

A Rule 16(c) Pretrial Conference Agenda for Computer-Based Discovery

Computer-Based Discovery in Federal Civil Litigation

Kenneth J. Withers
Federal Judicial Center
Washington, D.C.

APPENDIX A

The following checklist represents a maximalist approach. It should be scaled to fit the needs of the particular case, the resources of the parties, and the litigating styles of the attorneys involved.

I. When is a Detailed Rule 16 Notice Most Appropriate?

- When the substantive allegations involve computer-generated records, e.g., software development, e-commerce, unlawful Internet trafficking, etc.
- When the authenticity or completeness of computer records is likely to be contested
- When a substantial amount of disclosure or discovery will involve information or records in electronic form, e.g., e-mail, word processing, spreadsheets, and databases
- When one or both parties is an organization that routinely used computers in its day-to-day business operations during the period relevant to the facts of the case
- When one or both parties has converted substantial numbers of potentially relevant records to digital form for management or archival purposes
- When expert witnesses will develop testimony based in large part on computer data and/or modeling, or when either party plans to present a substantial amount of evidence in digital form at trial
- In any potential “big document” case in which cost associated with managing paper discovery could be avoided by encouraging exchange of digital or imaged documents (especially if multiple parties are involved)

The purpose of a detailed Rule 16 notice is to save the parties time and expense by anticipating the most common issues of computer-based discovery, developing a reasonable discovery plan, and avoiding unnecessary conflict. A detailed Rule 16 notice would not be appropriate if, in the opinion of the judge, the notice might serve to alarm the parties needlessly, raise unreasonable expectations or demands, or encourage the parties to engage in wasteful discovery.

II. Preservation of Evidence

A. What steps have counsel taken to ensure that likely discovery material in their clients’ possession (or in the possession of third parties) will be preserved until the discovery process is complete? If counsel have not yet identified all material that should be disclosed or may be discoverable, what steps have been taken to ensure that material will not be destroyed or changed before counsels’ investigations are complete?

If more specific direction is needed:

B. Have counsel identified computer records relevant to the subject matter of the action, e.g.,

- Word processing documents, including drafts or versions not necessarily in paper form
- Databases or spreadsheets containing relevant information
- E-mail, voicemail, or other computer-mediated communications
- Relevant system records, such as logs, Internet use history files, and access records

C. Have counsel located the following computer records:

- Active computer files on network servers
- Computer files on desktop or local hard drives
- Backup tapes or disks, wherever located
- Archival tapes or disks, wherever located
- Laptop computers, home computers, and other satellite locations
- Media or hardware on which relevant records may have been “deleted” but are recoverable using reasonable efforts

D. Have counsel made sure all relevant computer records at all relevant locations are secure, e.g.,

- Suspended all routine electronic document deletion and media recycling
- Segregated and secured backup and archival media
- Created “mirror” copies of all active network servers, desktop hard drives, laptops, and similar hardware

E. Have counsel considered entering into an agreement to preserve evidence?

F. Does either party plan to seek a preservation order from the court?

III. Disclosure and Preliminary Discovery

A. Have counsel designated technical point-persons who know about their clients’ computer systems to assist in managing computer records and answering discovery requests?

B. Have counsel prepared a description of their respective parties’ computer systems for exchange? Does either party need to know more before discovery can proceed?

If, after considering whether the hints in the following list may do more harm than good, the judge determines that the parties are unclear as to what they need to know at this stage and should get further guidance, the judge may suggest that they exchange information on the following points:

- Number, types, and locations of computers currently in use

- Number, types, and locations of computers no longer in use, but relevant to the facts of the case
- Operating system and application software currently in use
- Operating system and application software no longer in use, but relevant to the facts of the case
- Name and version of network operating system currently in use
- Names and versions of network operating systems no longer in use, but relevant to the facts of the case
- File-naming and location-saving conventions
- Disk or tape labeling conventions
- Backup and archival disk or tape inventories or schedules
- Most likely locations of records relevant to the subject matter of the action
- Backup rotation schedules and archiving procedures, including any backup programs in use at any relevant time
- Electronic records management policies and procedures
- Corporate policies regarding employee use of company computers and data
- Identities of all current and former personnel who had access to network administration, backup, archiving, or other system operations during any relevant time

C. Do counsel anticipate the need to notice any depositions or propound any interrogatories to obtain further information about the opposing party's computer systems or electronic records management procedures?

D. Have counsel explored with their clients (in appropriate situations) the procedures and costs involved to:

- Locate and isolate relevant files from e-mail, word processing, and other collections
- Recover relevant files generated on outdated or dormant computer systems (so-called "legacy data")
- Recover deleted relevant files from hard drives, backup media, and other sources

E. Do counsel anticipate the need to conduct an on-site inspection of the opposing party's computer system?

- Consideration of an agreed-upon protocol
- Permission to use outside experts
- Agreement on neutral expert

IV. Electronic Document Production

A. Will counsel use computerized litigation support databases to organize and store documents and other discovery material?

B. Have counsel considered common formats for all electronic document exchange, e.g., TIFF images with OCR-generated text, e-mail in ASCII format, etc.?

C. Have counsel (particularly in multi-party cases) considered a central electronic document repository?

D. Have counsel considered an attorney-client privilege non-waiver agreement, to avoid the costs associated with intensive privilege screening before production?

E. Do counsel anticipate requesting data in non-routine format, e.g.,

- Printing by respondent of electronic documents not normally in print form
- Creation by respondent of customized database reports
- Performance by respondent of customized searches or data mining

F. Have counsel agreed upon cost allocation outside the usual rule that parties absorb their own disclosure costs, e.g.,

- Requesting parties will pay non-routine data retrieval and production costs
- Parties will negotiate data recovery and legacy data restoration costs

G. Does either party anticipate objecting to the production of computer records or software necessary to manipulate the records based on:

- Trade secret
- Licensing restrictions
- Copyright restrictions
- Statutory or regulatory privacy restrictions

V. Testifying Experts

A. Will any testifying expert(s) rely on computer data provided by either party, or rely on his or her own data?

B. Will any testifying expert(s) use custom, proprietary, or publicly-available software to process data, generate a report, or make a presentation?

C. Do counsel anticipate requesting discovery of either the underlying data or the software used by any testifying expert?

VI. Anticipating Evidentiary Disputes

Have counsel considered discovery procedures designed to reduce or eliminate questions of authenticity, e.g.,

- Computer discovery supervised by neutral party
- Neutral, secure electronic document repository
- Exchange of read-only disks or CD-ROMs
- Chain-of-custody certifications