

# BEST PRACTICES FOR PREPARING YOUR BUSINESS FOR E-DISCOVERY

## I. Background

The Federal Rules of Civil Procedure provide for “document production” in the discovery process. Until recently, all types of “documents” were treated uniformly. However, the growth and diversification of electronic stored information has radically changed the term “document” and the underlying procedural needs for discovery. Congress addressed these needs in 2004 and 2005 by formulating amendments to the federal rules for “electronic discovery” and proposing them to the Supreme Court. The Supreme Court adopted these amendments in April 2006 and they went into effect on December 1, 2006.

## II. What is “Electronically Stored Information?”

Electronically Stored Information is any information that exists in a medium that can only be read by a computer. This includes things like email text messages, audio and video files, and word processing documents.

## III. How are Electronic Documents different?

*The differences can be grouped into six broad categories:*

1. Volume and Duplicability – Electronic information requires much less space to store and tends to accumulate much more quickly. Electronic information can also be replicated rapidly and on a very large scale (e.g., replies to emails that retain the original email).
2. Persistence – A shredded paper document is essentially irretrievable. However, even a “deleted” electronic document can remain on a computer’s hard drive until it has been written over.
3. Dynamic, Changeable Content – Computer information can change over time without human intervention so there is no final form (e.g., constantly updating webpage). More generally, electronically stored information can be changed easily and more thoroughly than paper documents.
4. Metadata – A large amount of electronically stored information is not readily apparent on the screen view of the file (i.e., edit history).
5. Environmental Dependence and Obsolescence – Electronic data can often be incomprehensible when separated from its environment. Electronic data can also become obsolete quickly because of rapid technological change.

6. Dispersion and Searchability – Paper documents tend to be consolidated, while electronic documents can reside in numerous locations. However, electronic data is searchable by automated methods.

(The Sedona Conference, The Sedona Principles: The Second Edition June 2007)

#### **IV. What policy needs did the 2006 amendments address?**

1. The Amendment to FRCP 34 sought to maximize the evidence discoverable by making all electronically stored information potentially subject to discovery. This is limited by the proportionality balancing test under FRCP 26(b)(2)(C)(iii).
2. The accessibility of information is taken into account by FRCP 26(b)(2)(B), a provision applicable exclusively to electronic information. Relevant electronic information can be withheld without a court order if it is “not reasonably accessible because of undue burden or cost” and there is an appropriate disclosure of the information’s sources. An opposing party can challenge the claim of undue burden or cost. If those are found, the opposing party can still obtain the information with “good cause.”
3. Protective orders against burdensome discovery were extended to electronic documents. FRCP 26(b)(2)(B). A producing party may seek a protective order to test its obligations to preserve or produce electronically stored information.
4. Efficient discovery is encouraged by requiring parties to meet as early as practicable to discuss issues surrounding discovery of electronically stored information. (FRCP 26(f)).
5. The difficulty of formatting some information is taken into account by FRCP 34(b). This provision allows production in either the original format or in a reasonably useable form.
6. The possibility of inadvertent disclosure of privileged materials with high volume disclosure is taken into account by the “claw-back” provision of FRCP 26(b)(5)(C). This provision provides a procedure in which a party can identify and retrieve inadvertent disclosures.
7. The amendments recognize the value of consistent routines of information management systems. FRCP 37(b) limits the sanctions for information loss due to “routine, good faith operation of information systems.”

## V. The 2007 Amendments did not change substantive law

According to the Advisory Committee Notes, the 2007 Amendments removed redundancies from the 2006 Amendments and changed the language to make the provision more understandable and consistent with the style of the rest of the federal rules.

## VI. The Duty to preserve documents

There is a common law duty to preserve potentially relevant information for pending or threatened litigation. Generally, this duty arises when it is reasonably apparent that a lawsuit could potentially occur. This duty requires a producing party to make reasonable efforts to identify and manage potentially relevant information. This duty is balanced with the right of a party to manage electronic information in a way that best serves its interests.

An inadequate information management system can have many adverse effects. Courts can sanction parties for spoiling evidence. Sanctions can range from monetary fines to default judgments. Spoiled evidence can also damage a party's credibility. Judges can give adverse inference jury instructions in which a jury can infer that destroyed evidence would have hurt the spoiling party's case.

The 2006 Amendments do not state how or when a duty to preserve is triggered. The scope of this obligation and the practices that might satisfy it are also not addressed. The only help the amendments give is through FRCP 37(f) which provides protection from sanctions when evidence is lost through a "routine, good faith" operation of information systems.

## VII. Notable Recent Cases

**Williams v. Sprint**, (D.Kan.) A recent class action suit produced two discovery orders from the same Magistrate Judge concerning the production of metadata. An order in 2005 required Excel spreadsheets to be produced in their native format with metadata. See "Williams I" 230 F.R.D. 640 (D.Kan. 2005). However, a 2006 order denied a motion to compel production of emails in their native format. See "Williams II" 2006 WL 3691604 (D.Kan. 2006).

"Williams I" – The Plaintiff requested Excel spreadsheets in their native format so it could perform calculations with the data. The excel documents' metadata included formulas that were only visible in the native format. The defendant did not produce the Excel spreadsheets in their native format and when it was compelled to do so, it "scrubbed" the metadata and locked certain cells of data. Defendant argued that orders to produce electronic documents generally should not require production of documents in their native format. The Court rejected this argument and held that electronic document production

should include metadata unless there was a timely objection, an agreement between parties otherwise, or a request for a protective order.

“Williams II” – The Plaintiff requested transmitted emails in their native format with their attachments attached to their corresponding emails. This request was made so that the plaintiff would not have to spend time matching emails with their attachments. Defendant objected to this request because producing the emails in this fashion would potentially reveal privileged information without the ability to redact it. The Court denied plaintiff’s request. It found defendant’s concerns over privilege trumped plaintiff’s interest in convenience.

**Coleman Holdings, Inc. v. Morgan Stanley**, 2005 WL 679071 (Fla.Cir.Ct. 2005). In a lawsuit for fraud in connection with a corporate merger, the plaintiffs made a voluminous request for company emails. These emails were stored on back-up tapes in warehouses and off-site locations and proved very difficult and costly to collect, review and produce. After many failures to comply with court-ordered discovery, the court sanctioned the defendant for “systematically failing” to produce evidence. The Court also sanctioned the defendant for writing over relevant emails after it had knowledge of possible legal action. The Judge gave an adverse inference instruction to the jury because of the defendant’s discovery violations. This inference allowed the jury to find that because the defendant could not produce certain emails, the fraud allegations must be true. The jury returned a verdict for over one billion dollars.

### **VIII. Best practices for an information management system**

It is rarely feasible for an information management system to preserve all records. However, a system cannot simply automatically delete all information and survive an evidence spoliation challenge. An information management system must be designed so it can function efficiently in both the regular course of business and in anticipation of litigation. A system’s features should also be well documented, so that in the event it is challenged, evidence can be provided to prove the system is designed and implemented in “good faith,” not to spoil evidence.

#### ***An Information Management System should:***

##### **Establish retention periods for records, categorized by content.**

- This reduces the costs of managing records beyond their business and legal necessity.
- Some types of materials might have statutory requirements. For example, Pension plan records must be retained for 6 years under ERISA. See. 29 C.F.R. § 4007.10 (2006)

**IX. Three steps for establishing a retention period schedule**

1. Determine your capability to implement a retention schedule. Electronic records management programs might be necessary.
2. Categorize records with the help of employees of all departments. This allows categories to be based upon the company's individualized needs and to be in terms easily administrable by all employees.
  - a. Consideration should also be given as to whether categories are narrowly-drawn or broadly-drawn. Narrow categories will allow for periods drawn precisely to business and legal needs, but will also be hard to administer. Broad categories will be easy to administer but less precisely drawn to need.
  - b. Highly distinct employees, units and geographic branches might benefit from specialized periods that differ from a company's uniform schedule.
3. Clearly fix retention periods to a readily ascertainable date in order to ensure consistent application of the record retention schedule.
  - a. Important factors to consider in setting a period's length:
    1. Applicable legal requirements for record retention
    2. Relevant statutes of limitations
    3. Expectation of future lawsuits
    4. Company's history and litigation profile
    5. Business utility and historical value of records
    6. Burden of retaining records and potentially having to search for and produce them for litigation

Establish a procedure for "record holds" when litigation is anticipated.

**Prepare for a record hold by:**

1. Defining the events that will trigger a hold (events should include actual or reasonably anticipated litigation, subpoenas, governmental examinations, governmental or internal investigations, or enforcement proceedings)

2. Identifying the individuals responsible for issuing and monitoring holds
3. Addressing how relevant information and individuals are identified
4. Laying out the steps of a record hold notice

**When issuing a “record hold” a system should:**

1. Verify receipt of a record hold notice
2. Verify compliance
3. Suspend all relevant automatic deletion programs and paper document destruction
4. Issue reminder notices and modifications of the record hold as needed
5. Alert record hold notice recipients of termination

Successful implementation of the system should include

**Employee education about policies regarding:**

1. Retention policies
2. Disposal Policies - timely and appropriate disposal of documents after retention policies
3. Record hold procedures

**An accurate index of all hard copy records**

1. This allows for efficient retrieval and disposal

**Automated Computer and Email Systems**

1. These can allow employees to categorize records that are automatically retained and deleted pursuant to the retention policy (in the absence of a record hold.)

**Regular review and modification of system**

1. This allows changes in business and legal needs to be addressed
2. This also allows implementation to be reviewed for efficiency

## **Documentation of system to assist with review**

1. This also provides evidence of a “good faith” information management system in the event the system is challenged.

(“Creating a Strong Foundation For Your Companies’ Record Management”, by William Dodero and Thomas Smith November 2007. *available at: <http://www.ediscoverylaw.com/2007/10/articles/news-updates/creating-a-strong-foundation-for-your-companys-records-management-practices/>* ).