Litigation Response Planning and Policies for E-Discovery

Save to myBoK

With the enactment of the Federal Rules of Civil Procedure (FRCP), the legal discovery process in healthcare is beginning a radical transformation. The rules governing the discovery of electronic information and the legal process will vary by court jurisdiction (federal, state, or local) as well as the nature, size, and type of case under litigation (civil, criminal, or class action). To prepare for these new changes, healthcare organizations must revisit how they manage information stored electronically.

To successfully manage e-discovery, health organizations must develop a well-defined structure and process to understand, manage, and prepare for litigation. Legal counsel and HIM and IT professionals should work together to successfully manage the electronic discovery (e-discovery) process, implement a litigation response plan, and develop or update organizational policies.

This practice brief outlines five key steps in developing a litigation response plan and process. It uses the FRCP as the foundation for its recommendations.

HIM and IT professionals should seek the opinion of their organization's legal counsel in the final development, review, and approval of the e-discovery plan, policies, and procedures.

How to Develop a Litigation Response Plan

1. Conduct an Evaluation of Applicable Rules

Legal counsel plays a crucial role in e-discovery preparation. As a first step, organizational legal counsel conducts a thorough evaluation of all e-discovery rules applicable at the federal, state, and local levels.

Following this evaluation, legal counsel should educate the governing board, senior and middle management, and other departments with whom it works closely (e.g., risk management, compliance, HIM, and IT) about these rules and regulations and how they expect they will be applied to the organization.

Within the organization, the actual process by which the discovery of electronic information will occur will depend on the jurisdiction of the court and the type and complexity of the case to be litigated. The process may also depend on the scope and complexity of the organization's business and state of operations.

2. Identify a Litigation Response Team

Fundamental to the management and administration of e-discovery is a group of interdisciplinary professionals who serve as the organization's litigation response team. This team is responsible for implementation and ongoing review of the e-discovery process.

The litigation response team should conduct an assessment of the organization's current practices against the e-discovery rules that are applicable to the organization and jurisdiction.

It should then implement new policy and procedures necessary to successfully manage the e-discovery process. This step includes discussion and analysis of e-discovery issues and development of organizational resources such as enterprise retention and destruction schedules and IT system diagrams.

The litigation response team should also oversee the identification, preservation, search, retrieval, and production of responsive electronic and other potentially relevant information related to pending and current litigation. It should provide input to legal counsel about the forms, formats, methods, status, costs, location, and burden of production of potentially responsive information. The team should also oversee the ongoing review, monitoring, and evaluation of e-discovery processes within the organization.

Litigation Response Team Roles

The litigation response team should be comprised, at a minimum, of individuals from the legal counsel or risk management, HIM, and IT departments. Depending on its type, structure, and complexity, the organization may choose to appoint other members to the team, which may include, but are not limited to:

- Chief medical information officer
- Compliance officer
- Executive management (chief operating officer, chief information officer)
- Executive nursing management (vice president of nursing)
- Financial officer
- Other designated department or business process area managers (business office, radiology, laboratory/pathology, emergency services, or other designated management)

Their roles are outlined in the following descriptions.

The governing board should maintain ultimate responsibility for the oversight of e-discovery within the organization. It should also approve the organization's operational plan for e-discovery if appropriate.

The CEO or his or her designee should work closely with legal counsel or risk management in the ongoing review of e-discovery litigation. The status of e-discovery litigation should be reported to the governing board on a regular basis. The litigation response team and planning process should be supported by an executive sponsor.

Depending on the size and structure of the organization, legal counsel and risk management may operate as a single department or separately. Legal counsel may be involved in one or a number of "meet and confer conferences" with opposing counsel and the court early in the litigation process. Because of this, legal counsel must play an integral role in oversight of the e-discovery process while working collaboratively with IT and HIM to ensure relevant information is identified, preserved, and produced in the face of pending litigation.

The IT department should provide the technical support for the organization's hardware and software systems. The IT department will be a valuable resource for legal counsel. The IT department can assist in describing to a court how the organization's technical systems are structured, maintained, and operate. IT should also be able to detail how data are accessed, stored, retrieved, and destroyed.

The IT department can play an integral role in development of the organization's information management plan and its ongoing maintenance and update. It should work closely with the HIM department to understand and articulate the organization's records management requirements.

The HIM department should provide authoritative and technical knowledge about the management of both paper and electronic health information within the organization. The HIM department traditionally has been recognized as the official custodian of the patient's medical records. Because of this, in most organizations, the HIM department accepts and processes subpoenas for patient medical records. HIM should work closely with legal counsel in the identification, preservation, and production of all information (electronic and paper) relevant to litigation.

The HIM director should be knowledgeable about the flow, forms, formats, and location of information and records maintained by the organization, including maintenance and management of the retention and destruction schedules. The HIM department should work closely with IT and be involved in the development of the organization's information management plan and its ongoing maintenance and update.

Depending on the structure of the organization, management from ancillary departments may support the IT and HIM departments in ensuring relevant information is identified, preserved, and retained in the face of pending litigation. The organization should establish the role of ancillary department management in an e-discovery team and organizational response to e-discovery requests for information. Each ancillary department should develop its own specific policies to describe the methods by which entries are made into the medical record and organizational process for ensuring the quality and integrity of the data.

The organization must also define the role of the medical staff in an e-discovery team and organizational response to an e-discovery request for information. Many healthcare organizations designate a member of its medical staff or an individual with extensive clinical background to function as the chief medical information officer. This person can be a valuable

resource to legal counsel in understanding the applications and functionality of the organization's information systems and the impact they have in the delivery of a patient's care. Medical staff rules, regulations, and bylaws should specify the practices for documentation in the medical record.

Depending on the structure and complexity of the organization, the compliance officer may or may not be designated as an active member of the organization's e-discovery team. Regardless of structure, the potential involvement of compliance in e-discovery cannot be overlooked. The compliance office should work closely with the litigation response team to ensure adherence with e-discovery organization policies and procedures.

Depending on the structure of the organization, the nursing office may support the IT and HIM departments in ensuring relevant information is identified, preserved, and retained in the face of pending litigation. The role of the nursing office on the e-discovery team and organizational response to an e-discovery request for information should be established by the organization. The nursing office should also develop its own specific policies that describe the methods by which nursing personnel make entries into the medical record and organizational process for ensuring the quality and integrity of the data.

E-discovery is the pretrial legal process used to describe the method by which parties will obtain and review electronically stored information. Amendments to the Federal Rules of Civil Procedure in December 2006 place electronically stored information on equal footing with paper documents in the court.

Electronic data of any kind can serve as evidence. This may cover data or devices including, but not limited to, text, images, voice, databases, spreadsheets, legacy systems, tape, PDAs, instant messages, e-mail, calendar files, and Web sites.

3. Analyze Issues, Risks, and Challenges

Prior to developing organizational policies and procedures, the litigation response team must analyze the new issues, risks, and challenges resulting from e-discovery. This analysis will shape policy and procedure. It will also identify gaps in organizational resources.

The topics below highlight the emerging challenges. Direct questions are provided for the litigation response team to use as discussion starters.

Characteristics of electronically stored information (ESI). ESI is information created, manipulated, communicated, stored, and best used in digital form. It requires the use of computer hardware and software. Organizations should distinguish ESI from conventional media such as paper documents, photographs, microfilm, and analog recordings in their e-discovery processes. The volume of ESI is significantly greater than that of paper documents.

Questions to answer:

- Where is ESI located within the organization?
- What will be the standard procedures and method(s) by which the organization will identify and disclose relevant ESI?

Preparing for a meet and confer pretrial conference. A judge, magistrate, or special master will oversee the e-discovery litigation between parties. Prior to trial, the parties' legal counsel will meet and confer with the judge, magistrate, or special master to discuss and agree upon matters and the approach to be taken with regard to the discovery of electronic information.

The meet and confer sessions could be conducted in one session or several. The actual number of sessions will depend on a multitude of factors affecting the case, including size, scope, and complexity of the case as well as the knowledge, education, and experience of the judge, magistrate, special master, and attorneys involved in the e-discovery litigation.

Given the expansive amounts of electronic information that exists within information systems today, e-discovery can be an intricate, time-consuming, and costly undertaking. Therefore, before an e-discovery meet and confer conference takes place, it is important that legal counsel is educated and knowledgeable about the organization's information systems and records management policies.

Questions to answer:

- In response to a request for ESI, how will the organization locate, index, cull, search, classify, and produce all potentially responsive information?
- What benefit (if any) would there be to an enterprise content and records management system?
- How will the organization determine its true costs to index, classify, store, cull, search, retrieve, and produce ESI?
- If asked, how would the organization describe the "good faith operation" of its information management systems?
- Is there a resource that identifies all information operating systems that are in existence within the organization, including the type, nature, and location of all information systems, as well as the voice, back-up, legacy, and orphan systems?
- Have all record custodians been identified?
- What are the organizational policies and procedure related to records storage, management, and destruction?
- Does counsel have a current copy of the organization's information management plan?
- Does counsel have a current copy of the organization's information technology operating procedures?

Four Levels of Custodianship

Electronically stored information presents organizations with four levels of record custodianship. These depend on a person or entity's relationship to the data and data system and proximity to the case in litigation. As in traditional paper-based records, HIM should remain the official custodian of the record.

Level 1: Primary or Direct Custodians. Those persons who work with the data directly or have direct involvement or knowledge of the events of the case. For example, a staff nurse who has made an entry into the medical record and is knowledgeable about the events of a case in litigation. Primary custodians may be deposed or required to testify because of their direct involvement or knowledge of the case.

Level 2: Data Owners or Stewards. Individuals with responsibility to oversee business process areas may be designated as the data owners or stewards. They have knowledge of the procedures used to create, manage, and preserve specific types of records. Examples of business process areas include finance, radiology, lab, risk management, compliance, and nursing.

Level 3: Business Associates and Third Parties. Contractors and others who serve a variety of functions associated with a party's information but who are not parties to the litigation. Examples include Internet service providers, application service providers such as a claims clearinghouse, and other providers who provide services ranging from off-site data storage to complete outsourcing of the IT department.

Level 4: Official Record and System Custodians. The HIM department historically has been the designated official custodian of the overall medical record. The HIM department has played an important role in the processing of subpoenas for the organization, whether or not the organization was named in litigation.

Definition of official custodian of the record. In the traditional, paper-based realm of healthcare discovery, designation of the "official custodian" of the medical record was clear. In most healthcare organizations the HIM department served in this capacity. The mechanics of the traditional paper-based discovery process have been tied closely with the identification of the official custodian of the medical record.

In today's ESI realm, the role of official custodian is not nearly as clear. The loss of a clear designation will generate issues with the retention, preservation, and production of electronically stored information.
ESI presents four basic levels of custodianship, described in the sidebar above.

In today's new realm of electronic discovery, the HIM department should be designated to maintain the administrative and technical knowledge about how ESI is managed and used within the organization. It should remain the official custodian of the record. The HIM department should be responsible for content and compliance responsibilities associated with the

management of electronic information. It should be knowledgeable about the forms, format, and location of potentially responsive ESI.

Staff within the IT department may serve as the official custodian of the information system. Examples of this include the computers, servers, back-up and legacy systems, communications and voice systems, and near-line media. The IT staff who serve in this capacity will play an essential role in the discovery of ESI.

These personnel run the technical infrastructure of the organization's information management systems on a day-to-day basis. They understand the overall relationships between the different files, structure, and storage mechanisms of the organizations' information management systems. Generally, IT staff aren't experts on the specific content or the related managed policies; instead they understand how the organization's systems operate on a technical level.

Questions for discussion:

- How will the organization define and delineate "official custodianship" of its health and business records?
- Have data owners and stewards and the records they manage been identified?
- How will the organization communicate to its data owners and stewards and business associates a potential need to identify, preserve, and produce potentially responsive information for e-discovery litigation?

Preservation and legal holds. The organization has a legal duty to preserve all potentially responsive information in the face of threatened or impending litigation. The scope of that duty encompasses all potential evidence related to those identifiable facts and may shift as litigation develops.

Questions for discussion:

- Has the organization completed a comprehensive retention and destruction schedule that identifies all enterprise records (both paper and electronic) as well as the data owners?
- What potential "triggers" will initiate a potential litigation investigation and possible legal hold?
- Who within the organization will be responsible for establishing a litigation hold?
- How will all potential evidence be assimilated, indexed, and produced?
- Who will monitor the legal hold and reissue or lift it as pertinent facts change over time?
- At what point in the process should legal counsel negotiate a stipulated plan for the preservation of data to make sure the opposing side understands its obligations and to limit its own potential liability?
- Will the organization need special technology to index, classify, store, cull, search, retrieve, and produce ESI?

Form(s) of production. In traditional paper-based discovery, the physical form of production occurs generally only through paper. Documents were entered into evidence by one of the following ways:

1. Admission under the Business Records Rule (Federal Rule of Evidence 803(6) ([Medical Records])

2. Authenticated and admitted under the Best Evidence Rules (Federal Rules of Evidence 1001 and 1001[3])

3. Authenticated, Bates stamped (sequentially numbered or date and time marked), indexed, and labeled to correspond to the categories of a document request

The FRCP provide that legal counsel meet and confer early in litigation and agree upon the form(s) and manner of production of ESI.

Questions for discussion:

- At what point in litigation involving production of ESI will legal counsel meet with HIM and IT to discuss the forms, format, and location of all potentially responsive information?
- How will legal counsel, HIM, and IT work together to identify the most cost-efficient and effective means to produce potentially responsive information?

Reasonably accessible information versus not reasonably accessible information. The FRCP contain provisions for two-tiered discovery. The management of ESI provides for some unique challenges not presented by paper-based and other traditional media. All ESI must be rendered usable through technology—computer, operating system, or application software.

ESI that is readily available through appropriate technology and able to be used and read is considered "accessible." Much of the electronic information subject to discovery is not easily rendered usable without appropriate technologies. This usually involves significant cost and burden. This type of ESI is considered "not reasonably accessible."

Questions for discussion:

- How will the organization produce ESI from the EHR system that is accessible to a plaintiff party if required?
- How will the organization account for and determine its true costs to search, cull, and produce data that are "reasonably accessible" versus data that are "not reasonably accessible."

Cost shifting. In traditional paper-based document discovery an organization's costs were generally associated with locating responsive documents, assembling them into proper order, Bates stamping them, and presenting them to the requesting party for inspection and copying. With e-discovery the costs to cull, search, retrieve, and produce ESI can be very expensive and will depend greatly on the location, form, accessibility, and format of the information.

The FRCP contain provisions to balance ESI discovery costs between the parties. If a party shows good cause, the court can order the search, retrieval, or testing and sampling of inaccessible information. An organization without appropriate technologies or methods to index, classify, store, cull, search, retrieve, and produce potentially responsive information could face escalating costs, burdens, and potentially sanctions.

Questions for discussion:

- How will the organization determine its true costs to index, classify, store, cull, search, retrieve, and produce ESI?
- How will the organization respond to third-party subpoenas for ESI?
- What measures will the organization take to determine the burden and cost of production of third-party ESI?

E-mail management. The effects resulting from the mismanagement of company e-mail relevant to litigation can have a negative impact on the organization. Through the persistent efforts of legal counsel, coupled with court opinion and enactment of the FRCP, e-mail has become a proverbial "cache to the cash" for a savvy litigant.

Questions for discussion:

- What systems and processes are in place for the classification, management, storage, and retention of company e-mail?
- What is the organization's policy with regard to the use and transmission of protected health information in company e-mail?
- What are the organization's current policies and practices with regard to the screening and monitoring of company e-mail?
- How will e-mail be searched, indexed, reviewed, retained, and produced if relevant to litigation?

The litigation response team must also analyze issues, risks, and challenges surrounding nonapparent and ancillary ESI.

The role, use, and retention of metadata and ephemeral data. Operating system and application software require that electronic files be labeled so that the information can be stored, retrieved, viewed, and communicated. This process creates bits of information about the data known as metadata.

Metadata can be a useful way to authenticate the integrity of data. Recent court opinion suggests that short-lived data (such as RAM) are potentially discoverable and should be preserved if the information does not exist in any other form or cannot be obtained through any other means or source. The potential for the discovery of ephemeral data could pose a significant burden upon the organization.

Questions for discussion:

- How will the organization identify, store, retain, and manage its metadata when required for e-discovery?
- Under what possible circumstances (if any) could the organization be ordered to preserve and produce ephemeral data for a legal proceeding?
- What are the locations, sources, and types of ephemeral data that exist within the organization?

Legacy data systems. In certain cases, the retrieval or restoration of ESI that is contained on legacy systems may be warranted. Access could solely depend on the availability of a retired operating system and application software. ESI that is

not migrated and inaccessible places significant burden on the organization when that ESI is needed for business or legal purposes.

Questions for discussion:

- What provisions will the organization establish to provide for the efficient and effective migration of legacy data?
- How long will legacy data not needed for business and legal purposes be retained?
- What will be the mechanism for destruction of legacy data?

Back-up media. One of the biggest problems facing organizations today is the common practice of replicating ESI wholesale, in mirror image, as a precaution against data loss in the event of a disaster. While mirror image back-up tapes may be good procedure for the short-term, the long-term implications of retaining them may be detrimental in litigation. It is important to remember that routine maintenance of back-up tapes makes information on the tape potentially discoverable. The organization could be ordered to search and restore its back-up tapes for a legal proceeding.

Questions for discussion:

- What is and should be organizational practice with regard to the disposition and processing of its back-up tapes and other media?
- Have retention and destruction schedules been established for back-up media?

Screening ESI for privilege. One of the greatest costs associated with the discovery of ESI is the potential waiver of privilege that could result from the inadvertent production of privileged material. The tremendous costs to screen ESI for privilege must be borne by the organization. In a healthcare organization, counsel will need to take added measure to ensure that no unauthorized protected health information is inadvertently produced to a requesting party.

Question for discussion:

- What will be the organization's policy and procedure with regard to screening for privilege?

Preparing for E-Discovery

E-discovery is a complex process that will require a multidisciplinary approach to successfully implement and manage. Developing a litigation response team, a plan, and policies are critical steps in the process. Healthcare organizations should complete the following 10 activities to prepare for e-discovery.

1. Establish a litigation response team with a designee from the legal, HIM, and IT departments

2. Review, revise, or develop an organizational information management plan and provide legal counsel with any and all previous plans developed by the organization

3. Identify the data owners or stewards within the organization

4. Review, revise, or develop an enterprise records retention schedule

5. Conduct thorough assessment of the locations, forms, and business and legal use for all legacy systems, back-up media, and orphaned data in existence

6. Review, revise, or develop organizational policies related to e-discovery

7. Review, revise, or develop organizational policy on e-mail management

8. Develop established approach and methodology to determine burdens and costs of producting electronically stored information

9. Identify designated person(s) responsible for establishing a legal hold within the organization and establish a process for communication and review of existing holds

10. Establish an organizational program to educate and train all management and staff on e-discovery compliance

AHIMA has a variety of resources on e-discovery available in the FORE Library: HIM Body of Knowledge at www.ahima.org. The September 2006 practice brief "The New Electronic Discovery Rule" provides a summary of key components of the FRCP and the impact on HIM and IT.

4. Develop Organizational Policy and Procedures

The next step in litigation response planning is development or updating of the organizational policies and procedures related to e-discovery. Organizations should have the following policy and procedures in place.

Preparation for a pretrial conference. This policy outlines the steps to complete prior to legal counsel attending a pretrial conference. The goal of this policy is to ensure that the organization adequately prepares for the pretrial conference, has researched key issues that will be addressed with the judge and plaintiff attorney during the conference, and understands what it is agreeing to in the discovery plan and the impact on pretrial activities.
(Sample policy)

Preservation and legal hold for health records and information. This policy outlines the process for preserving paper and electronic health records and related information when there is a reasonable anticipation of litigation. The policy guards against spoliation of evidence.
(Sample policy)

Retention, storage, and destruction of paper and electronic health information and records. This policy establishes the conditions and time periods for which paper-based and electronic health records will be stored, retained, and destroyed after they are no longer active for patient care or business purposes and to ensure appropriate availability of inactive records.
(Sample policy)

An enterprise record retention and destruction schedule should accompany this policy to provide a complete and accurate accounting of all relevant records within the organization.

Production and disclosure of electronic health information and records. This policy outlines the steps in the disclosure process for electronic and information records related to a legal proceeding. Many of these procedures would be managed through the release of information process within an HIM department.
(Sample policy)

5. Develop a System for Ongoing Monitoring and Evaluation

The response team's responsibilities extend to evaluating the efficacy of the organization's policies and procedures after implementation. This includes developing and regularly reviewing staff orientation and annual training materials and creating an ongoing audit and monitoring process.

Audit and monitoring activites can include audits of business process areas to determine compliance with e-discovery policies, as well as random audits of human resource files to verify staff training on e-discovery. The litigation response team should work with the compliance office to establish triggers and monitors to assess adherence to e-discovery policies throughout the organization.

References

AHIMA e-HIM Work Group on e-Discovery. "New Electronic Discovery Civil Rule." *Journal of AHIMA* 77, no. 8 (Sept. 2006): 68A–H.

Allman, T. "Ruling Offers Lessons for Counsel on Electronic Discovery Abuse." *Washington Legal Foundation* 19 (October 2004).

Allman, T. "Fostering a Compliance Culture: The Role of the Sedona Guidelines." *The Information Management Journal* (March/April 2005): 54–61.

Baldwin-Stried, Kimberly. “E-Discovery and HIM: How Amendments to the Federal Rules of Civil Procedure Will Affect HIM Professionals.” *Journal of AHIMA* 77, no. 9 (Oct. 2006): 58–60.

Dimick, Chris. “E-Discovery: Preparing for the Coming Rise in Electronic Discovery Requests.” *Journal of AHIMA* 78, no. 5 (May 2007): 24–29.

Jurevic, A. “When Technology and Health Care Collide: Issues with Electronic Medical Records and Electronic Mail.” University of Missouri Kansas City Law Review, Health Law Symposium, 1998.

Logan, D., J. Bace, and M. Gilbert. “Understanding E-Discovery Technology.” Gartner Research (ID Number: G00133224), 2005.

Marchand, L. “Discovery of Electronic Medical Records.” American Trial Lawyers Association Annual Convention Reference Materials, 2001.

Patzakis, J. “How the New Federal Rules Will Likely Change E-Discovery Practice.” *The Metropolitan Corporate Counsel* 38 (June 2006).

Patzakis, J., and B. Murphy. “The New Federal E-Discovery Rules and Their Impact.” Guidance Software audio seminar, June 2006.

Pooley, J., and D. Shaw. “Finding Out What’s There: Technical and Legal Aspects of Discovery.” *Texas Intellectual Property Law Journal* 4 (Fall 1995).

Solomon, S. “The Ever-Increasing Legal Challenge of Change Precipitated by Technology, Compliance and Law.” Paper presented at the 15th National Conference on Managing Electronic Records, May 2007, Chicago, IL.
US Courts. “Summary of the Report of the Judicial Conference Committee in Rules of Practice and Procedure.” September 2005. Available online at www.uscourts.gov/rules.

Prepared by

AHIMA e-Discovery Task Force:

Kim Baldwin-Stried Reich, MBA, MJ, RHIA, CHC, CPHQ
Deborah Beezley, RHIT
Michelle Dougherty, RHIA, CHP
Sandra Nunn, MA, RHIA, CHP
Lydia Washington, MS, RHIA, CPHIMS

Acknowledgments

Katherine Ball, MD
Jill Callahan Dennis, JD, RHIA
Neil Puller, MBA, MD

Article citation:
AHIMA e-Discovery Task Force. "Litigation Response Planning and Policies for E-Discovery." *Journal of AHIMA* 79, no.2 (February 2008): 69-75