

Best Practices in E-Discovery

These “Best Practices”, some of which are extracted from the Sedona Conference’s white papers on the Best Practices in Electronic Discovery and Best Practices in Electronic Record Management, are divided into 4 categories: **Preventive Measures, General Guidelines in E-discovery Practice, Crucial Considerations before Addressing the Harvesting of a Client’s Data and Critical Considerations for the Proponent of Discovery.**

Pre-discovery or “preventive” measures:

1. An organization should have reasonable written policies and procedures for managing its information and records, memorialized in formal protocols in data retention and e-mail use and retention policies (especially in light of the coming amendment to Federal Rule 37, establishing a “Safe Harbor” against claims of spoliation.)
2. An organization adopting an information and records management policy should consider including procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.
3. An organization’s policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or threatened litigation, governmental investigation or audit (or “Litigation and Regulatory Holds.”)

General guidelines in conducting E-discovery:

1. Parties to litigation should confer early in discovery regarding the preservation and production of electronic evidence.
2. Discovery requests should make as clear as possible what electronic data and documents are being asked for and responses to demands should disclose the scope and limits of what is being produced.
3. A responding party fulfills its good faith obligation to preserve and produce potentially responsive electronic data by using electronic tools and processes, such as data sampling and data “mining”

[Additional resources](#)
on Electronic
Discovery

Contact
[Paul Neale](#)



for consultation
on your next
case.

[e-News
Archive](#)



or the use of selection criteria, to identify the data most likely to contain responsive information.

4. The obligation to preserve electronic data requires good faith efforts to retain information that may be relevant to pending or threatened litigation. These preservation efforts may include (amongst other activities):
 - Notification to affected custodians of data;
 - Temporary suspension of electronic record and email retention policies;
 - Temporary suspension of system backup policies;
 - Temporary suspension of email auto-delete mechanisms;
 - Temporary suspension of desktop PC recycling protocols;
 - The imaging of hard drives;
 - Temporary suspension of system upgrades and the associated migration of data.
 - Memorializing preservation policy in written "Preservation Protocols".

Crucial steps to take before addressing the harvesting of electronic evidence from a client's data stores:

1. Identify and interview the crucial information officers and system administrators on aspects of the creation and management of electronic data.
2. Determine the electronic information actually generated by client (i.e.: determine the types of electronic data - e-mail, spreadsheets, Word documents, databases, etc. – that comprise the data stores of client.)
3. Conduct an inventory of the client's computer network infrastructure.
4. "Flowchart" electronic information to determine the manner in which information flows from and to different custodians.
5. Analyze the flowcharts to determine, if feasible, who are the custodians most likely to have relevant information and for whom various priorities should be assigned.
6. Identify how and where electronic information is stored (i.e.: is data mostly located internally upon local and wide-area networks; what is the type and volume of "distributed data" in existence - data on portable or removable media; does the organization outsource the storage of its data to third-party

storage vendors: do custodians routinely download important information to their own personal laptops, PDA's, home desktop PCs, etc.)

7. Identify how data is backed up for disaster recovery purposes and how it is catalogued and where backup media can be found.
8. Determine what logs are maintained of system activity.
9. Memorialize the electronic process and strategy in formal written "Electronic Discovery Protocols".
10. Hire an expert when deemed appropriate.

Crucial steps in conducting Electronic Discovery as a Proponent of E-discovery:

1. Send a "Preservation of Evidence Letter" to the respondent.
2. In written discovery include definitions, instructions and specific questions targeting issues relevant to electronic discovery.
3. Conduct a Rule 30 (b) (6) deposition of knowledgeable IT staff from the party-respondent's organization.
4. Focus upon backup media and collect those backup tapes potentially relevant to the action.
5. Collect relevant "distributed data" located upon removable or portable storage media.
6. Inquire of every witness concerning computer usage within the organization.
7. Make image copies of targeted hard drives.
8. Make image copies of targeted hard drives.
9. Write protect and virus check all storage media.
10. Maintain and meticulously preserve chain of custody documentation.
11. Hire an expert when deemed appropriate.

[Go to top](#)

This document is provided for informational purposes only. The information contained in this document is provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and freedom from infringement. The user assumes the entire risk as to the accuracy and the use of this document.

(c)2005 DOAR Litigation Consulting - All Rights Reserved.
170 Earle Avenue, Lynbrook, NY 11563

□