

Frequently Asked Questions

Electronic Discovery and Data Preservation

1. What do “electronic discovery” and “data preservation” mean?

“Discovery” is the process by which relevant information is exchanged between parties in a lawsuit. It is conducted via production of documents and the taking of depositions. Federal and state courts have long recognized that electronic data is subject to the same discovery rules as other evidence relevant to a lawsuit. The issue has received substantial national attention recently, however, because of a series of court rulings resulting in the imposition of huge sanctions on parties for their failure to preserve electronic data and because of amendments to the Federal Rules of Civil Procedure that took effect on December 1, 2006. Upon notice that a lawsuit has been commenced against the University (or a charge filed with an administrative agency), or if it is reasonably anticipated that a lawsuit may be brought (or a charge filed), the University and all of its faculty and staff members are now under a legal duty to preserve all evidence, whether hard copy or electronic, that might become *relevant* to the lawsuit.

2. What data needs to be preserved?

The new federal rules require a party to suspend routine or intentional purging, overwriting, re-using, deleting, or any other destruction of electronic information relevant to a lawsuit, including electronic information wherever it is stored – at a University work station, on a laptop, or at an employee’s home. It includes all forms of electronic communications – e.g., e-mail, word processing, calendars, voice messages, instant messages, spreadsheets, videos, photographs, information in PDA’s, and data in any other locations where electronic information may be stored. This electronic information must be preserved so that it can be retrieved – if necessary – at a later time. The information must be preserved in its original electronic form, so that all information contained within it, whether visible or not, is also available for inspection – i.e., it is not sufficient to make a hard copy of electronic communication.

3. What will I have to do?

You will be notified of the duty to preserve electronically stored information through a notice called a “litigation hold” (or a “preservation hold”). You will then be asked to cooperate with the Office of University Counsel, the IT Security

Office, and your local IT personnel to ensure that we identify and preserve all potential sources of electronically stored information in your possession or under your control. You will be asked to complete and return a questionnaire identifying all potential sources of electronically stored information. It is critical that you complete and return this questionnaire without delay. Until IT personnel have taken steps to preserve your electronically stored information, you should be particularly careful not to delete, destroy, purge, overwrite, or otherwise modify existing electronic data.

4. For how long will this go on?

Counsel or IT Security will notify you when you and the University are no longer obligated to retain the preserved data. Generally, this will be when the statute of limitations has expired with respect to the claim or – if litigation has been commenced – when the lawsuit and all appeals have been concluded. When the duty to preserve evidence ends, the archived data will be returned to you or destroyed, at your option.

5. Do I need to also preserve data on my home computer?

The same rules apply to any computer that stores information potentially relevant to a lawsuit. Thus, if you use your home computer for University-related business (including e-mail on your University e-mail account or on a personal account such as AOL, gMail, etc.), you must preserve the data on that computer.

6. Can I take personal or sensitive material that isn't relevant to the case off my computer?

You may remove data from your computer (or segregate it from the data that will be preserved) if you are absolutely certain that it is unrelated to the claim (e.g., correspondence entirely unrelated to University employees or University business, income tax returns, your music library, etc.). However, we often find that it is difficult at the beginning of a lawsuit to be certain about what might later turn out to be relevant. So, you should examine each and every file you are considering deleting – i.e., do not make wholesale deletions of data. You may be questioned under oath at a later date by an attorney representing the opposing party about what data you may have destroyed.

7. I already deleted something that might be relevant - - Should I be concerned about that?

The duty to preserve information arises only when you reasonably anticipate litigation. Electronically stored information not preserved before that time should not create a problem.

8. What if I am involved in an ongoing matter relating to the person who is suing the University?

You must also preserve any new electronic information that is generated after receipt of a *litigation hold* that may be *relevant* to the dispute (such as an employment claim by a current employee where relevant new documents may be created during the ongoing employment relationship). The IT Security Office will work with you to ensure the preservation of new data, probably with EZ Back-up Service.

9. Who is going to be paying for the cost of preserving ESI?

The costs associated with complying with the e-discovery requirements will be handled in the same manner as other litigation expenses are presently handled.

10. Who will be looking at my data?

Initially, no one will review your data. If and when a discovery request is made, you may be asked to conduct a search of the data or IT Security personnel will conduct the search. IT Security will store centrally all preserved data. You will have the opportunity to be present if and when your data is ever accessed. On occasion, before a discovery request is made, the Office of University Counsel may want to review electronically stored information to assist in answering the lawsuit or to comply with initial discovery obligations.

11. Who decides what data will be turned over to the opposing party?

The same rules of relevance that apply to "paper" discovery also apply to the discovery of electronically stored information. Before any data is turned over to the opposing party, the Office of University Counsel will review it for relevance and determine that it is not otherwise protected or privileged.

12. Since when did we have to go to all this trouble?

Electronically stored information has been discoverable since the 1980's. Because of the egregious misconduct by several defendants and because of the ever-widening use of computers, over the last several years the courts have developed rules specific to the preservation of electronic data. The new amendments to the Federal Rules of Civil Procedure addressing electronic discovery took effect December 1, 2006.

13. What if I don't want to disclose my data?

The University and its employees have a legal duty to preserve, and subject to the rules governing discovery, turn over electronically stored information. In short, the law does not offer us a choice. Failure to abide by the law may result in judicially imposed monetary sanctions and adverse findings in the litigation. We

will take steps to protect your privacy and to ensure that protected/privileged information is not disclosed, but ultimately the court will be the arbiter of whether sensitive information must be disclosed.

14. What should I do with my electronic data if I leave the University?

If you plan to leave your employment with the University during the pendency of a lawsuit for which you have received a preservation hold, you should confer with the Office of University Counsel or the IT Security Office before relinquishing control of your computer.

15. What if I have additional questions?

Contact the Office of University Counsel or the IT Security Office.