

E-Discovery: Amendments to the Federal Rules of Civil Procedure

On December 1, 2006, amendments to **The Federal Rules of Civil Procedure** (FRCP) went into effect and deal with the conduct of all civil suits brought in Federal district courts and include specific guidelines for discovery and disclosure.

These amendments are a significant departure from traditional paper discovery rules to electronic discovery. The Supreme Court recognizes the importance of electronically stored information and the prohibitive costs of document review and protection of privileged documents. The proposed amendments will affect the way corporations manage their electronically stored information.

Electronic discovery, or **e-Discovery**, refers to "any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case". The increase of electronic information has led to a new era in legal proceedings whereby courts can now mandate searches of digital data for evidence. This process is known as e-discovery, short for electronic discovery. E-discovery can include searching data on a single computer as well as on a network.

New amendments to the law that went into effect in December state that both parties involved in any court hearings have 30 days to determine how to give access to data for the purpose of gathering evidence for the case. A small to medium business will need reliable systems for email archiving and document retention. Fortunately, archiving and storage solutions are available that can help these businesses save valuable time and money, and hopefully avoid expensive penalties in the unfortunate event of court proceedings.

With Enterprise Content Management* (ECM), the two rules to focus on include FRCP 26(b)(5) and FRCP 34(b):

- **FRCP 26(b)(5)** deals with General Provisions Governing Discovery; Duty of Disclosure; Discovery Scope and Limits; and Claims of Privilege or Protection of Trial Preparation Materials.
- **FRCP 34(b)** focuses on the Production of Documents, Electronically Stored Information, and Things. These amendments to the FRCP address a general corporate problem - the volume of electronically stored information and its maintenance.

During an electronic discovery process, all types of data serve as evidence- from e-mails, Microsoft Office files, accounting databases, CAD/CAM files, spreadsheets, audio files, calendar files, Web sites, and any other electronically-stored information text documents. Email is often the most valuable source of evidence in civil or criminal litigation because of slack corporate management.

Recommendations

Even though the new e-discovery regulations would place a great deal of responsibility on business owners; everyone can be prepared by learning about the regulations, and implementing the following recommendations:

Implement a system for email archiving: Emails are now considered valid sources of evidence in some legal cases, and therefore it is important to have an email archiving system in place. If businesses have their own email servers, they should back up their server; so that information is not lost should there be any physical damage to the server. If you use an external email provider, businesses should implement a system to back up all company emails so they have access to them when necessary. [Click here for additional information on email compliance.](#)

Install security solutions: Taking into account the importance of electronic documents and electronic information within a legal context, it is necessary to make sure that businesses have original, uncorrupted versions. Creating multiple layers of protection around computers and valuable electronic information is critical. Businesses should have antivirus and firewalls software installed on every device, including firewalls on corporate networks, and Virtual Private Networks (VPNs) for remote connections. Also important is the implementation of security software and antivirus software on email servers.

Implement a backup and recovery solution: Most often, emails and other information in electronic form are kept on many pieces of physical hardware. The ability to securely store and retrieve this data is an important part of regulation compliance. Businesses could consider implementing a disk-based backup solution so that they do not lose valuable information. Disk-based backup not only assures you of timely backups without requiring manual tape backups, it also stores newer versions of documents as changes are made, and allows businesses to quickly and easily search and retrieve relevant data. [Click here for more information on backup storage options.](#)

Create corporate policies: Corporate policies that provide guidelines on document retention and email archiving need to be created and communicated by giving your employees specific actions to take regarding how and where to save important information, you are taking proactive steps towards making businesses compliant with new regulations.

Conclusion

New regulations, including the amendments to the Federal Rules of Civil Procedure require businesses to take responsibility for their electronic information, including archiving and providing quick access to data that may be required in the case of legal proceedings. By learning about these changes to the law and implementing technology solutions, businesses can become compliant. Plus, being prepared can help you avoid possibly costly penalties.

* Enterprise Content Management (ECM) is the technologies used to capture, manage, store, preserve, and deliver content and documents related to organizational processes. ECM is about managing information assets. It is a framework enabling the management of information assets across an organization, and ties in platforms and programs such as; Electronic Document Management, Electronic Records Management, Business Process Management, Collaboration, Web Content Management, and Digital Asset Management.

Content from AIIM.org and Symantec.