

# **Electronic Discovery in the 21<sup>st</sup> Century**

---

If your company is brought into litigation, or if it reasonably anticipates the likelihood of litigation, it has an affirmative obligation to identify and preserve all data that might be relevant to such lawsuit. Below is a summary of a company's discovery obligations should they bring suit or be sued in federal court.

Please note that the below rules reflect a trend that imposes heightened discovery obligations on litigants, due to the vast amount of electronic data created and retained by companies in connection with their business operations. To ensure an ability to comply with these onerous discovery rules, your organization should maintain an up-to-date map of their entire "eRecords" landscape and employ IT professionals capable of identifying and managing this data should the company become embroiled in litigation. If unprepared, a company may find itself reactively scrambling to meet its discovery obligations, which will cost the company much more than had it proactively established a protocol for identifying, retaining and retrieving its records.

Please also bear in mind that the below summary is *not* intended to account for all possible discovery issues that may confront a party in the event of litigation. If your company is anticipating litigation or is involved in a pending suit, it is essential that it retain litigation counsel who can help the company satisfy applicable discovery rules and advocate for interpretations of these rules that benefit the company's strategic position.

## **THE AMENDED FEDERAL DISCOVERY RULES**

On December 1, 2006 the Federal Rules of Civil Procedure ("FRCP") were revised to address numerous "eDiscovery" issues. These amendments make the efficient management of a company's electronic records more important than ever. First and foremost, these amended rules make it very clear that electronic records are discoverable. Litigants now have a clear responsibility to preserve and produce "eRecords" and failure to do so could lead to significant court sanctions.

Specifically, FRCP Rule 26(a) expressly adds "electronically stored information" (ESI) as a category of discoverable data. In other words, if a company brings a suit or is sued in federal court, there is no "wobble room" for holding back content stored on electronic media, including but not limited to various electronic databases, instant messaging, image and audio files, and PDA's, assuming this content is relevant to the lawsuit. Moreover, the language within these amended federal rules is inclusive enough to cover any electronic media developed in the future.

**Initial Discovery Planning Conference.** FRCP Rule 26(f) requires that before discovery commences, all parties in a lawsuit meet and confer "as soon as practicable<sup>1</sup>," to discuss any issues about preserving discoverable information (ESI and non-electronic records) and to develop a proposed discovery plan. This discovery plan should address the proposed format in which ESI is to be produced and whether ESI in certain locations is "reasonably accessible."

During this planning conference, the parties should discuss their computer systems in order to develop a discovery plan that takes into account the capabilities of these systems. In most cases, IT professionals should be included during these "meet and confer" talks. It will also be necessary for the company's

---

<sup>1</sup> The parties must confer as soon as practicable and in any event at least 21 days before a scheduling conference is to be held or a scheduling order is due under FRCP Rule 16(b).

counsel to have sufficient familiarity with the company computer systems and data, enabling the attorney to identify which sources of ESI will be searched, which data will be preserved, and in what format each type of ESI should be produced. Please note that the parties' discussion regarding data preservation should pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities.

**Initial Written Disclosures.** In general, a party must provide Initial Written Disclosures to all litigants within 14 days of the above-mentioned discovery planning conference. Among other things, these written disclosures must include a list by document type and location of all records (ESI and non-electronic) in the party's custody or control that may potentially be used to support this party's claims and defenses in the case.

**Safe Harbor Provision for "Good Faith" Disposal of ESI.** As part of the December 2006 amendments to the FRCP, 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." While this rule has been described as creating a "safe harbor" for parties who have lost or discarded relevant ESI in the normal course of business operations, many commentators have stressed that these "protections" are largely illusory.

For example, if a party fails to intervene to suspend a routine business operation that deletes or overwrites data, a court could determine that the failure to retain this data was not done in good faith. Moreover, even if a party demonstrates that it acted in "good faith," a court may find that "exceptional circumstances" trump this party's good faith such that the imposition of sanctions may be justified. Finally, a court must be satisfied that the data in question was lost or overwritten in the normal course of business operations. In essence, while a cursory reading of Rule 37 may allay fears regarding lost or overwritten electronic data, the real effect of Rule 37 puts a party's legal department on notice to ensure that litigation holds and data destruction policies are legally defensible.

One of the best ways for a company to avoid sanctions under the FRCP is to adopt and implement a robust program for the retention and routine disposal of ESI, coupled with a consistent methodology for identifying and preserving ESI that could be relevant to pending or reasonably foreseeable litigation. Further tips to ensure compliance with these FRCP are listed later in this article.

**Format of Document Production.** Once discovery actually commences in a federal case, FRCP Rule 34(b) allows the requesting party to specify the format in which various types of ESI are to be produced. If the responding party does not wish to produce the electronic documents in the requested format, it must object to this proposed format in its discovery response, state the reasons for the objection, and specify which alternative format(s) it intends to produce the ESI in.

Furthermore, unless the parties otherwise agree or a court otherwise orders, the responding party must produce ESI in a "reasonably usable" format, or in the form in which the data is ordinarily maintained. The question regarding whether a particular format is "reasonably usable" is open to interpretation by the courts and often depends upon the circumstances of the case. For many types of ESI, including email, a text-searchable PDF is considered a "reasonably usable" format.

**Inaccessible Data:** FRCP Rule 26 (b)(2) provides that a party need *not* retrieve and produce ESI from sources that the party identifies in its discovery responses as “not reasonably accessible<sup>2</sup>” because of undue burden or cost. However, an unsubstantiated statement regarding an undue burden is insufficient. The party claiming inaccessibility bears the burden of demonstrating that this data is too difficult or costly to retrieve and produce.

Even if a party can demonstrate that data is inaccessible, a court may still order discovery from this source if the requesting party shows “good cause.” For example, a defendant company may demonstrate that terabytes of data stored on back-up tapes are “inaccessible,” due to the excessive legal costs to review such data, however, a court may order production because the subject-matter of these tapes may go to the heart of the litigation. In such cases, a court has the discretion to shift costs so that both litigants share the expense of the document review and production.

Finally, even if “inaccessible” records need not be produced, a party is still obligated to preserve this potentially responsive data.

**Tips for Complying with the amended FRCP.** Ultimately, these amended federal rules impose significant burdens on companies that become embroiled in litigation. Businesses should maintain an up-to-date map of their entire eRecords landscape and employ IT professional capable of answering specific questions -- from both parties’ counsel – including the number of discoverable document repositories, the file types and locations, access constraints to these files and the cost implications of data retrieval and production.

At a minimum, it is recommended that your company take the following measures:

- Maintain a list of all servers that store both “structured” and “unstructured” data;
- Implement and enforce a policy that defines which types of files are retained and for how long;
- Develop a strategy for managing the storage needs of rapidly growing e-mail systems;
- Add an archiving system to all e-mail servers; *and*
- Train the company’s IT professions regarding their responsibilities under the amended rules

---

<sup>2</sup> As with the requirement that electronic data be produced in a “reasonable usable” format, the question of whether electronic data is “reasonably accessible” is open to interpretation by the courts and depends upon the circumstances of the case.