists within the company, and where it resides. Such capability requires an archive for all electronic records, especially email, IM, and Bloomberg data; as well as the ability to quickly and comprehensively search the amassed archive in order to produce requested data within the FRCP time frames.

As of December 1, 2006, electronically-stored information is no longer automatically excluded from discovery requests. Instead, electronic records must now be included unless otherwise specified and discovery searches must include electronically stored information. In short, the new amendments to the FRCP require companies be able to:

- Find, collect, store and process documents so that the requesting (plaintiff) and the responding (defendant) parties can determine – pretrial – the scope of the discovery requests.
- Prevent the accidental, or willful, destruction of requested data once the litigation is pending.
- Determine what electronic data may not be “reasonably accessible” because of “undue burden or cost.”
- Provide validity of any claims of privilege on requested data.
- Set the parameters on how parties should handle inadvertently disclosed material that was deemed privileged.
- Produce the results of a discovery request within a specific timeframe or face fines and penalties.

WHEN ARE THE FEDERAL RULES OF CIVIL PROCEDURE TO BECOME LAW?

The amendments went into effect December 1, 2006.

WHAT ARE THE PENALTIES FOR FAILING TO ADHERE TO THE FEDERAL RULES OF CIVIL PROCEDURE?

Section V, Rule 37 “Failure to Make or Cooperate in Discovery; Sanctions” details the penalties when a party fails to produce requested information, fails to respond to or permit an inspection of requested data, or provides an incomplete disclosure of data (which is treated as a failure to disclose, answer or respond).

- When a failure to produce data has been determined by the court, the court can require the offending party to pay the expenses and attorney fees of the opponent.
- If the failure to respond occurs during deposition, the failure may be considered a contempt of court.
- If the responding party fails to obey a discovery order the court may
 - a) determine that the matter on which the request was based is accepted, i.e. because evidence was not produced to the contrary, the statement of fact the discovery order was meant to determine, is now established (the reverse of “innocent until proven guilty”).
 - b) refuse to allow the disobedient party to support or oppose claims or defenses, and prohibit the party from introducing other matters into evidence.
 - c) stay proceedings, dismiss the action, or find a judgment by default against the disobedient party.
- If the responding party fails to disclose data, or produces false, misleading or incomplete discovery results
 - a) The court may require payment of reasonable expenses, including attorney's fees, caused by the failure and may also impose sanctions such as informing the jury of the failure to make the disclosure.

While the penalties for non-production, and deliberate, or inadvertent, destruction of data have become more severe under the new amendments to the Federal Rules of Civil Procedure, a "safe harbor" provision has also been added to the FRCP. In Rule 37, paragraph (f), the provision prevents the court from imposing sanctions or penalties on a party for failing to provide electronically-stored information that was "lost as a result of routine, good faith operation of an electronic information system." In short, companies with a documented and enforced electronic data retention policy cannot be penalized for data loss which occurred during routine destruction of old data that was not previously marked for legal hold. Companies who show bad faith by inconsistent retention enforcement, willful data destruction or negligence in retention can be heavily sanctioned, fined or lose the case altogether.

HOW DO FIRMS COMPLY WITH THE FEDERAL RULES OF CIVIL PROCEDURE?

Preparing for litigation under the Federal Rules of Civil Procedure Recommendations should include implementing a set of best practices:

- Aggregate email, IM, Bloomberg, etc. into an archive: a centralized and manageable repository is significantly easier to maintain, control and search in the event of a discovery request. Consolidation of data reduces storage overhead, inadvertent data loss at the desktop level, as well as undue time and cost to search laptops, backup tapes and disparate data vaults.
- Implement enforceable retention policies: A consistent retention and destruction, policy reduces liability under the "safe harbor" clause. Removing control of retention from the hands of end-users will ensure that data destroyed in an appropriate and systematic way. More importantly, make sure that the archive solution offers a "legal hold" function to prevent electronic communications from being deleted once litigation is pending.
- Make sure you have a robust search engine: Just because a company has aggregated all the electronic data into the proverbial haystack by implementing an archive, it doesn't mean needles are easily found if the data is searchable at the most granular level. Full-text indexing of the archive, tagging messages with additional metadata, and establishing audit trails of usage are critical to the rapid search and complete production of relevant data.
- Have the ability to tag "privileged" communications: pre-tagging messages as "privileged," or case work product prevents inadvertent release of sensitive data as part of the discovery result. Further, the FRCP requires that any data withheld under privilege be called out in a separate statement, in order to establish validity of the claim. Archives that automatically generate "Privilege logs" as a corollary to the search result can alleviate time and cost in protecting privileged information.

HOW DOES ZL TECHNOLOGIES ADDRESS THE FEDERAL RULES OF CIVIL PROCEDURE?

ZL Technologies offers solutions for the complete capture, archiving, tagging, indexing and searching electronic records in the event of litigation, and for the routine management and retention of email, IM and Bloomberg communications. The ZL Unified Archive Suite offers:

- Comprehensive capture of mail, including BCCs and group list aliases
- Full-Text Indexing for granular search
- Pre-tagging and categorization of mail
- Attorney-client privilege flagging (Policy and Ad-hoc)
- Advanced retention policy creation
- Legal holds
- Global Single Instance Storage (SIS) for reduction of storage overhead
- One-click export to a variety of data formats

Companies may choose from a full suite of integrated modules, which reside on the ZL Email Management Platform, mixing and matching solutions to meet individual requirements.

ABOUT ZL TECHNOLOGIES

Established in 1999, ZL Technologies, Inc. (ZL) provides cutting-edge enterprise software solutions for email archiving, regulatory compliance, litigation support, corporate governance, content management, file archiving, and secure email. ZL's flagship product, the Unified Archive, offers comprehensive email and file archiving and management for companies using Lotus Notes/Domino, Microsoft Exchange, Bloomberg, and others. The suite provides a highly flexible framework that is fully scalable, enabling organizations of all sizes to meet legal discovery, compliance, and storage management requirements. With a proven track record and an impressive list of clients, including Walgreens, Bank of New York Mellon, Pacific Life, and Morgan Keegan, among other top global institutions, ZL has emerged as the premier provider of email archiving and compliance solutions. For more information, please visit www.ZLTI.com

To learn more about how ZL Technologies can help you take control of your data, call us at 408.240.8989 or visit us online at www.ZLTI.com