CONTRIBUTED CONTENT & PRESENTATIONS

New Federal Rules Changes Regarding Electronic Documents: Is Your Company Prepared?

Co-Author: Karen E. Anzuini

DECEMBER 7, 2006

New Federal Rules of Civil Procedure became effective December 1, 2006. These rules deal largely with issues related to the production of electronically stored information (ESI) in cases of litigation. They have a huge impact on any organization that may become involved in a lawsuit. The consequences of failing to be aware of and follow these rules can be devastating to companies and company executives. Sanctions may be imposed not only when a party has acted in bad faith, but also in the course of ordinary negligence.

One key feature of the new Federal Rules of Civil Procedure provides a "safe harbor" for companies that fail to produce electronically stored data in litigation if the data was lost pursuant to the "routine, good-faith operation of an electronic information system." Companies that have implemented such a system may not be sanctioned for losing the data, absent "exceptional circumstances". As a result, companies should take advantage of this protection and reduce their risk of potential liability for loss of data by making sure they have an electronic information system in place that meets the requirements of the new rule.

There have been a number of well publicized examples of large organizations that have been fined many millions of dollars for the destruction of data relevant to a lawsuit. Such fines for destruction of data can be imposed upon any size organization, mid-sized, large or small.

ESI includes email, word processing documents, databases, voicemail messages, instant messages, text messages, web sites and any other information stored in an electronic format. It can reside on corporate servers, corporate or home pcs or laptops, cell phones, Blackberrys, flash drives, voicemail servers, backup tapes and a myriad of other devices. Locating and producing ESI can be very time consuming and extremely costly. In addition, best practices may require that a litigation hold be put in place as soon as litigation is anticipated.

So what steps should your organization take to reduce risk, keep costs down, and ensure you are prepared for any litigation requiring the production of ESI?

Have a Document Retention Policy that includes policies for paper and electronic data.

A Document Retention Policy clarifies what type of documents and data must be retained and for how long, A policy will promote efficiency, reduce storage and administration costs, help ensure

compliance with federal and state laws and regulations, and help protect you in litigation. The destruction of documents according to a clearly communicated and enforced Document Retention Policy, put in place for valid business purposes may help convince the courts that the destruction of certain data is reasonable. A Document Retention Policy must be communicated and enforced to be effective.

Know where your data lives
A comprehensive data map which documents where each type of data is stored (network servers, laptops, home pcs, mobile devices, etc) will not only be invaluable when requests for data are made in connection with a lawsuit, but may also bring to light some risk management issues that had not previously been considered. Such documentation should include the type of data, location(s), and custodians. You might find that going through this exercise will result in changes in other policies that streamline, standardize and secure the storage of your organizations' valuable data.

Locate and document the location of ALL of your backup tapes and know what they contain
The retrieval of data from backup tapes can be one of the most costly and time consuming exercises in data production. Older tapes may not be compatible with new hardware and software systems, but may need to be produced in a lawsuit. Because older backup tapes are seldom accessed, they may be stored in locations that current IT staff are not even aware of, only to be accidentally found at a later date. Companies and their key executives may be sanctioned because backup tapes were only accidentally located after data for the lawsuit has been produced. Cataloging the contents of backup tapes in the ordinary course of business will save time and cost later. Does a tape contain emails and databases, word processing documents, or financial information? From what dates? Not knowing what kind of information is on the tapes may cause you to go through any and all of them that may contain relevant data. The time and cost can be extremely high. Backup tapes are to be included in any Document Retention Policy, with retention and destruction schedules consistent with the rest of the policy.

Have a Litigation Response plan
Before you are involved in a lawsuit have a plan for how to implement a litigation hold. Know who needs to be included in any communications and what the procedures will be. How do you ensure compliance? Failure to comply can result in costly sanctions and additional lawsuits. Depending on the size of your organization, a Litigation Response Team may be identified, including a cross section of employees from the legal, technical, risk management, human resources and records retention functions.

Implementing these items will require teamwork, time, and money, but will result in increased efficiencies and security, diminished risk and longer term cost reduction. Keeping the policies and procedures up to date will be an ongoing business process.

Being unprepared can be devastating to an organization and it's executives. It can also result in a lot of unwanted publicity, harming an organizations reputation and it's future.

With the recent changes in law and the importance of having a timely, effective plan for these legal issues, you should make sure your company's information is in compliance. For more information

regarding this and other issues regarding E-discovery, please contact David Mellott or any of our E-Discovery team at 216-363-4465.