

ACUTA Alert: Federal Rules Governing Destruction of Electronically Stored Information (Dec. 2006)

Suite 200
152 W. Zandale Drive
Lexington, KY 40503-2486

TEL 859-278-3338
FAX 859-278-3268
NET www.acuta.org

ACUTA member institutions should be aware of new rules which may dramatically impact their obligations to preserve and produce electronically stored information (“ESI”). ESI includes virtually anything that can be stored in an electronic format such as e-mails, computer and network activity logs, cache and temporary Internet files, digital recordings, voice mails stored in an electronic format or accessible via a computer, spreadsheets, and telephone logs. (The rules do not contain a definitive list of what constitutes ESI.) Each institution should consult with counsel to determine the policies and procedures that their institution needs to implement to comply with applicable law. This Alert provides only a broad overview of how the new rules may impact ACUTA members and what steps they should consider taking.

Effective December 1, 2006, the U.S. Supreme Court approved several amendments to the Federal Rules of Civil Procedure covering ESI and electronic discovery. In general, the amendments clarify parties’ obligations to produce ESI during federal civil litigation. ACUTA members, however, need to be familiar with the rules and take appropriate action even if federal litigation is not looming on the horizon. The failure to take appropriate steps now, and ensure the proper retention and storage of ESI, could subject an institution to significant sanctions in the future or result in considerable forensic accounting costs if the institution is ordered to retrieve ESI on a backward looking basis. In one recent case, for example, a court fined a company \$15 million for failing to properly identify ESI.

What Types of ESI Will We Have to Produce?

Under the new rules, institutions will have to identify two types of ESI during the initial stages of federal litigation: (1) ESI that is potentially relevant and reasonably accessible; and (2) ESI that is potentially relevant but *not* “reasonably accessible because of undue burden or cost.” In general, institutions will have an affirmative duty to produce ESI falling into the first category, but will not have to produce ESI that is not reasonably accessible. Accordingly, it is incumbent upon information technology managers to organize and store ESI in a manner that will enable the institution and its attorneys to identify relevant ESI and determine what subset of that information is reasonably accessible.

How Do We Determine What “Reasonably Accessible” Means?

The phrase “reasonably accessible” is, by necessity, a malleable term and institutions should consult counsel for more guidance. Part of the definitional problem is that a court may find certain ESI to be reasonably accessible in one case

(Continued)

*Supporting higher
education communications
technology professionals
in contributing to the
achievement of the
strategic mission of their
institutions.*

but not reasonably accessible in another. For example, in litigation involving a relatively small amount of money, courts will be more inclined to consider ESI not reasonably accessible than in cases involving a substantial amount of money. Institutions should bear in mind, however, that they may have the burden of proving that producing certain ESI will be prohibitively expensive. Thus, the more information institutions have about their ESI, and the costs associated with producing that information, the better prepared they will be for litigation. With these caveats in mind, however, some general observations can be made.

Courts *may* find the following types of ESI not reasonably accessible and thus not subject to production in federal litigation:

- ESI destroyed in good faith in accordance with a reasonable document retention policy.
- ESI stored on backup-tape systems for disaster recovery purposes.
- Legacy data from computer systems which are no longer in use.

How Can We Determine Whether ESI Is Potentially Relevant to Litigation?

Unfortunately, it is impossible to identify every piece of ESI that could become relevant in future litigation. Accordingly, each institution should explore this topic with counsel. There are some events, however, that may trigger an institution's obligation to retain ESI:

- Major accidents and injuries.
- Employee terminations.
- Internal investigations into meritorious claims.
- Threats to sue the institution.

Can We Ever Destroy ESI?

There is currently significant confusion over an institution's obligation to preserve ESI. Institutions typically recycle, overwrite, and change information without manual prompting and without regard to on-going litigation. Most computer systems, for example, purge e-mails at regular intervals. Thus, institutions lose a significant amount of ESI due to the routine operation of its computer system. The new federal rules reflect an understanding that institutions cannot retain all ESI indefinitely.

The new rules contain a safe harbor that generally prevents institutions from being sanctioned for failing to provide ESI destroyed by the routine, good-faith operation of an electronic information system. Here are some examples of routine destruction operations that *may* fall within the safe harbor.

- Automatic overwriting of information.
- Programs that automatically change metadata.
- Programs that automatically discard information that has not been accessed for a certain period of time.
- Databases that automatically update, create, or discard information without manual direction.

Significantly, however, a party may be under an obligation to prevent the routine destruction of information when there is reason to know that the information could be relevant. For example, an institution may be sanctioned if it knows that certain relevant e-mails are scheduled to be purged, but takes no action to preserve the e-mails. In accordance with a proper document retention policy, however, institutions may destroy ESI when there is no need for it. Thus, each institution should work closely with its counsel to determine when routine destruction operations should be suspended and whether it has an obligation to do so. To that end, institutions should explore policies and procedures for issuing “litigation holds” on certain ESI. A litigation hold is an order issued by an institution advising its employees to preserve information.

Summary of Steps that Information Technology Managers Should Take:

- Ensure that your institution has a comprehensive data retention policy for ESI based on the revised federal rules.
- Identify routine document destruction activities that can be suspended if the need arises.
- Design a plan for suspending routine document destruction.
- Ensure that there is a mechanism for informing employees of litigation holds.
- Implement a program to educate campus employees about the institution’s document retention policy and ensure strict compliance.
- Identify activities and programs that destroy or store ESI.
- Ensure that the institution’s attorneys are fully aware of the campus’ IT capabilities and the institution’s ESI.
- Work closely with the institution’s counsel to create a plan for storing ESI in a manner that will decrease the institution’s retrieval expenses.
- Identify ESI that is not “reasonably accessible because of undue burden or cost.”
- Ascertain the institution’s capacity for preserving snapshots of data that automatically change.

Following is a link to the new rules as amended, including commentary:
http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf. If you have questions regarding legal interpretation, please consult with your institution’s legal counsel.

ACUTA Legislative/Regulatory Affairs Committee

End