



## Top 10 Tips to Prepare for FRCP Changes

## Introduction

The recent changes to the Federal Rules of Civil Procedure (FRCP) focus on the rapidly evolving practice of electronic discovery before the federal courts. The modifications are intended to alleviate issues arising from production of electronically stored information.

The rules will have an impact on litigators, in-house counsel, and other attorneys with responsibility for providing companies with general corporate governance advice. The following 10 tips provide a practical approach to readiness under the Federal Rules.

### Tip #1: Read and Understand the Rules and the Committee Notes.

Lawyers who choose to ignore the rules or wait until they're engaged in litigation before earnestly perusing them will be at a distinct disadvantage. Several of the rules require action immediately upon the filing of a complaint or service of summons. Waiting to review these requirements until after litigation commences is not a viable option.

The rules to become intimately acquainted with include:

- **Rule 16**, which establishes process for the parties and court to address early issues pertaining to the disclosure and discovery of electronic information
- **Rule 26** which requires parties to discuss issues of electronic evidence at the discovery-planning conference—inadvertent waiver of privilege, preservation of evidence, form of production
- **Rule 33**, which specifically calls for a search of electronically stored information in answer to interrogatories involving review of business records
- **Rule 34**, which adds a new category of discoverable information called “electronically stored information” and gives options for form of production
- **Rule 37**, which creates a “safe harbor” should electronic evidence be lost because of routine operation of a company’s computer systems
- **Rule 45**, which outlines conditions for non-party production of electronically stored information
- **Form 35**, which includes the parties’ proposed discovery plan for electronically stored information

In addition to becoming familiar with the rules, counsel should take a look at the FRCP committee notes, which give specific examples and explain the rationale behind many of the rules. These notes are invaluable to lawyers who must prepare to take an active role in the production of their clients’ electronically stored documents.

### Tip #2: Become Familiar with Information Technology.

Very few lawyers have technical backgrounds or advanced training on computer storage systems. Those lawyers who are so trained may have an advantage in the short term. But any advantage will be short-lived because other lawyers will quickly come up to speed once they realize the necessity of doing so. The rules require that all lawyers become more familiar with the terminology used by IT personnel. A working knowledge of terms such

as “metadata,” “scrubbing,” and “de-duplication” is necessary to communicate effectively with IT personnel, Rule 30(b)(6) witnesses, expert witnesses, and retained consultants. A good starting place for learning some of the technical terminology is the *Sedona Conference Glossary: E-Discovery and Digital Information Management* ([www.sedonaconference.org](http://www.sedonaconference.org)).

Counsel should also try to learn about their clients’ data storage systems and the locations of key storage facilities, archives, and information technology, as this information may prove vital in the implementation and auditing of the company’s document-retention program. It will also enable in-house counsel to quickly track and locate stored information.

The rules draw a distinction between accessible and inaccessible data. See Rules 26(b)(2)(B) and 45(d)(1)(D). With limited exception, a party is under no obligation to produce electronic data that it identifies as not reasonably accessible due to undue cost or burden. Accessible electronic information includes online data that are stored traditionally on a hard drive with relatively easy access. Inaccessible data would generally include erased or fragmented data or obsolete data or storage devices formatted on systems that are no longer supported by the company.

Counsel should be aware of the company’s backup procedures, including their timing, duration, and the format in which the backup data are stored. This information will enable counsel to quickly realize whether the data are easily accessible or whether potentially time-consuming and costly steps must be taken to recover the information.

In essence, lawyers must learn to “talk the talk” to ensure what they communicate to their outside counsel (and ultimately the courts) about their electronic data storage and retrieval is both reliable and accurate.

### **Tip #3: Understand the Different Types of Evidence Created by Your Clients.**

The most noticeable change in the rules related to discovery is the emphasis on electronic data production. Rule 34 defines a new category of discoverable information known as “electronically stored information.” Electronically stored information includes writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained or translated. Considering that roughly two-thirds of documents are never put in printed form, the rules encourage the transfer of electronic data rather than making computer printouts. A company that produces data electronically is under no duty to produce the same documents in paper form. Rule 34(b)(iii).

As with traditional paper documents, parties in litigation have an affirmative duty to provide a copy, or description by category and location, of all electronically stored information the parties have in their possession, custody, or control that they may use to support their claims or defenses. Rule 26(a)(1)(B). Counsel must be prepared to meet and confer early in the litigation process to discuss issues related to the disclosure of electronically stored information, including data preservation and any potential inaccessibility of relevant data. Counsel also has an absolute duty to communicate with the client and key personnel to make sure that all electronically stored information is identified and accounted for. Even if counsel believes the data are inaccessible and will not be produced, their existence still must be disclosed to the opposing party.

### **Tip #4: Implement or Update Document-Retention Policies to Include Electronically Stored Information.**

Every company should have a global document-retention policy that limits how long information is kept and sets forth the procedures for uniform and timely destruction of both paper documents and electronic data. The

policy should also define what types of information are to be retained and destroyed, where retained information is to be stored, and who shall have access to retained information. In addition, counsel must put protocols in place to make sure the retention policy is actively enforced and periodically audited. The policy should then be implemented in all locations, including subsidiaries and affiliated companies. (Differences in foreign law and policy may demand special attention for overseas office locations.) Failure to have such a policy can mean catastrophic litigation results. See *Zubulake v. UBS Warburg* (“Zubulake V”), 2006 U.S. Dist. Lexis 13574 (July 20, 2004) and *Coleman (Parent) Holdings v. Morgan Stanley & Co.*, 2006 Extra Lexis 94 (Fla. Cir. Ct. Mar. 23, 2005) (appellate court reversed on appeal without considering discovery abuses in *Morgan Stanley v. Coleman (Parent) Holdings*, 2007 Fla. App. LEXIS 4167 (Fla. Ct. App., March 21, 2007)).

How long must electronically stored information be kept? A company bound by regulatory obligations may have a pre-determined retention period (e.g., SEC-regulated companies are bound by Rule 17a-4 of the Securities and Exchange Act, which, among other things, requires companies to retain emails for at least three years.) In the absence of an affirmative duty to place a “litigation hold” on document destruction, companies operating outside a specific regulatory framework are typically expected by courts to retain electronic information only as long as is necessary and practical for business purposes.

A good document-retention policy may also be a company’s best defense against claims of spoliation by an opposing party. Under Rule 37’s “safe harbor provision,” absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide data lost as a result of routine, good-faith operation of an electronic information system.

In developing a legally defensible policy, companies must balance their need for archival information against the expense of storing and maintaining that information. They should also determine what resources the company must allocate to search and review the stored information. Under the rules, due to undue burden or cost, a company would not need to produce electronically stored information from sources that are not reasonably accessible. Rules 26(b)(2)(B) and 45(d)(1)(D). Thus, a company’s retention—or more accurately destruction—policy should strive toward an efficient and economical information management system, which in turn will help reduce some of the burden attributed to document production in litigation. Keep in mind that the majority of discovery-related expense is often the attorney time spent reviewing documents.

#### **Tip #5: Identify a Client’s Potential Storage Media Both Internally and Externally.**

In addition to the company’s internal computer data and storage systems, in-house counsel should become familiar with any external means and mechanisms used to store and back up information. In-house counsel must also identify third-party companies used to retain, transfer, or destroy data. The company should have procedures in place to track electronic information that may exist outside the company’s storage systems. The task may be particularly daunting given that relevant information may be stored not only on an employee’s office computer and laptop, but also on a personal digital assistant or PDA (e.g., BlackBerry®), smart phone, MP3 player, flash drive, or other media storage devices. It is not uncommon for documents to appear in more than one, or even all, of these transient media.

For example, many PDAs are synchronized with an employee’s work computer. If the employee wants to work on a particular project over the weekend, she may email it to her home computer or transfer the data to her iPod or flash drive. Once at home, the employee uploads the information to her home computer. When finished working on the data, the employee emails the final version to herself, with the document being instantaneously sent as

an attachment to her office computer, PDA, smart phone and laptop. It will then remain on all of these devices until deleted, either manually or automatically. If an employee's work product becomes the subject of litigation, these multiple copies of the document could potentially be relevant as they may evidence different iterations of the document. Tracking an employee's work product can lead counsel down a slippery slope, although transient data may be considered inaccessible if the organization has no current means to preserve the information and it is not kept in the ordinary course of business. See *Convolve, Inc. v. Compaq*, 223 F.R.D. 162 (S.D.N.Y. 2004).

**Tip #6: Understand the Difference and Impact of Various Data Production Formats.**

The rules require parties to meet and confer early in litigation to try to reach an agreement on how documents will be produced. Rule 26(f)(3). If an agreement cannot be reached, a document must be produced "in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable." Rule 34(b)(ii). The court may issue a scheduling order that includes provisions for the disclosure and discovery of electronically stored information. Rule 16(b)(5).

Counsel should be aware of the various software applications licensed and utilized by their clients, as this knowledge will prove invaluable in determining the type of evidence the company is creating and what form of production makes sense given the amount of data to be processed and the need to review any data for relevance and privilege. Once this information is obtained, counsel will be in a position to communicate effectively with the client about the company's data production needs early on—in some cases even prior to the commencement of litigation.

**Tip #7: Have Litigation Hold Procedures in Place.**

The only common law duty to preserve documents and information exists when a company is on notice of pending litigation. At that point, a "litigation hold" must be implemented to retain documents the company reasonably believes would be discoverable. See *Zubulake v. UBS Warburg LLC, (Zubulake IV)*, 2003 U.S. Dist. Lexis 18771 (S.D.N.Y., Oct. 22, 2003). This duty commonly arises when a party receives a demand letter or summons and complaint. However, the duty may also arise sooner if a party has sufficient information to put it on notice of a credible threat of litigation.

The notice does not have to be of actual litigation, but can also concern only potential litigation. *Phoenix Four, Inc. v. Strategic Res. Corp.*, 2006 U.S. Dist. Lexis 32211 (S.D.N.Y. May 22, 2006). To determine when a party anticipated litigation, the court must engage in a very fact-intensive, backward-looking inquiry. While the identification of the precise point when a party truly anticipates litigation is elusive, courts have held that any document destruction done to alleviate fear of future litigation is inappropriate. See, e.g., *Byrnie v. Town of Cromwell*, Bd. of Ed., 243 F.3d 93, 108 (2d Cir. 2001); *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998). Thus, document-retention policies that seek to destroy metadata or an electronic document's embedded data may be highly scrutinized by the court. See, e.g., *Samsung Electronics Co. v. Rambus, Inc.*, 2006 U.S. Dist. Lexis 50007, p. 46 (E.D.Va. July 18, 2006) ("[A] document-retention policy adopted to justify the destruction of relevant evidence is not a valid document-retention policy.") However, even presuming litigation is anticipated, a party is not required to halt its entire document-retention/destruction program, but only to put in place a litigation hold to ensure relevant documents are preserved. *Id.*

Because this obligation is an affirmative one, the company and its officers having notice of the discovery obligation must communicate it to employees in possession of discoverable information. *Heng Chan v. Triple 8 Palace*, 2005 U.S. Dist. LEXIS 16520 p. 16 (S.D.N.Y. 2005). In-house counsel should educate employees regarding this

affirmative obligation and the consequences of an employee's failure to act. While the obligation imposes a burden, a benefit also exists in preventing sanctions against a party in litigation under Rule 37(f)'s safe harbor provision.

**Tip #8: Develop a Litigation Strategy and Action Plan for IT Personnel.**

In-house counsel may want to get an early start by selecting key personnel in the company's IT department who can assist with issues that may arise in future litigation. This team will be responsible for keeping counsel apprised of the most recently acquired technologies that impact data storage or relate to the company's document-retention program.

Counsel may also want to interview and train potential Rule 30(b)(6) witnesses who have knowledge and can effectively articulate their expertise with all aspects of the company's electronic data and storage systems, including but not limited to: (1) network structure and usage policies; (2) persons responsible for ongoing operations, maintenance, and expansion; (3) backup systems for all data files, including email and voice-mails; (4) document retention policies; (5) company procedures regarding employee use of personal electronic devices, including computers, cell phones, media players, and personal digital assistants; (6) operating software and proprietary applications; (7) types of databases utilized by company; and (8) Web-based information, including policies and protocol for temporary files, system history files, Web site information, Web site log files; cache files, and cookies. See *Leonard v. McDaniel*, 2006 U.S. Dist. LEXIS 18650 (D. Nev. March 31, 2006).

A Rule 30(b)(6) witness may be the company's IT director or some other individual qualified to discuss all aspects of the company's computer systems. The witness should also be familiar with the company's "chain-of-custody" procedures as outlined in its document-retention policy and be able to establish a complete chain of custody for all electronically stored information. This witness will become a trusted adviser to the company's legal department and a valued resource to outside counsel in litigation.

**Tip #9: Protect Against the Inadvertent Disclosure of Privileged Documents.**

The sheer volume of electronic document production makes inadvertent disclosure of a privileged document a serious concern for in-house counsel and litigators alike. More and more lawyers are being compelled to produce millions of documents that at some point earlier in time were disorganized, existed only on computer hard drives or backup tapes, or had never before been put in physical form.

Counsel should put procedures in place at the outset of litigation (if not before) to account for and segregate potentially privileged documents. If practical, it may be wise to have all potentially privileged documents stored on segregated or partitioned hard drives, servers, or a backup system. Counsel should ensure that all employees who have access to privileged information consistently mark or code these documents as such so that they can be easily retrieved and segregated should the need arise.

If inadvertent disclosure occurs in litigation, Rules 26(b)(5) and 45(d)(2)(B) require counsel to notify all parties who received potentially privileged documents and to state the grounds for the privilege claim being made. Once notified, the receiving party may not use or disclose the information to third parties until the claim is resolved. The receiving party has the option of promptly presenting the information to the court under seal for a determination of the privilege claim.

If the receiving party has already disclosed the information to third parties, it must take reasonable steps to retrieve the information. Issues regarding potential waiver or forfeiture of the privilege claim based on production are reserved for determination by the court.

The rules also seem to embrace use of non-waiver agreements. These agreements between parties provide for the return of privileged documents after inadvertent production. Rules 16(b) and 26(f) codify the court's authority to incorporate such agreements into a case management order. However, these agreements may not bind third parties, and in some jurisdictions may be considered evidence of a party's intentional waiver. See *Hopson v. City of Baltimore*, 232 F.R.D. 228, 240 (D. Md. 2005).

**Tip #10: Communicate Promptly with All Parties and the Court Regarding Delays or Other Issues and Act Diligently.**

Given the potential size of data collection, production, and review, it is foreseeable, if not inevitable, that something may not go according to plan. When this occurs, counsel should use good-faith efforts to communicate with all affected parties and the court if necessary.

Counsel should refrain from unilaterally obstructing, altering, or destroying another party's access to evidence, and must strongly advise their clients to do the same. If parties and their counsel are unable to resolve issues relating to the production of electronically stored information, they should raise those issues with the court. See Rule 16(b)(5). (Judge's scheduling order may include provisions for disclosure or discovery of electronically stored information.) If a protective order under Rule 26(c) is appropriate, counsel should move for one promptly.

**Conclusion**

The Federal Rules recognize that electronic evidence is on the same footing as other discoverable evidence. They also acknowledge the increasing volume of electronic data and the increased burden that electronic data may impose on a party. They allow federal judges to play a more active role in the discovery process when voluminous amounts of electronic data are at issue.

The issues that electronic discovery presents are not trivial and may require assistance beyond counsel expertise. Some of the most challenging issues are around privilege, form of production, determination of accessibility, and safe harbor. Any outside expert consulted for help in understanding and dealing with these challenges should have extensive experience in e-discovery matters and should be able to provide the following:

- An understanding of IT systems and electronic document types
- Experience with backup systems and the cost of recovering information from them
- The ability to produce electronic evidence in multiple forms—TIFF, PDF, or native file, depending on the circumstances of the matter
- The ability to collect data quickly, economically, and in a forensically sound manner
- The ability to recover information that has been lost, if necessary
- Methods for quickly identifying privileged documents
- Expertise in document-retention and litigation hold policies and procedures

Cases are won or lost on discovery issues. The rules require considerably more attention by in-house lawyers and their trial counsel to the preservation and disclosure of relevant electronic information. Lawyers who understand these rules and have the expertise to use them effectively will have the upper hand.

### The Discovery Experts: Industry Relations

LexisNexis Discovery Services has the right consulting and technology choice for every discovery need. Top law firms, corporations and government agencies rely on the LexisNexis® products and services, Applied Discovery®, Concordance™, and Hosted FYI™, to meet their discovery obligations on time, accurately and cost-effectively. Services include records management consulting, data collection, forensics, media restoration, data filtering, data processing, review and document production in the format that each matter requires. The Industry Relations team works to educate the legal community on the continually evolving case law and technology of electronic discovery.

For more information or to contact the experts, please visit [lexisnexis.com/discovery](http://lexisnexis.com/discovery).

