

Project Planning for E-Discovery: A One-Page Guide

Corporate electronic document repositories are enormous and the responsive portion is typically very small. Cost-effective e-discovery therefore requires drastic culling. The culling must be done in a way that is rational, defensible, in good faith, and in compliance with the scope of Rule 26. The approach outlined below has proven successful.

Interview client to identify pertinent custodians. All discovery begins with identifying the people likely to possess or have access to responsive documents. In the context of corporate e-discovery, these people are called "custodians." A custodian is generally a person with a logon account on the client's network. E-discovery is custodian-based because electronic documents are typically organized or controlled by logon identity: mailboxes, home directories, permission to access shared directories and databases, and possession of local hard drives and other storage devices. **Important:** Be sure to identify departed custodians who were present during the relevant period.

Interview client's IT administrators to identify pertinent repositories. Using the list of pertinent custodians, interview the client's IT department to determine location, scope, and format of the repositories to which those custodians had access. This includes: overview of pertinent network architecture, identification of pertinent systems and repositories for each custodian, inventory of the backup media for those systems, local equipment issued to each custodian, and company policies on disaster recovery and document retention. **Important:** Be sure to address the entire relevant time period. Be sure to identify pending system changes that could cause data loss.

Issue preservation letters; implement preservation plan. There should be two preservation letters. The first is directed to pertinent custodians instructing them to preserve documents based on subject matter (specific issues, projects, products, companies, people, etc.). The second is directed to IT personnel instructing them to preserve repositories that contain those documents. The letters must provide concrete guidance. The preservation plan itself must allow for practical necessities such as increasing mailbox quota size or authorizing purchase of additional backup tapes. **Important:** If a custodian has an incentive to spoliolate evidence, preserve that custodian's repositories before issuing the preservation memo.

Interview custodians to identify pertinent subsets. The next level of culling is to determine the potentially-responsive subsets of the repositories to which the custodians have access. This is done by interviewing the custodians to determine where and how they organize their documents. If there is a rational and reliable file organization structure (such as organizing documents by folder) this may be sufficient. If the repositories are disorganized, it may be easier to take entire repositories and just use the filtering techniques described below (note, however, that this is more costly).

Develop a harvesting plan. Once the pertinent subsets are identified, you must address the logistics of harvesting copies that can be processed for review. For active files, this can be done by copying mailboxes and repositories to portable hard drives. For archived files on tape, this can be done by restoring tapes to extract the pertinent portions. **Important:** Files must be extracted in a way that does not alter their evidentiary quality. The procedures must be fully documented. Many corporate IT departments do not have the resources or background to conduct proper harvesting in-house.

Computer forensics. In some cases (especially those involving spoliation or misconduct) it may be necessary to preserve forensic images of some computers. This is a specialized form of harvesting that captures the entire content of a physical medium (like a hard drive) so deleted files and other hidden data might be recovered. Due to the time and expense involved, this is usually done only when there is a specific need for this level of analysis.

Prepare for automatic disclosures and preliminary conference. For federal cases, the information gathered above prepares you to comply with these requirements. **Important:** At the preliminary conference, you should generally not agree to produce in native format. It is better to produce in a mainstream e-discovery format compatible with litigation-support database and review systems. This format typically includes TIFF images endorsed with numbers and confidentiality legends, searchable text, and searchable metadata.

Develop processing criteria. The harvested collections need to be deduplicated and processed in preparation for being loaded into a document review system. For large collections, it is common practice to do further culling by means of keyword filtering. At the end of these processes, you will have a culled universe of potentially-responsive documents ready to be reviewed for actual responsiveness and privilege. **Important:** Be sure to document the filtering and processing criteria so you have a record of what was done.

Prepare a review and coding plan. This is where you develop your attorney review budget, define the issue-spotting elements for your reviewers, choose your coding fields, set your criteria for determining what is responsive, staff up, and train your review team. Depending on the nature of the data, a two-pass approach (easy calls / hard calls) is often the most cost-effective.

Produce. After review, the result of these steps will be a collection of coded documents appropriate for production. At this point, the responsive files should be converted to the production format described above so it can be served on the opposing party.

Other side: Federal Rules for E-Discovery

For more information, please call.