IRON MOUNTAIN®

WHITE PAPER

Rule 26 and Other Amendments to the Federal Rules of Civil Procedure: New challenges for litigation readiness

Table of Contents

EXECUTIVE SUMMARY

Litigation involving your company is an inevitable fact of business life. When it happens, will your records management program help or hinder your defense? The newly amended Rule 26 and other changes to the Federal Rules of Civil Procedure (FRCP), which govern the production of evidence in most federal court cases, make the efficient management of corporate electronic records (eRecords) more vitally important than ever. Failure to comply with the new electronic discovery (eDiscovery) rules can mean fines, sanctions, executive liability, a drop in stock price, and other risks.

This paper explains the specific impacts of key FRCP amendments on your records management program:

- Rule 26(a), which explicitly defines electronically stored information (ESI) as discoverable
- Rule 26(f), which mandates early meet-and-confer sessions specifically to resolve eDiscovery issues
- Rule 26(b)(5), which addresses the inadvertent production of privileged information during eDiscovery
- Rule 26(b)(2), which provides guidance regarding claims that requested eRecords are unduly burdensome to produce
- Rule 37(f), which covers the loss of potential evidence in the course of routine records disposal

In conclusion, the paper describes how you can leverage appropriate technology and best practices to reduce cost and risk, while providing optimal support for your legal team.

READY OR NOT, HERE COME THE NEW RULES ON EDISCOVERY

Sooner or later your company will be involved in litigation[1]—and when it is, your records management program will be severely tested. Are you prepared to produce relevant e-mails and attachments, instant messages, transaction logs, video files, and other eRecords upon request? As a host of well-publicized cases have vividly illustrated, businesses that bungle eDiscovery are incurring multi-million dollar fines, spending more millions retrieving and analyzing enormous volumes of information, and damaging their reputations in the bargain.

Already inundated with terabytes of data and challenged by heightened regulatory scrutiny, many organizations are struggling to bring their records management programs into compliance. New amendments[2] to Rule 26 and other Federal Rules of Civil Procedure, which govern discovery in civil litigation, both exacerbate the pressures and multiply the consequences of failure. Now when litigation happens, the unprepared will find themselves reactively scrambling to address complex eDiscovery requests, exposed to levels of cost and risk undreamed of just a few years ago.

---

[1] *Some sobering statistics from an October 2005 study of corporate counsel by the law firm Fulbright & Jaworski, LLP: (1) U.S. companies with at least $1 billion in annual revenue are engaged in an average of 147 lawsuits simultaneously. (2) On average, most businesses with average revenues under $1 billion are managing 37 lawsuits at any given time. (3) Nearly one-third of firms spend more than 2% of their gross revenues on legal expenses, while 10% of businesses spend more than 5%.*

[2] *Scheduled to take effect on December 1, 2006, the new rules could be adopted three months in advance or even sooner in some states. New Jersey, for example, voted on July 27, 2006, that it would adopt the new FRCP amendments in their entirety, effective September 1, 2006. Other states, including Texas and California, have either adopted some of the new rules already, and/or have some of their own rules already in place.*

RULE 26: OBJECTIVES AND OVERVIEW

The new amendments centered on FRCP Rule 26[3] are landmark changes aimed specifically at helping courts and litigators navigate the brave new world of ESI. The amendments embrace several key objectives. Overall, they take crucial steps to deal specifically with the unprecedented challenges of eDiscovery and eRecords. They are further intended to accelerate the exchange of information during the pre-trial period, while facilitating a smoother, less conflict-ridden, and less financially burdensome legal process for all parties.

These guidelines compel businesses to pay attention as never before to how their records management program facilitates or frustrates eDiscovery. There is now far less legal ambiguity to hide behind where eRecords are concerned; and many fewer excuses for businesses that cannot readily answer questions about what records they have, where they are located, what form they are in, who is responsible for them, what policies govern their retention and disposal, and how quickly they can be reviewed and produced in a specified format.

The new amendments can be categorized in terms of five major eDiscovery areas:

- Defining ESI as a separate class of discoverable information
- Mandatory meet-and-confer sessions to address eDiscovery issues must take place very early in the litigation
- "Reasonably inaccessible" electronic data and rules governing its production
- Principles related to "claims of privilege" and "clawback agreements" in cases of inadvertent production of privileged ESI
- Protection for organizations that inadvertently destroy potentially discoverable records in the course of normal, "good faith" records management operations

Details on each of these areas follow.

Making all forms of ESI discoverable

The new Rule 26(a) explicitly defines ESI as a specific category of information to be disclosed. There is no longer any ambiguity about whether digital data constitutes a "document." Businesses now have a clear responsibility to produce eRecords.

These amendments also permit the requesting party to request that ESI be produced in specific formats. The responding party can object to the request, but the parties must first meet and confer in an attempt to resolve the disagreement before a motion to compel can be filed. If need be, the court may order the form of production. Companies therefore need to know exactly what formats their eRecords are stored in, what metadata is associated with them, and what formats they can reasonably be converted into.

[3] *The amendments also impact Rules 16, 33, 34, 37, and 45 in addition to Rule 26.*

Mandatory early meet-and-confer

Among the most important of the newly amended FRCP for businesses is Rule 26(f), which requires parties to meet within 120 days of the filing of litigation, and at least twenty-one days prior to the scheduling conference, specifically to discuss eDiscovery issues. The purpose of this Rule is to avoid loss of ESI and ensure its usability and timely production by resolving concerns up-front.

During these sessions, parties must make every effort to reach agreement on logistical issues, including relevant repositories and classes of information, production formats, and matters of privilege. Companies must promptly identify all sources of ESI in their initial disclosures, meaning not only e-mail servers and backup tapes, but also deleted data, data on systems no longer in use, and data in remote or third-party locations. All of this data must be identified up-front if the data will be used in claims or defenses. A report must then be provided to the court, pursuant to a scheduling order.

The implications of Rule 26(f) are huge. Companies now need an up-to-date map of their entire eRecords landscape at their fingertips, along with the commensurate IT expertise to address and answer specific questions—from both parties' counsel—about numbers of discoverable repositories, file types and locations, access timeframes, access constraints, cost implications, and relevance of metadata, etc. The need for the producing party (and often the requesting party as well) to bring a technology expert at meet-and-confer sessions is virtually a given.

Your ability to know and describe your system capabilities so your attorneys can negotiate reasonable time schedules and limits for production volume will be critical. Organizations that lack a comprehensive map of potentially relevant records will be at a major disadvantage from the outset, playing catch-up just when they should be doing serious analysis of the case. Conversely, businesses that can produce accurate inventories of electronic data repositories can save themselves millions of dollars in eDiscovery and settlement costs, and possibly even sway the outcome of the proceedings.

Rule 26(f) also demands that parties give early attention to data preservation. Providers risk claims of spoliation[4] of evidence if litigation holds are not instituted quickly and efficiently since production requirements will be known up-front. On the other hand, the ability to agree during meet-and-confer sessions on what must be preserved versus what can be disposed of per standard retention policies can save companies money and protect against subsequent spoliation claims.

Claims of Privilege after inadvertent production

The greater the volume of ESI produced in a lawsuit, the greater the likelihood that privileged information, such as trade secrets or financial information, may be inadvertently produced. The traditional ability to inspect all data and filter out privileged information is simply not possible given the staggering quantity and variety of eRecords that can be involved in large, complex litigations. For example, it is estimated that the average gigabyte of e-mail contains 100,000 printed pages of information, as compared to 3,000 pages for the average box of printed records. Hundreds of thousands of pages of ESI are now the norm in bigger cases[5].

---

[4] *Spoliation is broadly defined as "the destruction, alteration, or mutilation of evidence."*

[5] *To cite but one example, the Federal Energy Regulatory Commission (FERC) posted more than 1.6 million pieces of e-mail and other Enron documents on the Web in a searchable database.*

Rule 26(b)(5) includes a new section covering the accidental production of privileged information. It permits organizations to retract ("clawback") privileged information following its discovery. Potential concerns regarding privilege are to be discussed during meet-and-confer sessions as part of the discovery plan.

If information deemed privileged is produced, the producing party can notify the recipient of this assertion and the basis for it. The requesting party must return, sequester, or destroy the information promptly, and is barred from disclosing it until the claim is resolved. Further, if the recipient has already disclosed the privileged information prior to notification, it must take reasonable steps to retrieve it. In any event, the producing party must preserve the privileged information until the litigation is resolved.

Recipients can naturally dispute claims of privilege by submitting the information to the court for a ruling. The producer must make responsible attempts to avoid such disclosures—sloppy production is not an excuse and may imply a waiver of privilege. Moreover, producers must assert claims of privilege within a "reasonable time," again requiring a handle on the data. Courts will weigh these factors in determining whether to waive or forfeit a claim of privilege.

ESI that is not "reasonably accessible"

Rule 26(b)(2) addresses the reality that some ESI can be unduly burdensome to produce.

In acknowledging that some information may be overwhelmingly difficult to retrieve (e.g., because the hardware/software required to restore it is obsolete, or the media it resides on is damaged), this rule specifies that a party need not produce eRecords it regards as "not reasonably accessible because of undue burden or cost."[6]

If, following meet-and-confer sessions, a claim of reasonable inaccessibility remains unresolved, the requesting party can introduce a motion to compel production to dispute the assertion. Likewise, the responding party can seek a protective order from the court barring production.

In either case, however, the burden is on the responding party to prove that the information is not reasonably accessible. Further, if the requestor can demonstrate that there is just cause showing that the evidence should be produced, the court may then order its production. When might ESI be deemed reasonably inaccessible? A range of factors will be involved, including:

- The burden or expenses of producing outweighs the likely benefit or relevance of the data
- The request is unduly cumulative or duplicative
- The quantity of data involved
- A party's inability to obtain the same or equivalent information from more accessible sources
- The magnitude of the issues at stake in the litigation
- The resources of the parties involved

[6] *Consider this metric: eDiscovery searches can cost $1,000 to $2,500 per backup tape and involve thousands of tapes.*

In practice, therefore, a smaller company being sued for $100,000 and seeking to avoid an estimated cost burden of $200,000 to recover requested ESI might receive a favorable ruling of reasonable inaccessibility. However, a global enterprise could be compelled to do whatever is necessary to produce similar evidence, particularly in a case where more is at stake.

To show proof of reasonable inaccessibility, the producing party must be able to identify the data repositories it deems inaccessible, and provide details as to what these sources contain and what producing the requested information will entail. Further, identifying sources as inaccessible does not relieve the producing party of its responsibility to preserve the material as potential evidence.

In short: organizations lacking solid records management programs are much more likely to be burned by this rule than helped by it.

Safe harbor for "good faith" records disposal

Rule 37(f) is an entirely new and highly controversial amendment to the FRCP. In recognition of the fact that companies cannot preserve all the data they generate, its purpose is to provide limited protection against sanctions for parties that have disposed of potentially discoverable data in the normal course of "good faith" business operations.

The rule states: "...absent exceptional circumstances, a court may not impose sanctions as the result of the routine, good-faith operation of an electronic information system." However, a company's routine procedures will be carefully examined in this context.

This rule addresses the loss of ESI through routine procedures like deleting old e-mails and recycling storage media. While its intent is to prevent the sanctioning of innocent parties, it does not provide a loophole for organizations that purposefully destroy relevant data outside the bounds of documented procedures. If you cannot produce data that your policy says you should have available, you risk sanctions. If you have no retention policy, you risk sanctions.

Nor does Rule 37(f) help companies that fail to preserve records via appropriate litigation holds—even before a suit is actually filed. Your company is on notice and must cease the destruction of relevant records anytime litigation is reasonably foreseeable.

The concept of "reasonably foreseeable" is in the eye of the beholder, and there is a risk that a plaintiff will allege (after litigation has begun and the plaintiff discovers that routine destruction of information occurred) that the defendant should have realized, months earlier, that litigation would ensue if the defendant didn't accede to the plaintiff's requests, and thereby add a spoliation charge to the litigation. Therefore, your company should consider a policy that monitors disputes from early in their life, to be cognizant when they have developed to a point where litigation is reasonably foreseeable.

Courts will question how well policies are enforced, when litigation could have been foreseen, how quickly litigation holds were communicated, and so forth. In precedent-setting cases like *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) the court has found that litigants must take affirmative steps to preserve documents, including:

- Issuing a litigation hold at the outset of the litigation or when litigation is "reasonably anticipated"
- Communicating the litigation hold directly to all key employees
- Reiterating the litigation hold instructions regularly and monitoring compliance with the litigation hold

Even when a company fails despite good-faith efforts to enforce a litigation hold and inadvertently disposes of records, it can still face sanctions for willful destruction of documents. In worst-case scenarios, businesses struggling to avoid sanctions have frozen all data disposal activities during litigation because they cannot identify pertinent records.

Companies that proactively establish a litigation hold process can ensure that the right records are kept while non-relevant data is processed routinely, thus reducing both litigation threats and preservation costs. By the same token, inadequate records management policies increase risk and confer no protection. Yet many companies continue to take this "head in the sand" approach. According to the 2006 *Workplace E-mail, Instant Messaging & Blog Survey* by the American Management Association (AMA) and The ePolicy Institute, 66% of companies surveyed lack policies for saving, purging, and managing e-mail.

While the courts' interpretation of Rule 37(f) is not yet known, it is likely that it will offer little protection to enterprises with lax records management programs. New archiving technology makes long-term data preservation more feasible, for instance. Further, companies involved in multiple, overlapping lawsuits may have limited capability to dispose of data and hence limited eligibility for protection.

IMPLICATIONS OF RULE 26 FOR RECORDS MANAGEMENT

The new Rule 26 and the other changes to the FRCP make the eDiscovery process more transparent in terms of disclosure. Organizations need to know exactly where their data is kept, what data storage technology is used to backup and archive them, how the retention schedule applies to them, how and when they are disposed of, how long it will take to produce them, and what formats they can readily be produced in, etc. The IT, Legal, and Records Management teams all need to work closely together to (1) establish a compliant, defensible eDiscovery process and (2) deal with eDiscovery issues early in litigation through the meet-and-confer process.

Identifying and preserving ESI

Another important shift brought about by the new Rule 26 is the courts' increased emphasis on identifying and preserving relevant ESI. Companies not only must know the terrain of their records management landscape—including everything from e-mail to instant messages to handhelds to BlackBerries to voicemail to laptops—they must also be able to traverse it quickly and efficiently to control retention and disposal. If you can't explain where you put your data, or if you can't act quickly to prevent the destruction of potential evidence, you face sanctions or worse.

Likewise, it is absolutely essential for businesses to develop, document, institute, and verifiably enforce formal litigation hold and data preservation procedures. This includes creating communication distribution lists, documenting relevant activities, and defining procedures and accountability for instituting, monitoring, and releasing litigation holds. If you cannot enforce litigation holds you are at grave risk. This is particularly true of e-mail systems, which are subpoenaed in a rapidly rising percentage of cases.

Handling privileged information

Rule 26(b) has specific implications for how companies handle privileged information. Ideally it should be stored in separate repositories or otherwise classified as privileged upon storage, in order to meaningfully protect it during eDiscovery. This could save a great deal of time, money, and embarrassment in the course of litigation, and will be vastly preferable to the false sense of security that clawback agreements might engender.

The bottom line

The bottom-line ramifications of Rule 26 and related changes are abundantly clear: To have any hope of dealing with eDiscovery challenges in a risk-averse manner, businesses must formalize document preservation and retention policies and procedures in a consistent, compliant, "good faith" records management program that proactively manages all forms of data—electronic and physical—enterprise wide.

The knowledge and control afforded by such a program enables you to enact and enforce litigation holds, document a compliant chain of custody, prevent spoliation claims, negotiate in good faith during meet-and-confer sessions, avoid turning over privileged information, support claims of reasonable inaccessibility, and provide a safe harbor in the event that potential evidence has been destroyed.

Reducing complexity is especially useful here. Programs that specify consistent policies across medias and formats; and which rely on fewer, broader categories to ensure greater uniformity, will be easier for all parties to understand, explain, and work within. At the same time, a compliant records management program reduces complexity and cost at its root, by mitigating over-retention and thereby reducing the amount of material that must be sifted for eDiscovery.

NEXT STEPS

Specific actions that businesses should take to prepare for litigation now and in the future:

- ✓ Formalize document preservation and retention policies and procedures in a consistent, compliant, "good faith" records management program
- ✓ Establish a litigation readiness team of Legal, IT, and Records Management that will establish the eDiscovery process and deal with eDiscovery issues
- ✓ Inventory systems and sources of data, and identify their content, location, and preferred form of production
- ✓ For key systems, perform an initial assessment of the cost and methods of production to identify "not reasonably accessible" systems
- ✓ Identify system custodians (administrators) and make sure they understand their roles
- ✓ Apply retention policies to the systems and data sources
- ✓ Develop, document, institute, and verifiably enforce formal litigation hold and data preservation procedures.

Reaping the benefits

Companies that implement records management best practices will be vastly better prepared to meet the challenges of Rule 26. They can also easily demonstrate good faith and consistent implementation to courts, regulators and shareholders, while reducing storage and disposal fees and strengthening their business continuity and disaster recovery programs.

Effective CRM programs often yield verifiable cost savings that pay for the initial program investment many times over, while making the ongoing program self-funding. Additionally, though it may be more difficult to measure, further cost savings can be gained by averting litigation and other compliance risk issues.

Iron Mountain solutions and services can empower your organization to shift from a reactive response to a stance of proactive readiness.

For more information on how to design a legally credible Compliant Records Management Program, visit www.ironmountain.com/compliance.

APPENDIX A

Rule	Description	Implications
26(a)	Explicitly makes "electronically stored information" a category of discoverable data, and each party must furnish the other a copy or description of all discoverable material (including ESI) in its possession or control	No more maneuvering room around producing instant messages, PDAs, or other forms of electronic data; must have location of all data "at your fingertips"
26(b)(2)	Sets up provisions to deal with ESI that is not "reasonably accessible"	Requires companies to know early on what ESI discovery may be difficult or expensive, and identify it to other parties, with reasonable specificity
26(b)(5)	Clarifies procedures for retrieval of privileged information that was produced inadvertently	Places a premium on the producing party's determination of what was actually in produced ESI as promptly as practicable
26(f)	Mandates early meet-and-confer sessions	Requires businesses to know precisely where all their records are kept, in what format, for how long, etc., in order to negotiate eDiscovery issues
37(f)	Provides "safe harbor" in the event of "good faith" destruction of discoverable data	Obligates businesses to have a compliant records management program to show "good faith"

Table 1: Summary of new FRCP eDiscovery guidelines

SUGGESTED REFERENCES

Martha K. Gooding. "Electronic Discovery: Change is in the Wind." *Howrey LLP.* http://www.howrey.com/docs/E-Discovery.pdf.

Sharon Fisher. "E-discovery rules deadline moves up in some states." *Computerworld.* August 14, 2006. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002445.

Deborah Gage and Kim S. Nash. "E-Mail Retention: The High Cost of Digging Up Data." *Baseline.* August 2, 2006. http://www.baselinemag.com/article2/0,1540,1998003,00.asp.

Carolyn Southerland. "Are Litigators Ready for the New Meet-and-Confer Sessions?" *The National Law Journal.* July 25, 2006. http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1153744533061.

A Fios, Inc. white paper. *Working Through the Practical Implications of the Amended Federal Rules of Civil Procedure.* July 2006. http://www.fiosinc.com/resources/pdfFiles/200608FRCP_Amendments_whitepaper.pdf.

Elissa A. Santo. "E-Discovery Explosion: Can the new FRCP amendments help pick up the pieces?" *Legal Assistant Today.* July/August 2006. www.legalassistanttoday.com/issue_archive/feature1_ja06.htm.

Cornell Law School. Text of the new Rule 26 and other upcoming amendments to the FRCP. http://www.law.cornell.edu/rules/frcp/Rule26.htm.

745 Atlantic Avenue
Boston, Massachusetts 02111
(800) 899-IRON

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout North America, Europe, Latin America, and Asia Pacific. For more information, visit our Web site at **www.ironmountain.com**.