E-Discovery Toolkit

Disclaimer

The following e-discovery topics and samples are provided for informational purposes only and are not to be construed as legal advice. The e-discovery topics provided are issues for institutions to consider when e-discovery requests might involve university data; however the topics are neither all-inclusive or exhaustive, nor is every topic applicable to every college or university. Samples contained in this document should be seen as a starting point for discussion and may need to be modified as appropriate for the intended use. **For the foregoing reasons, we highly recommend that any intended use of the topics and samples be reviewed by appropriate general counsel at your institution.** If you have questions or comments regarding this toolkit, please contact the Higher Education Information Security Council.

Related Resources

- Electronic Records Management Toolkit
- Records Retention and Disposition Toolkit

Laws and Rules Driving E-Discovery

The Federal Rules of Civil Procedure (FRCP) govern the evidence discovery process for litigation in Federal and U.S. District Courts. Prior to December 2006, the FRCP included no specific provisions dealing with electronically stored information (ESI), which led to ad hoc and inconsistent decisions being made with regard to ESI discovery. Through the actions of the Advisory Committee on Civil Rules, amendments to the FRCP that specifically dealt with ESI were enacted. Many state evidentiary rules apply to the production of electronic information as part of the discovery process in state courts Provisions of particular interest in the FRCP are highlighted below. (*Source: Adler, M. Peter, "Federal E-Discovery Rules – Hindrance or Opportunity?" EDUCAUSE Live! webinar, January 9, 2007*)

1) Electronic discovery and the means of handling ESI discovery issues must be addressed very early in the progress of the case. Included may be such issues as sources of relevant ESI, burden and cost of retrieving and preserving it, the form in which it must be provided, and access privileges. (FRCP Rules 16, 26, and 34)

2) ESI that imposes an undue burden or cost to make it accessible need not be provided initially, but may later need to be produced, as determined on a case-by-case basis. Examples of ESI data that might not be reasonably accessible include, but not limited to:

- Information backups created for disaster recovery.
- Legacy information from technically obsolete systems.
- Remnants of deleted information that would require the aid of forensic specialists to recover.
- Databases designed to produce information only in ways not useful to the case.

See the Sedona Conference for guidelines.

3) The presumption is that the responding party will bear the cost of producing the requested ESI; however, the court may decide otherwise.

4) The duty to preserve relevant ESI may precede formal proceedings. This duty includes the requirement to suspend information destruction policies and procedures affecting the relevant ESI. As stated in FRCP Rule 37(f), however, "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." It is important to note that similar provisions may exist for state courts as well.

Resource: The Federal Rules of Civil Procedure (FRCP)

When Does the E-Discovery "Clock" Start?

The duty to preserve relevant ESI may commence upon:

- Initiation of a lawsuit by or against the institution;
- Institution is put on notice by a party that litigation is or may be imminent or;
- Institution has knowledge of facts that indicate litigation is reasonably anticipated.

What is Subject to E-Discovery

Electronically Stored Information (ESI)---All electronically stored information and data subject to possession, control, or custody of an institution regardless of its format and the media on which it is stored. ESI includes, but is not limited to: electronic files; communications, including e-mail and instant messages sent or received, and voicemail; data produced by calendaring software; and information management software. In addition to specific data that are electronically stored and readily retrievable, ESI includes data that may not be visible that is generated by computer hard-drive, e-mail and instant messaging, information management software, handheld computer devices (ex: Blackberry), telecommunications devices, and back-up storage devices. ESI may be stored on different electronic devices and removable devices (ex: internal and external drives, PDAs, smart phones, servers, laptops, backup tapes, thumb drives, CDs, DVDs) and may also reside at different locations (e.g., on the home or work systems, institutionally-owned or personal systems, in departmental files, etc.).

1) Data Files

- Active
- Archived

- Backups
- Legacy
- Internet (Web)

2) System Files

- Audit trails
- Access control lists
- Metadata
- Logs
- Internet "Footprints"
    - Cookies
    - Internet History
    - Browser Activity

3) Electronic Communications

- E-mail
- Instant messages

Sources may include:

1) Hardware Devices (*Samples*)

- Servers
- Desktops
- Laptops
- Personal Digital Assistants (PDA)
- Mobile Phone
- USB Drives
- Network appliances
- Storage area Networks (SANS)
- Backup Media (e.g., CD, tape)
- Internal and external disk drives
- MP3 / IPOD players

2) Software Applications (*Samples*)

- ERP systems
- CRM Systems
- Financial / Accounting Systems
- Student Information Systems
- e-Learning Management Systems
- Software application code
- E-mail systems / service
- Voicemail systems
- Instant messaging system / service
- Calendaring systems
- Network activity monitoring systems
- Third-party systems? (e.g., ISP, outsourcer, etc)
- Archiving / Records Management systems (e.g., Filenet)
- Collaboration systems
- Database various
- Spreadsheets

Locations may include:

- Work devices, applications, and departments.
- Home devices and applications.
- Third-party devices and applications. It is critical to understand what institutional data is held by third parties and the terms of the contracts and other arrangements that govern access to such data should it ever be required as part of a Litigation Hold Notice.

It is very important that ESI is preserved in its original electronic form so that all information contained within it, whether visible or not, is also available for inspection.

Source: Victor, Ira, "The E-Discovery Tidal Wave: Plan Ahead or Drown", 2009 Government Technology Conference

Roles and Responsibilities of Personnel Involved in E-Discovery May Include

Legal Counsel

- Determine if circumstances indicate the need for a Litigation Hold Notice.
- Determine the scope of the Hold to be issued.
- Issue a Litigation Hold Notice.
    - Identify the IT and records management personnel and others who can assist in protecting and preserving ESI and other relevant information.
    - Identify the specific individuals (end users) whom may have responsive ESI.
    - Identify the categories of information that are to be preserved.

    - Utilize an ESI questionnaire or discovery survey to facilitate the location of ESI.
- Identify the scope and collection method of the ESI.
- Review collected ESI to determine if responsive and or subject to evidentiary privileges.
- Identify and segregate confidential information.
- Monitor the Hold.
- Release the Hold.

End Users Who Receive a Litigation Hold Notice

- Review the Hold, and acknowledge the receipt.
- Comply with any instructions accompanying the Hold.
- Preserve current status.
    - Suspend all personal practices regarding the destruction of ESI related to the Hold (e.g., deletion of e-mails, voice mail, drafts of documents, accessing a document that may be altered by opening it, etc.).
    - If possible, disable all known automated functions that affect cache internet/temp folder creation (e.g., automatic deletion of e-mails or other ESI) if not possible contact IT to disable these functions.
    - Contact legal counsel when needing access to a document or file containing ESI that may be relevant to the Hold.
- Complete any questionnaires included with the Litigation Hold Notice and return as instructed.
- Identify location of all potentially responsive information.
- Collect and preserve information if possible to do so without changing the nature of the information, otherwise seek IT assistance in doing so.
- Provide relevant computers/devices (including personally-owned computers and mobile devices).
- Request assistance as needed.
- Follow records retention policy upon removal of the Hold.

IT Employee Who Receives a Litigation Hold Notice

- Review Litigation Hold Notice and determine need for immediate action, including need to disable automated functions that delete or alter ESI.
- Consult with legal counsel to identify the scope of data that must be preserved, the identification methods, collection processes, and searches.
- Collect the data as specified.
- Assist with litigation support if determined necessary by legal counsel.
- Follow records retention policy upon removal of the Hold.

Records Manager Who Receives a Litigation Hold Notice

- Review Litigation Hold Notices and take action as needed.
- Monitor Holds prior to approving record transfer/destruction.
- Follow records retention policy upon removal of the Hold.

Best Practices to Consider Prior to a Litigation Hold Notice (i.e., what to do to prevent an e-discovery request from becoming an all consuming monster)

Given the need to directly discuss issues of existence, accessibility, and form up front, institutions must know where and how electronic information is stored and the cost of production prior to start of litigation. Bad organization, poor records retention practices, or an ad-hoc response to e-discovery requests is no longer an excuse. (Schaufendel, May 2007)

Failure to respond or to respond in a timely manner to an e-discovery request can result in adverse inference jury instruction (i.e., a judge instructing the jury to assume that the missing evidence would have been adverse to the party that failed to produce it) and/or fines and penalties.

Institutions should consider the following best practices to mitigate the risk of having significant unplanned business interruptions and costly diversion of staff and technology resources by an e-discovery request:

1) Set up an E-Discovery Team. The Team should assess institutional readiness, provide support during litigation, and apply lessons learned to update processes, policies and procedures as needed. The Team should include members from legal counsel, compliance, records management, IT, key business areas, and risk management.
2) Inventory institutional information assets (i.e., what does the institution have), their nature (i.e., how are they stored and format), and their location (i.e., where is it located) specifically for confidential information. Include back-ups, convenience copies, etc.
3) Identify and define institution roles and responsibilities for information owners and custodians.
4) Define a clear and sound records retention/management policy and procedures for paper and digital information and communicate it to all employees.

- What constitutes a record.
- How should records be archived.
- How should records be de-duplicated to ensure only one authoritative copy.
- What document metadata should be preserved.

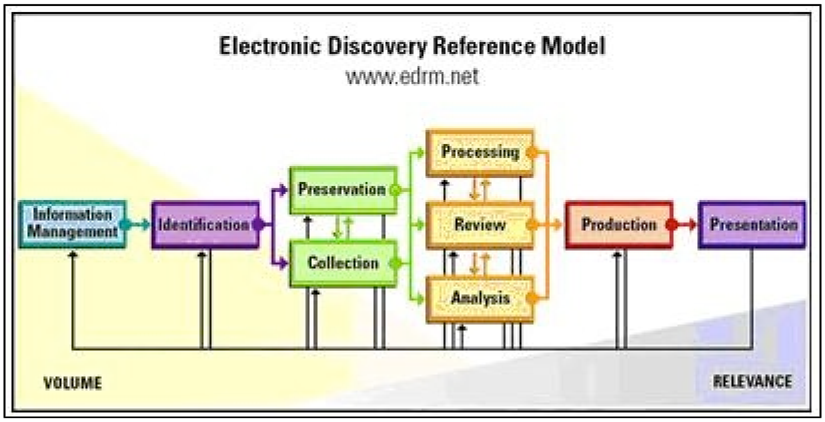
5) Ensure that the records retention/management policy and procedures cover the entire information life-cycle from creation to destruction and that the procedures are repeatable.
6) Audit the records retention/management policy to ensure appropriate enforcement.
7) Define and implement a process for handling and coordination e-discovery requests. Just like a disaster recovery plan, the process should include roles, corresponding tasks, and communication channels.
8) Define and implement a process and procedures regarding the manner IT department shall handle e-discovery requests and retaining information in response to a litigation hold notice.
9) Provide IT staff with appropriate training in e-discovery searching and/or retain a third-party service provider to perform the e-discovery searching.
10) Use appropriate technology to automate or support compliance with the records retention/management policy.
11) Review periodically ESI archiving technologies to ensure that they can recover potentially required ESI, in addition to their backup and disaster recovery capabilities.

In implementing the best practices listed above, institutions should be aware of four common misunderstandings regarding e-discovery: (Henry, March 2008)

- **Saving all information indefinitely is the best way to manage risk.** Over-saving information (potential over-disclosure) can be as risky as not saving enough information.
- **Believing that centralization of all data will help finding it.** Knowing what information an institution has and knowing where it is located (Best Practice #2) is a more effective long-term approach.
- **Most e-discovery problems are related to e-mail.** E-mail is often an important piece of evidence in a lawsuit but it is only one of many types of ESI that might need to be preserved
- **ESI preserved to fulfill an e-discovery request must always be "forensically" extracted and preserved.** The standard for retrieving and preserving ESI will depend on the applicable discovery rules, the nature of the case and other factors. However, institutions do need to demonstrate that the methodology used to collect and store the information is trustworthy. Prudence and documentation are always key.

E-Discovery Models

1) The Electronic Discovery Reference Model (EDRM)
EDRM is a widely-referenced guideline for managing the e-discovery process, which was developed through the efforts of over 125 organizations. First launched in May 2006, the goal of the EDRM is to facilitate the transfer of ESI between discovery steps. Participants have continued enhancing the model since 2006 and have created a content rich website. In brief, the EDRM divides the e-discovery process into the six major stages depicted in the diagram and descriptions that follow.



Stage 1: Information Management--Getting your electronic house in order to mitigate risk and expenses should electronic discovery become an issue, from initial creation of electronically stored information through its final disposition.

Stage 2: Identification--Locating potential sources of ESI and determining its scope, breadth and depth.

Stage 3: Preservation--Ensuring that ESI is protected against inappropriate alteration or destruction.

- ***Collection***--Gathering ESI for further use in the electronic discovery process (processing, review, etc.).

Stage 4: Processing--Reducing the volume of ESI and converting it, if necessary, to forms more suitable for review and analysis.

- ***Review***--Evaluating ESI for relevance and privilege.
- ***Analysis***--Evaluating ESI for content and context, including key patterns, topics, people and discussion.

Stage 5: Production--Delivering ESI to others in appropriate forms and using appropriate delivery mechanisms.

Stage 6: Presentation--Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native and near-native forms.

The process model is conceptual, not prescriptive, i.e., not all stages are necessarily needed in all cases and the order in which they are undertaken may vary depending upon the nature of any given case. It is also an iterative model. Stages are repeated as needed to adjust and refine ESI collected. As one proceeds through the process, the volume of ESI should decrease as its relevance increases.

An overarching step not explicitly included in the model is the meticulous documentation of data collection methodology – how data was preserved (Preservation step) and collected (Collection step) – and process. Data produced during an e-discovery request may not make it to court for several months and, possibly, even years. Accurate recollection of how the institution fulfilled the request and the steps taken to produce it, and the capability to explain it or repeat it, will be essential. (*Tower-Pierce, March 2008*)

2) Sedona Conference "Commentary on Legal Holds: The Trigger & The Process"

The "Commentary on Legal Holds: The Trigger & The Process" paper provides the general guidelines below, along with helpful illustrations for fulfilling the duty of collecting and preserving information relevant to anticipated litigation.

Triggering the Duty of Preservation

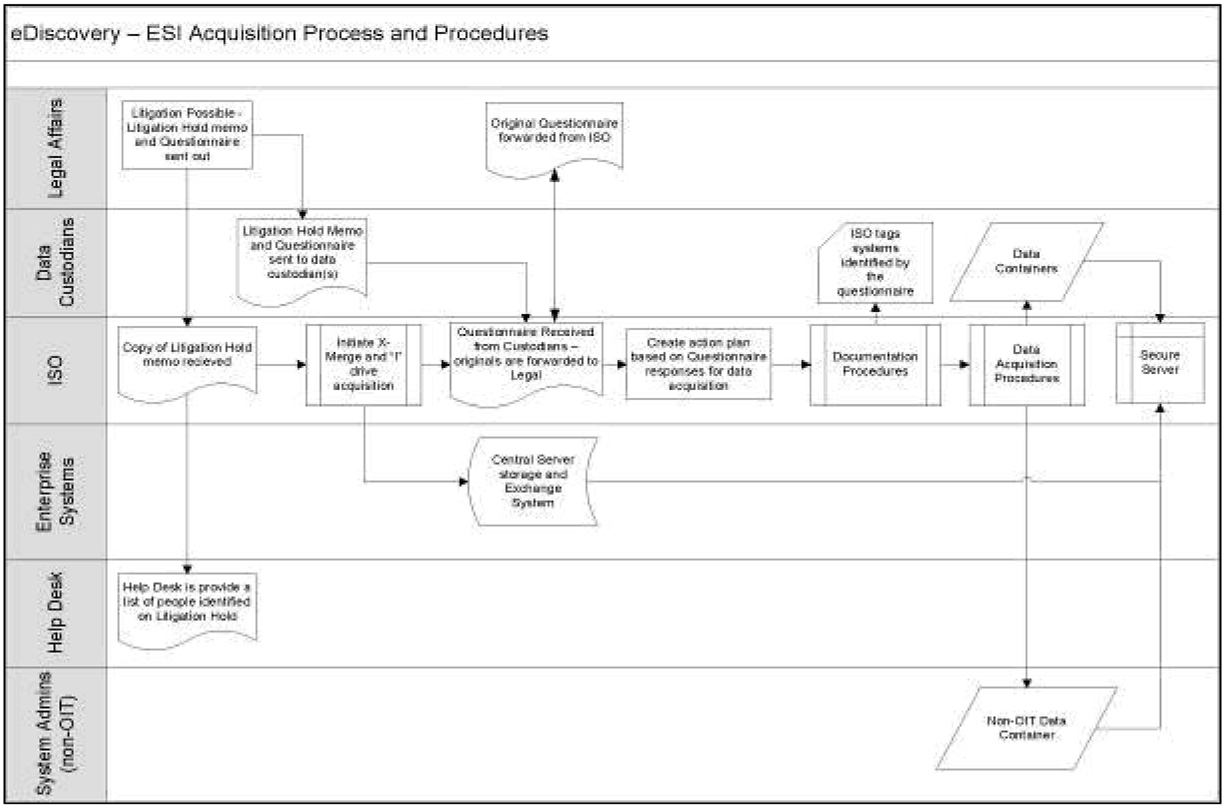
- Reasonable anticipation of litigation arises when an organization is on notice of a credible threat it will become involved in litigation or anticipates taking action to initiate litigation.
- The adoption and consistent implementation of a policy defining a document retention decision-making process is one factor that demonstrates reasonableness and good faith in meeting preservation obligations.

- The use of established procedures for the reporting of information relating to a potential threat of litigation to a responsible decision maker is a factor that demonstrates reasonableness and good faith in meeting preservation obligations.
- The determination of whether litigation is reasonably anticipated should be based on good faith, reasonableness, a reasonable investigation and an evaluation of the relevant facts and circumstances.
- Judicial evaluation of a legal hold decision should be based on the good faith and reasonableness of the decision (including whether a legal hold is necessary and how the legal hold should be executed) at the time it was made.

Implementing the Legal Hold

- When a duty to preserve arises, reasonable steps should be taken to identify and preserve relevant information as soon as is practicable. Depending on the circumstances, a written legal hold (including a reservation notice to persons likely to have relevant information) should be issued.
- In determining the scope of information that should be preserved, the nature of the issues raised in the matter, experience in similar circumstances and the amount in controversy are factors that may be considered.
- A legal hold is most effective when it:
    - Identifies the persons who are likely to have relevant information and communicates a preservation notice to those persons;
    - Communicates the preservation notice in a manner that ensures the recipients will receive actual, comprehensible and effective notice of the requirement to preserve information;
    - Is in written form;
    - Clearly defines what information is to be preserved and how the preservation is to be undertaken;
    - Is periodically reviewed and, when necessary, reissued in either its original or an amended form.
- The legal hold policy and process of implementing the legal hold in a specific case should be documented considering that both the policy and the process may be subject to scrutiny by the opposing party and review by the court.
- The implementation of a legal hold should be regularly monitored to ensure compliance.
- The legal hold process should include provisions for the release of the hold upon the termination of the matter at issue.

3) Models Used in Institutions of Higher Education


eDiscovery – ESI Acquisition Process and Procedures
Legal Affairs
Data Custodians
ISO
Enterprise Systems
Help Desk
System Admins (non-OIT)
Litigation Possible - Litigation Hold memo and Questionnaire sent out
Original Questionnaire forwarded from ISO
Litigation Hold Memo and Questionnaire sent to data custodian(s)
ISO tags systems identified by the questionnaire
Data Containers
Copy of Litigation Hold memo recieved
Initiate X-Merge and "I" drive acquisition
Questionnaire Received from Custodians – originals are forwarded to Legal
Create action plan based on Questionnaire responses for data acquisition
Documentation Procedures
Data Acquisition Procedures
Secure Server
Central Server storage and Exchange System
Help Desk is provide a list of people identified on Litigation Hold
Non-OIT Data Container

Graphic Revised February 3, 2009. Information Security Office – University of Texas at San Antonio. (ISO: Information Security Officer; OIT: Office of Information Technology)

Issues Associated with E-Discovery and Potential Gaps

- **E-mail** – E-mails are often overlooked in record management policies and may be retained long after they serve any useful purpose. Multiple copies of the same email may exist throughout a university's records system. The need to treat email as a potential source of official institutional records is only recently gaining attention within higher education. Educating management and staff on this requirement and providing technology and guidance for managing qualifying email records can be huge undertakings requiring several years to complete. System backups and log files – Operating system and database backups, as well as a wide-range of event log files, often contain information that could be subject to e-discovery. Decisions on the creation and retention schedules for these files are likely to have been driven solely on technical considerations, such disaster recovery, performance tracking, problem analysis, auditing, etc., and made on a system by system basis. Determining what backup and log files exist at any given time could be a daunting process.
- **Research Data** – While there may be exceptions, ESI containing research data and/or intellectual property would be handled the same as any other data subject to e-discovery. Of consideration:

    - Research sponsored by the Department of Defense.
    - Review contracts associated with sponsored research for terms related to court disclosure.
    - The discovery process allows for the negotiation of court orders that stipulate in detail how the data will be protected from inappropriate disclosure.
- **Metadata** – A discovery order may require the production of metadata associated with the ESI. Metadata may be altered by accessing a file as part of a search for responsive ESI.
- **Other Media and Formats** – Information subject to e-discovery can be on various media (CDs, DVDs, USB drives, magnetic tapes, etc.) in various file formats. Some media and formats could be technologically out of date, but still retrievable with significant effort.
- **Distributed Computing Environments** – While there are exceptions, few institutions operate completely centralized, locked down computing environments that allow electronic information to be easily located and retrieved. In institutions with distributed computing environments, IT staff in multiple organizational units will most likely need to be involved in any given e-discovery case. Coordination of data collection efforts can obviously be far more challenging and time-consuming in such environments
- **What determines scope? What levels vs. Everything** – Everything that is potentially relevant to the legal claim that triggered the e-discovery request should be preserved. The scope of "everything" is determined on a case-by-case basis by the institution's legal counsel.
- **Is there such a thing as an Unreasonable Request?** – "Unreasonable" is subject to interpretation. Initially the producing party makes the call on what is reasonably accessible and FRCP Rules 16, 26, and 34 provide a procedure for challenging a claim that information is not reasonably accessible. The producing party must show undue burden or cost.
- **Institutional Cost. Who pays? IT? Legal? Affected Department?** – Though it is understood that the responding party (the responding institution) will bear the cost of an e-discovery request, from an institutional perspective, whose budget is directly impacted. Example: a reasonable request needs compliance. University A will bear the cost of producing the information. For XYZ reason, to comply with request the institution needs to purchase one server and 3 TB of additional storage. Out of whose budget is the cost of this hardware is coming out? Central IT's budget? Legal Counsel's budget?
- **Reliance on Discovery Surveys**

Is Outsourcing an Option?

Institutions of higher education that do not have the storage, technology, and/or human resources to adequately respond to an e-discovery request may decide to utilize third-party service providers for assistance in retrieving, storing, sorting, and/or reviewing information. Also, third-party service providers may be able to assist with cost estimates in cases when arguing that information is not reasonably accessible is needed.

The downside of outsourcing is that e-discovery services are not cheap and it may be difficult for institutions of higher education to determine if particular services are effective or necessary and/or to justify the cost associated with these services.

Resource: Best Practices For The Selection Of E-Discovery Vendors

Lessons Learned (the hard way)

- Qualcomm Inc. v. Broadcom Corp. – Lesson: Benefits of adequate planning
- Flagg v. City of Detroit – Lesson: Data held by third-party service providers
- State v. Voorhies – Lesson: Perils of overlooking Instant Messaging (IM)
- Nursing Home Pension Fund v. Oracle Corp. – Need to preserve confidentiality and integrity
- Many Others...

Other Resources

- EDUCAUSE Resource Page: E-Discovery
- Electronic Discovery Law
- Electronic Discovery Resources
- National Center for State Courts (NCSC) Resource Guide
- Managing Discovery of Electronic Information: A Pocket Guide for Judges
- Lexis/Nexis Electronic Discovery Wiki

#Top of page

? Questions or comments? ℹ Contact us.