

Process Options for Consideration in Responding to Federal Rules of Civil Procedure for Electronic Discovery

Required Activities

To meet the changes to the Federal Rules of Civil Procedure there are three discrete activities and phases: hold, preserve and search.

- Hold – take technical steps necessary to ensure that normal business practices such as backup tape recycling or other data purging processes, including individuals deleting their e-mail, are interrupted so as not to lose data. Since implementing a hold on normal business operations can cause many adverse operational side affects implementing a hold is not a desirable situation.
- Preserve – collect a snapshot of electronic data to store and preserve in the event of search requests. Very quick preservation should limit or even eliminate the necessity of implementing a hold on business operations.
- Search – execute keyword and timeframe searches on preserved data for the purpose of discovering all lawsuit relevant documents, including searches explicitly requested by the plaintiffs.

Please note that the considerations outlined here only applied to data in the individual's direct possession. Should it be appropriate to acquire copies of such data sources as e-mail stored on a server or system back-ups, any selective data gathering with the intent of addressing privacy concerns would be largely moot.

Concerns That The University Must Consider

A number of drivers and concerns must be taken into account as the University works to establish procedures and practices to respond to the changes in the Federal Rules for Civil Procedures:

1. Individual privacy
The processes implemented to respond to electronic data preservation and discovery must take into account the infringements upon and concerns of the individual privacy of our community members.
2. Prevention of data loss
Our processes and procedures must take steps necessary to preserve our data from loss upon being notified of a potential lawsuit. Data loss can come from inadvertent or intentional deletion of files, lost data stores or other events.

3. Minimize individual disruptions
Our processes must be conscious of the strong potential for significant investments of time by the individuals named in the lawsuit. It is probably not acceptable for us to implement processes that require defendants to spend dozens of hours searching for all relevant data in all areas of their computers.
4. Operational efficiencies
The activities required to meet these new rules must be operationally efficient to ensure timely preservation and processing of the data. Further, the University must take all practical steps to ensure staff can effectively scale to the operational demands.
5. Process consistency
The University must ensure the processes and procedures developed to meet these new rules are consistently followed and executed. Consistency will be very important if our processes are questioned in court.

Since the changes to the federal procedures do not dictate how holds, data preservation and searches need to be implemented, the University has options to accomplish these tasks. It is important, however, that the University determine who performs these activities and how these requirements will be met to ensure consistent and defensible procedures.

Available Options

The purpose of the following sections is to provide a set of viable options for us to consider as we balance such issues as operational efficiencies, personal privacy and the others mentioned above.

Who Executes the Process

The first question that must be addressed is who or which office should be responsible for collecting and preserving the electronic data. There are probably three logical choices at the University: technical support in the local unit, the end user or owner of the computer or CIT (“Central IT”) Staff.

- *Local IT Support* – Upon notification of a potential or actual lawsuit, this option would require the Office of University Counsel to identify and meet with the local unit and their IT personnel to determine what needs to be collected and how this collection will be accomplished. Every unit would be required to understand the established processes, execute the processes, store or deliver the information and support the IT needs of the lawsuit.
- *End user or owner of the computer* – Upon notification of a potential or actual lawsuit, this option would require the Office of University Counsel to meet with the affected unit and provide the requirements that must be met and the IT procedures that must be followed to those identified in the lawsuit. Upon this

notification, each defendant would be required to understand the established processes, execute the processes, store or deliver the information and support the IT needs of the lawsuit.

- *CIT Staff* – Upon notification of a potential or actual lawsuit, this option would require the Office of University Counsel to meet with CIT to determine what needs to be collected and how this collection will be accomplished for the environment of the specific unit. CIT, in coordination with local personnel, would then execute the established process, store and deliver the required information.

To help assess and evaluate these options the concerns that were outlined above will be used.

	Protect Individual Privacy	Prevent Data Loss	Minimize Individual Disruptions	Operationally Efficient	Process Consistency
Local IT Support	3	2	2	2	2
End User	1	3	3	3	3
CIT Staff	2	1	1	1	1

(1=Best, 2=Average, 3=Worst)

What Process Makes Sense for the University

The second question that must be answered is what processes should be used for the collection of these potentially relevant data. Similar to the initial question there are a number of options available to the University. While variants of these options can fairly easily be identified, the main options are:

- *Modify our data handling processes* – This option would look to introduce policy and procedures that would require all University members who are involved with employment, tenure or other such decisions to store all business related data and documents on a centrally available server. This would require standardization of and changes to our current individual business handling practices and the deployment of university-wide or local data storage.
- *Preserve data using the CIT EZ Back-up Service* – This option would require each affected University member to install a data preservation specific instance of the EZ Backup service on all computers that may contain relevant information. This technique could be used for the initial preservation as well as meet on-going preservation needs. While this solution may be more costly from a central infrastructure point of view, it is probably the most operationally efficient, most easily satisfies on-going preservation requirements and meets fewer privacy concerns. This option could further be augmented through established data

handling procedures to help ensure better separation of university and private data.

- *Preserve only the data that are known to be associated with the case* – This option would require each affected individual to perform a potentially exhaustive search of all the computers used for University business and then make copies of identified documents to be delivered to the Office of University Counsel. Because documents are often not provided very descriptive names, files tend to be strewn about across the hard drive and the volume of data will probably be huge this may be an extremely laborious task. Further, the Office of University Counsel will need to weigh as to whether this option meets the requirements for preservation.
- *Preserve only data that are collected from default or known locations of the computer* – This option would make copies of all documents and text from known or well established locations on the hard drive. Some examples of these locations include the My Documents folder on Windows systems, the Attachments folder for mail applications, etc. While this would minimize the amount of personal involvement required by the computer owner or user, it could potentially include the collection of personal information.
- *Image the entire computer* – With this option, a full system image of each computer would be collected and stored. This image would include everything that is stored on the hard drive including business data, personal data, web caches and meta data about the files. This is by far the most operationally efficient process.
- *Remove all known personal data prior to executing a full image of the computer* – This option can be used in conjunction with the previous ones. It would allow or require the computer user or owner to search out and remove all files and other data that are identified to be purely of a personal nature prior to a full image of the computer hard drive. This would allow for the removal of such things as personal tax documents, personal word documents or personal e-mail.

To help assess and evaluate these options the concerns that were outlined above will be used.

	Protect Individual Privacy	Prevent Data Loss	Minimize Individual Disruptions	Operationally Efficient	Process Consistency
Introduce data handling policy and procedures	1	2	2	1	2

Use centrally available EZ Backup Service	2	1	1	1	1
Only data known to be associated with case	1	3	3	3	3
Data collected from typical locations	2	2	1	1	1
Image everything	3	1	1	2	1
Remove personal data prior to image	1	2	3	2	2

(1=Best, 2=Average, 3=Worst)