

PSC White Paper



e-Discovery Compliance

Meeting the Requirements of the Federal Rules of Civil Procedure (FRCP)

Progressive corporate legal departments are taking overt action to improve their electronic discovery readiness through assessment and planning. They are putting resources in place to gain better understanding of their electronically stored information (ESI) and data repositories. They are creating a dialogue with their IT department in which they discuss what business processes will be required as a result of the changes. In addition, they are creating formal discovery response plans to reduce the unpredictability of the discovery and mitigate risk.

The new Federal Rules of Civil Procedure (FRCP), which took effect in December 2006, has changed the way companies are required to handle electronic documents. One of the biggest changes has been the time frame for responding to a discovery request, which has become much more compressed, requiring counsel to act much faster. Ninety-nine days from the time a suit is served in Federal Court is not enough time to do the proper planning on a large litigation matter or to develop a comprehensive e-discovery plan that can be used during negotiations with opposing counsel. The time crunch is further compounded by the significantly expanded scope of discovery along with the change in definition of what is subject to discovery -- everything from e-mail to voice mail and proprietary files stored on databases. Any document that could become evidence in a federal case, such as interstate lawsuits, compliance regulations (such as HIPAA and Sarbanes-Oxley), EEOC and other employment issues, immigration cases, and actions by the Internal Revenue Service, are included. Actually, it is difficult to think of any business document that might not be covered.

What must an organization do to comply?

While a litigant is under no duty to keep or retain every document in its possession, it is, however, under a duty to preserve what it knows or reasonably should know, is relevant in action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of the pending discovery request. Having said that, every organization now needs to set up a policy on what electronic documents need to be preserved and what needs to be destroyed and why and when. As long as the rules are consistent and not event-based, it will put organizations at lesser risk to meet the new FRCP laws on e-discovery.

Why did the laws change?

Prior to the new FRCP rules, courts had tremendous leeway in how they handled electronically stored documents. The problem is that attorneys did not know the rules or the risks until a judge made his or her decision. Some famous cases involving e-mail, for example, include:

- A jury awarded \$800 million in punitive damages when Morgan Stanley repeatedly failed to produce e-mails in a timely manner. The judge stated that "efforts to hide its e-mails" were evidence of "guilt." (Coleman Holdings v. Morgan Stanley)
- A jury awarded \$29.2 million in the largest single sex discrimination verdict in U.S. history after UBS Warburg could not produce copies of relevant e-mails. The jury was instructed to "infer that the [missing] evidence would have been unfavorable" to the defendant. (Zubulake v. UBS Warburg)
- The SEC imposed a fine of \$10 million on Banc of America Securities, the brokerage arm of Bank of America, after they "repeatedly failed to promptly furnish" e-mail and gave "misinformation".

All electronically stored documents must be disclosed to an opposing party in a case, who then can discuss the formats for presenting the documents, place a time limit for the disclosure, and stipulate a "good-faith" test on retention schedules.



It's all in the way we listen.®

PSC Group, LLC is a professional services consulting firm that specializes in business process architecture, information technology and back-office integration. We have extensive experience with a wide variety of collaboration products, applications, processes and systems including ERP, CRM, Portal, and Workflow.

When it comes to workflow, business intelligence, information management, and the control of business processes, PSC can provide you with a competitive advantage through the smart and effective application of technology.

CONTACT

Jose Blanco
office: 800.592.8003
direct: 847.969.8429
jblanco@psclistsens.com

PSC Group, LLC
Chicago, Kansas City,
Minneapolis

www.psclistsens.com

Companies using sophisticated enterprise content management ECM systems are typically ahead of other companies when it comes to complying with the FRCP. However, protections may need to be added and additional systems, like those that manage e-mail, may need to be added.

What needs to be disclosed?

The new law requires an exhaustive search for all electronically stored information, including e-mail that is "in the possession, custody, or control of the party." It must be disclosed "without awaiting a discovery request" (Rule 26(a)(1)). The only exception is for privileged information, which does not need to be disclosed. The search must be done at the beginning of a legal case and certainly no later than the first pre-trial discovery-related meeting, which is required to be within 99 days (Rule 16(b)). In General, a party *must make the initial disclosures at or within 14 days after the court order*. This means that Content Management systems and IT departments will need to respond much more quickly to discovery and internal investigation requests.

The phrase "in the possession, custody, or control of the party" has not been interpreted by the courts. Companies, working with legal counsel, should decide what is prudent. For example, can an employee's laptop or BlackBerry device be considered under the control of the company, even if it is in a remote location? Companies should consider keeping a centralized copy or backup of everything, including e-mail that might be stored on a remote device.

The law continues to state that as a result of the search, a "copy of, or a description by category and location" of all electronically stored information that "the disclosing party may use to support its claims or defenses" must be presented. (Rule 26(a)(1))

Even if the one party "identifies the information as not reasonably accessible because of undue burden or cost," its description, category, and location must be disclosed (Rule 26(b)(2)(B)). This means that the information must be identified, even if it is difficult to retrieve. Nothing can be left out and opposing counsel can challenge. Delay is not an option.

It is expected that most documents will need to be produced in their original form, although the companies can discuss the form in which data is to be produced (Rule 26(f)(3)). In a landmark 2004 case, the U.S. District Court ruled that electronic documents must be produced "in native format" and "with their metadata intact." (Williams v. Sprint) Metadata includes message attributes such as file owner, creation date, routing details, the sender, receivers, and subject line.

Retention Schedules

FRCP Rule 37(f) protects companies from sanctions for deleting e-mail as part of "routine, good-faith operation". This so-called safe harbor provision protects companies that delete documents as part of ordinary business activities. Unfortunately, "routine, good-faith operation" is not defined. The authoritative Advisory Committee on Civil Rules has stated that an entity would usually be protected if it took "reasonable steps to preserve the information after it knew or should have known the information was discoverable."

An implication of Rule 37(f) is that sanctions may be imposed if email is deleted in bad faith. Certainly, any company with a "delete all email" policy or a 30, 60, or 90 day retention policy for the purpose of destroying "smoking guns" ought to consider whether its policy would stand a court test of "good-faith". In addition, if a company claims that all documents are deleted after 90 days, they need to be sure that every copy is deleted. For example, if an employee keeps a copy of e-mail from a customer for more than 90 days, deleting it from the server after 90 days does not "delete" is legally, it just makes it harder to find.

Extra caution must be taken with any information that could be used as evidence. For example, many companies consider it a best practice to place a "litigation hold" on documents and e-mail from or to employees who may be relevant to a case. Organizational retention policies should be reviewed by all the key stakeholders: legal, HR, Finance, and IT. The retention policy and practice should not be relegated to the IT department or based solely on storage capacity. Determine whether the policies reflect "good-faith" operations appropriate for the business needs of the organization. Some points to consider in creating a retention schedule include compliance regulations, the length of a typical company contract, and the statute-of-limitations for potential federal offenses.

Overall, companies need to make sure that their content management systems and other data retrieval systems cover all electronically stored information, including email attachments. Make sure that you can quickly find relevant information-even if it is located on a remote system, present it in its original form, and manage retention schedules.

Suspension in the event of litigation.

If a lawsuit, governmental investigation or subpoena is filed, served or appears imminent, the retention policy may be suspended requiring that documents relating to the lawsuit or potential legal issue(s) or audits be retained. If the IT department receives notification that the Policy has been suspended, they must resume retaining all of the documents that have been designated to keep rather than destroying them pursuant to the Policy.

The Bottom Line

FRCP is just the latest example of how information technology is intrinsically involved with our everyday business process. If we live by IT, then we may also die by IT. The management of electronically stored information is serious business. Not properly managed, IT can also become very expensive, both in real cost and legal penalties. Storing information is the easy part, finding it when you need it is another story. So you might as well do a good job of up-front planning and implement the right architecture. Doing so will save you money in the long run in more ways than one. It will not only avoid those hefty penalties, but it will make your day-to-day operations more efficient and productive.

Table of Sample Documents to be Retained and Suggested Retention Periods

Type of Record	Suggested Retention Period
Intellectual property documentation	Permanent
General correspondence	Three years
Corporate records such as articles of incorporation, bylaws, minutes of meetings, stock registers, etc.	Permanent
Ethics-related documents, such as communication/hotline logs, bulletins, and reports	Indefinite (review every 5 years)
Facilities Records:	
Acquisition or construction data	Indefinite (review every 10 years)
Appraisals	Indefinite (review every 5 years)
Leases	Permanent
Maintenance/repair records	Five years
Plans and specifications	Until superseded
Property management data	Indefinite
Property records for assets of over \$10,000 after disposition	Three years
Finance Records:	
<u>Acquisitions/Divestitures</u>	
Data for acquired/divested	Permanent
Data for non-acquired/ non-divested	Five years
<u>Banking</u>	
Bank statements, reconciliations, deposit slips, cancelled checks	Seven years
<u>Accounting</u>	
Accounts payable	Seven years
Accounts receivable	Seven years
Audit reports	Seven years
Chart of accounts	Permanent
Expense records	Seven years
Annual financial statements	Permanent
Other financial support	Three years
Monthly financial statements	Three years
General ledger	Permanent
Inventory records	Seven years
Loan documents	Seven years after final payment
Purchase orders	Seven years
Sales records	Seven years
Paid Invoices (Accounts Payable)	Seven years
<u>Tax</u>	
Tax returns	Permanent
Supporting documentation for items of income and expense	Four years
<u>Insurance</u>	
Expired policies	Permanent
Other insurance and related documents such as claims for loss/damage, accident reports, appraisals, etc.	Three years
<u>Employee</u>	
Advertisements/Job Postings	One to two years
Applicant interview records and application	Three years after application for individuals not hired; three years after termination for individuals hired
Peer reviews	Seven years after termination
Performance reviews	Seven years after termination
Employee records	Permanent

Type of Record	Suggested Retention Period
Job descriptions	Permanent
Employee handbooks/manuals	Permanent
Test results (aptitude)	Two years
Training and educational records	Three years after termination
Leave documents (FMLA)	Three years
Employment contracts	Three years after termination
Sick/Disability leave (including related medical information)	Three years after termination
HIPAA Privacy documents, policies and procedures	Six years
Insurance information	Three years
Medical information (Non-FMLA)	Six years
Time sheets	Seven years
Payroll journals	Seven years
Payroll tax returns	Seven years
W-2 forms	Seven years
<u>Pension Information</u>	
ERISA plan descriptions, summary annual reports	Six years
Pension payments/records	Three years after death
Pension plan documents	Permanent
Service/eligibility records	Permanent
<u>Safety Records</u>	
Accident reports	Five years
Drug/alcohol testing reports	1 year (negative results) and Five years (Positive results)
Hazardous exposure/monitoring reports (MSDS)	Thirty years from substance last received in workplace
OSHA logs	Five years
Workers' compensation records	Three years from date of disablement

It's all in the way we listen.®