CNA
We can show you more.®

CAREFULLY SPEAKING®

CS 2015 ISSUE 2

Electronic Record Requests: Meeting the Challenge of E-discovery

E-discovery in the pre-trial phase of litigation refers to the request for and disclosure of electronically stored information (ESI) in order to establish basic facts about the case. E-discovery requests often extend beyond resident care records to include email messages, voicemail recordings, databases, digital images, telephone logs and other archived material. In the context of litigation, e-discovery involves more than the rephrasing of discovery requests to include electronic records and data: It also redefines the nature of legally relevant documentation, thereby necessitating a thorough review of information management policies, especially in such areas as record retention, HIPAA compliance and data security.

E-discovery is especially challenging in aging services-related litigation, due to the volume of records that can accumulate during a typical multi-year resident stay. Failure to properly manage discovery requests involving ESI can lead to unnecessary and expensive evidentiary conflicts, potentially undermining an organization's defense posture. Faulty procedures also may result in unintentional disclosure of protected resident information, with serious legal consequences. Finally, deletion of ESI can result in charges of spoliation of evidence, potentially subjecting organizations to sanctions, adverse jury instructions and high damage awards.

For these reasons and others, administrators and legal counsel must develop and implement a coordinated e-discovery response process that complies with legal requirements and reflects the organization's data storage infrastructure. This edition of *CareFully Speaking*® focuses on the key risk control areas of identifying discoverable ESI, updating electronic information-handling procedures and enhancing response to discovery requests, while protecting resident confidentiality and organizational interests. The strategies offered within this resource are general in nature. As state laws vary significantly regarding e-discovery, leaders should consult with an attorney knowledgeable about applicable statutes and regulations.

Would you like to read *CareFully Speaking*® online? Visit **www.cna.com/healthcare**, click on "Search CNA" in the top right-hand corner of the screen, type the article's full title in the search box and then click on the magnifying glass icon.

LITIGATION RESPONSE TEAM

Compliance with discovery requests often demands a concerted effort to compile and process a wide range of information in a variety of formats. E-discovery readiness therefore requires formation of a litigation response team, which should include legal counsel, a compliance officer, a risk and/or quality improvement manager, nursing and medical directors, and knowledgeable health information management (HIM) and information technology (IT) professionals. This task force should be made responsible for drafting, implementing and revising policies and procedures; monitoring retention schedules; and enhancing awareness of and compliance with data security and resident privacy requirements. For more information about litigation preparedness, see "E-Discovery Litigation and Regulatory Investigation Response Planning: Crucial Components of Your Organization's Information and Data Governance Processes," from the American Health Information Management Association (AHIMA).

The following sections are intended to aid litigation response teams in organizing their e-discovery compliance efforts. The various points are summarized in checklist form on pages 8-11.

In general, data are deemed part of the legal record if they relate to the provision of clinical care and would reasonably be expected to be released upon discovery request.

DISCOVERABLE DATA

The concept of a "legal health record" as defined by AHIMA has been adopted by many organizations. In general, data are deemed part of the legal record if they relate to the provision of clinical care and would reasonably be expected to be released upon discovery request. While there is no definitive answer at present as to exactly what types of electronic data are discoverable, the following material is likely to be deemed legally relevant:

- *Audio files* – i.e., recordings of dictation, shift-to-shift reports, resident telephone calls and other oral communications.
- *Clinical decision-support data* – i.e., alerts, reminders, pop-ups and similar tools within an electronic resident care record designed to aid in the clinical decision-making process.
- *Continuing care data* – i.e., records received from another healthcare provider involved in the resident's course of care.
- *Digital images* – i.e., radiographs and similar results of diagnostic procedures or telemedical consultations.
- *Messages* – i.e., email messages, voicemail recordings, mobile telephone texts and other one-to-one communications, if these are deemed directly relevant and possible to produce without undue burden or expense.
- *Metadata* – i.e., "hidden" data used to authenticate the integrity of electronic entries by revealing when they were made, accessed, reviewed and/or altered.
- *Mobile clinical data* – i.e., real-time resident care data, such as vital signs and medication status, captured via "smartphone" applications and transmitted to providers.
- *Personal health data* – i.e., any information created, owned and managed by the resident and provided to an aging services organization, such as medication tracking records and comprehensive history profiles.
- *System source data* – i.e., data from which interpretations, summaries and notes are derived following procedures, treatments and ancillary care, including complication and readmission rates.
- *Statistical data* – i.e., data found in large group files, which can be extracted using computer scanning software.

E-discovery requests may be broad, potentially encompassing databases that contain privileged risk management and quality improvement records. Therefore, written policy should address storage and disposition of certain types of information, which customarily are protected from disclosure based upon quality assurance, risk management, error analysis or peer review privilege. The following types of data are especially sensitive, requiring an *in camera* inspection by a judge prior to their release:

- *Demographic data about former residents* – i.e., names, birth dates, Social Security numbers and forwarding addresses of potential material witnesses.
- *Grievance logs* – i.e., lists of employee and resident complaints.
- *Incident reports* – i.e., documentation of internal investigations of adverse events.
- *Internal peer review evaluations* – i.e., performance-related records for physicians and other providers.
- *Notes from risk managers or nursing directors* – i.e., observations made during routine risk and quality management projects and/or investigations.
- *Personnel files* – i.e., performance evaluations, disciplinary records and other information associated with staff members.

When filing an e-discovery request, a plaintiff's attorney will consider all the processes and systems that converge to produce a legal health record, beyond the obvious components of a computerized or paper-based resident care record. Organizations should be prepared to document in diagram format all the sources of electronic data in their possession, including servers, proprietary data sources, network shares, cloud data, desktop and laptop computers, personal devices and removable media.

To learn more about the scope and breadth of e-discovery, see the list of e-discovery rules on page 7.

QUICK LINKS

From AHIMA:

- AHIMA e-Discovery Task Force. "AHIMA Model E-Discovery Policies: Preservation and Legal Hold for Health Information and Records." See also "AHIMA Model E-Discovery Policies: Production and Disclosure of Health Information and Records for E-Discovery" and "Litigation Response Planning and Policies for E-Discovery." *Journal of AHIMA*, February 2008, volume 79:2.
- "Avoid Legal Missteps with a Litigation Response Plan." *AHIMA Advantage, volume* 12:7, 2008.
- Dougherty, M. "How Legal Is Your EHR?: Identifying Key Functions That Support a Legal Record." *Journal of AHIMA*, February 2008, volume 79:2, pages 24-30.

Other sources:

- Harris, B. and Rashbaum, K. "Electronic Medical Information Preservation and Legal Holds: Why the Healthcare Industry Needs to Take Action," a Legal Hold Pro™ Signature Paper, March 2011.
- The Legal Health Record in the Age of e-Discovery, an audio-slide presentation by Backman, C. and Carter, J., April 2009. Available for purchase from the Healthcare Information and Management Systems Society eLearning Academy.

DUTY TO PRESERVE DATA

As a general rule, the duty to preserve data arises when an aging services organization is in receipt of a lawsuit or subpoena, or when it reasonably anticipates litigation. Common triggering events include:

- A demand letter from a lawyer.
- An accusation of discrimination, harassment or abuse by a resident or employee, or a complaint that a state or federal law has been violated.
- A meeting with a resident and/or family member accompanied by an attorney.
- A threat by a resident or relative to sue the organization.

If litigation is likely, the organization is duty-bound to preserve all data germane to the dispute. Determining the scope of preservation requires identifying who created the relevant data and where the data are stored. This often involves interviewing staff and providers, as well as analyzing the organization's IT infrastructure and reviewing data storage and retention policies.

INFORMATION RETENTION AND DESTRUCTION

It is impossible to predict exactly what types of information may be discoverable in litigation. Therefore, it is prudent to assume that all ESI may be vulnerable to e-discovery, and hence must be either retained or destroyed according to legally compliant written policy. Consult with legal counsel, as well as HIM and IT professionals, to ensure that data storage protocols address the following legal, technical and operational issues:

- *Statutory and/or regulatory obligations*, including conditions and time periods for enterprise-wide retention.
- *Accessibility of resident care e-documents* using current medical storage technology.
- *Clear labeling of e-files in operating systems and application software* to expedite storage, retrieval, viewing and sharing of information.
- *Identification and storage of metadata*, as defined on page 2.
- *Processing and disposing of "hidden" information*, such as old backup tapes, instant messages, voicemail recordings, word-processing drafts and shadow records (i.e., additional copies of primary database files).
- *Storage of inactive electronic resident care records* and other archived materials for easy retrieval.
- *Provisions for the reliable migration of legacy data* from retired operating systems and application software.
- *Contractual obligations for vendors, contractors and other third parties* regarding security, preservation and retrieval of organizational data.

Erasing discoverable data may lead to allegations of deliberate destruction of evidence. Fortunately, rule 37(e) of the amended *Federal Rules of Civil Procedure* (FRCP) and the many state statutes that mirror this rule provide a "safe harbor" for organizations that cannot produce requested ESI because it was deleted in good faith during the course of routine operations.

To avail itself of this safeguard, an aging services organization must demonstrate that it has:

- *Adopted a legally compliant records management policy* and consistently followed this policy.
- *Implemented industry best practices* concerning record management and data integrity.
- *Documented a chain of events for all e-record destruction*, recording the date of data deletion and the reasons behind it.

LITIGATION HOLDS

Whenever a court issues a hold on resident care-related records due to current or pending litigation, normal data disposition practices are suspended. If records integral to a lawsuit are destroyed after a record preservation order has been issued, the organization may be held liable for spoliation or intentional destruction of evidence, resulting in severe penalties. For this reason, some organizations secure all litigation-relevant data in a specially designated computer server.

In addition to responding to court-imposed holds, aging services administrators also should issue a written hold notice whenever they reasonably anticipate litigation, informing custodians of their duty to prevent the deletion or destruction of any potentially relevant information. Depending upon the case, a litigation hold notice also may include a questionnaire designed to help legal counsel elicit information about pertinent data sources from health IT professionals and risk managers.

The written policy on subpoena processing and litigation hold orders should specify:

- Actions or warning signs that trigger a legal hold.
- The individual responsible for the receipt and processing of legal hold subpoenas.
- The process for initiating a legal hold prior to a court order.
- Procedures for implementing and monitoring a legal hold.
- Special technology required to prevent loss or deletion of relevant electronic documents.
- Circumstances for lifting or re-issuing a legal hold.
- Criteria for retaining an e-discovery litigation consultant or software vendor to assist with searching, compiling, reviewing and/or analyzing data.

PRETRIAL CONFERENCES

E-discovery requests should trigger the same response protocol as traditional requests – i.e., validity check, attorney review, processing and production. However, due to the sometimes complex technical issues involved in electronic discovery, different questions and potential disputes may arise.

To enhance procedural efficiency, the federal rules suggest a pretrial conference, giving opposing parties the opportunity to arrive at a mutually acceptable agreement on data disclosure by discussing such issues as information accessibility, storage format, preservation and costs. Administrators should be prepared to answer the following routine inquiries, among others, from plaintiff's attorneys during the pretrial conference:

- Where do data reside for the applicable dates?
- Where are documents saved on the network?
- Where are backup data stored?
- Are archived data located on servers, networked hard drives or removable media?
- Where are relevant e-mail messages, texts and voicemail recordings stored?
- Can deleted files be recovered and produced?
- In what format(s) can the data be produced?

If records integral to a lawsuit are destroyed after a record preservation order has been issued, the organization may be held liable for spoliation or intentional destruction of evidence, resulting in severe penalties.

'REASONABLE ACCESSIBILITY'

When reviewing e-discovery requests, courts typically weigh the relevance of the data against the burden placed upon the defendant. If information is readily accessible using standard methods, it will probably be presumed discoverable. However, most e-discovery statutes exempt defendants from the obligation to produce electronic information that would require excessive cost or effort to recover.

In determining whether or not data are reasonably accessible, the court will consider the following questions, among others:

- Is the discovery request unreasonably cumulative or duplicative?
- Can the information be obtained in another way that is less difficult or costly?
- Are electronic data stored on-site or off-site?
- Do the data reside on a current server or accounting system, or on an obsolete legacy system?
- Have sufficient time and effort been expended in responding to the discovery request?
- Does the burden or expense of the proposed discovery outweigh the likely evidentiary benefit?
- Were the specified data deleted, and if so, was the deletion pursuant to a formal document retention/destruction policy?
- Do the data or the underlying tables in which they reside require rebuilding?

Responses to these questions should be carefully evaluated and documented by the organization.

The Sedona Conference® has published guidelines regarding the concept of "reasonable accessibility" of electronic records. The organization's Commentary on Preservation, Management and Identification of Sources of Information That Are Not Reasonably Accessible emphasizes the importance of cooperative efforts to settle disputes regarding accessibility of electronic sources.

Data are generally expected to be produced in a widely used storage format. Often, the requesting party specifies a desired format. The responding organization either accepts the suggestion or files an objection, explaining why the request would strain the organization's record management capabilities and suggesting an alternative format that would better serve the purpose.

CONFIDENTIALITY

Privacy is another potentially significant issue when producing electronic data. HIPAA, state-enacted privacy protections or attorney-client privilege may serve to pre-empt the amended federal rules. Relevant legal privileges should be asserted early on in the proceeding, in order to prevent possible privacy or security breaches.

To ensure compliance with HIPAA when producing electronic records, section 13405(c) of the Health Information Technology for Economic and Clinical Health (HITECH) Act requires an accounting of certain protected electronic health records. Also, the HIPAA Privacy Rule under the HITECH Act requires issuance of an "access report" whenever a resident's electronic protected health information is accessed, listing the names of those requesting records, as well as the dates and times of the requests.

To avoid a potential misstep, organizations should establish a protocol for identifying and exempting protected data from discovery. If protected information is inadvertently produced in the course of litigation, the rules provide for its return and/or destruction.

CNA is dedicated to improving the defense posture of aging services organizations. In addition to the risk management strategies contained within *CareFully Speaking*® and our other healthcare newsletters, CNA has compiled a risk management guide aimed at aging services providers. Practical Resources to Aid in Safeguarding Residents and Minimizing Risk, offers a wide range of guidelines, sample forms, checklists, and other assessment and quality enhancement tools.

DATA SECURITY AND BUSINESS CONTINUITY

Prevention of data loss or corruption is a critical element of electronic record management and e-discovery compliance. In the event of a disaster, security breach, system breakdown or other unexpected occurrence, an effective emergency and recovery plan can preserve the integrity of an information network, including potentially discoverable data. For a detailed discussion of business continuity planning, see CNA's Emergency Management Planning: Assessing Risk, Preparing for Recovery.

E-discovery presents a wide range of challenges for aging services organizations, which can only be met by careful planning and close collaboration among administrators, risk managers, information management staff and legal counsel. The strategies outlined herein are designed to assist leadership in reviewing and (if necessary) revising current e-discovery policies, thus enhancing the organization's ability to respond to electronic document requests in a systematic, timely and appropriate manner.

E-discovery Rules

The potential magnitude of e-discovery requests creates new demands on organizations with respect to electronic record management. In order to fulfill their responsibilities in this area, administrators, medical directors, senior management, HIM and IT personnel, and others involved with data management must remain apprised of evolving e-discovery rules and expectations.

The following documents serve as primary references concerning the scope and breadth of e-discovery, and should be consulted whenever questions arise:

- ***The Federal Rules of Civil Procedure (FRCP)** serve as a model for many e-discovery rules adopted at the state level. The federal rules recently underwent review, resulting in proposed changes that may significantly affect e-discovery and information governance practices. The proposed amendments emphasize the importance in discovery requests of cooperation, proportionality and reasonableness. These changes, which have been adopted by the United States Supreme Court and submitted to Congress for approval, are scheduled to take effect December 1, 2015.**
- **The National Conference of Commissioners on Uniform State Laws' *Rules Relating to Discovery of Electronically Stored Information*** *reflect the federal specifications and provide additional guidance for organizations.*

* These changes include amendments to Rules 1, 4, 16, 26, 30, 31, 33, 34, 37, 55 and 84, as well as the Appendix of Forms. The changes with the greatest potential impact on e-discovery are within Rule 1, which emphasizes the cooperation of adverse parties in discovery; Rule 26(b)(1), which has been amended to focus on limiting the scope of discovery; and Rule 37(e), which addresses sanctions for failure to preserve ESI.

Prevention of data loss or corruption is a critical element of electronic record management and e-discovery compliance.

e-Discovery: Planning and Compliance Checklist

COMPLIANCE MEASUREMENT	YES/NO	IS THIS INITIATIVE SUPPORTED BY A WRITTEN POLICY OR DEPARTMENTAL PROCEDURE? (IF SO, WHEN WAS IT APPROVED AND REVIEWED?)	COMMENTS/ REVISIONS/ ENHANCEMENTS NEEDED
TASK FORCE INITIATIVES			
1. *Have legal counsel and risk management conducted a joint evaluation of applicable e-discovery rules* at the federal, state and local levels?			
2. *Are regular discussions about e-discovery requirements and procedures held* with: ▪ Governing board members? ▪ Senior administrators? ▪ Nursing and medical directors? ▪ Leaders of health information management and information technology departments?			
3. *Has an e-discovery response team been convened*, and does it include representatives from: ▪ Legal counsel? ▪ Risk management? ▪ Nursing and medical staff leadership? ▪ Health information management? ▪ Information technology? ▪ Information security? ▪ Privacy compliance?			
4. *Has a comprehensive staff communication and education program been prepared* regarding e-discovery compliance requirements?			
5. *Does the organization formally define the components of the legal resident care record*, including both electronic and paper documents?			
6. *Has the e-discovery response team identified all sources of electronic data*, noted their location and indicated their relevance to the legal resident care record?			
7. *Is there a written, comprehensive definition of discoverable electronically stored information (ESI)*, which includes: ▪ Residents' health records? ▪ Metadata? ▪ Statistical data? ▪ Source systems data? ▪ Continuing care records? ▪ Clinical decision-support information? ▪ Personal health data? ▪ Email messages, voice-mail recordings, texts and instant messages? ▪ Server log entries? ▪ Audio files? ▪ Calendar notes? ▪ Digital images?			

COMPLIANCE MEASUREMENT	YES/NO	IS THIS INITIATIVE SUPPORTED BY A WRITTEN POLICY OR DEPARTMENTAL PROCEDURE? (IF SO, WHEN WAS IT APPROVED AND REVIEWED?)	COMMENTS/ REVISIONS/ ENHANCEMENTS NEEDED
POLICY REVIEW			
1. *Has the e-discovery team reviewed existing policies and procedures* pertaining to: ▪ Legal health record maintenance and disclosure? ▪ Electronic record management, retention and storage? ▪ Electronic record preservation during litigation?			
2. *Are written ESI policies regularly reviewed*, and do they ensure that: ▪ Protected information is not accidentally or intentionally modified or destroyed by employees? ▪ Requested data are reviewed prior to production, in order to ensure that privileged information is not disclosed? ▪ A custodian of the legal health record is appointed in all types of pending or current litigation? ▪ Applicable statutory and regulatory obligations are complied with, including conditions and periods for enterprise-wide retention and storage of records? ▪ Metadata and other system source data are clearly identified and securely stored? ▪ Legacy data from retired operating systems and application software are retained? ▪ Outside vendors and contractors understand their obligation to preserve and retrieve data relating to the legal health record?			
3. *Are policy revisions approved by executive leadership*, and are obsolete policies carefully archived?			
4. *Can revised policies be implemented using existing hardware and software*, or are technical upgrades necessary?			
5. *Have all policies and procedures concerning e-discovery practices been reviewed by legal counsel*, signed off by the governing board and published within the organization?			

COMPLIANCE MEASUREMENT	YES/NO	IS THIS INITIATIVE SUPPORTED BY A WRITTEN POLICY OR DEPARTMENTAL PROCEDURE? (IF SO, WHEN WAS IT APPROVED AND REVIEWED?)	COMMENTS/ REVISIONS/ ENHANCEMENTS NEEDED
ESI PRESERVATION			
1. *Has the organization named an official custodian of the legal health record* and defined the custodian's duties regarding data preservation?			
2. *Is there a formal mechanism for alerting the custodian and other data owners of potential litigation* and the consequent need to collect, organize and secure relevant records and other information?			
3. *Does the organization have a comprehensive record preservation policy* that specifies: ▪ Signs of potential litigation that trigger a legal hold? ▪ The individual responsible for receipt and processing of a legal hold subpoena? ▪ A process for establishing a voluntary legal hold prior to a court order? ▪ Approved methods for implementing, monitoring and documenting a legal hold? ▪ Technical requirements for instituting a legal hold? ▪ Circumstances for lifting or re-issuing a legal hold? ▪ Criteria for retaining an e-discovery litigation consultant and/or software vendor to assist with searching, gathering, reviewing and analyzing data?			
4. *Is there an enterprise record management committee* responsible for: ▪ Creating a record retention schedule? ▪ Acquiring, commissioning and/or updating software applications? ▪ Approving new electronic forms? ▪ Maintaining the electronic resident care record system? ▪ Tracking data migration throughout the network? ▪ Monitoring hardware and software performance? ▪ Accounting for damaged, inaccessible or lost records?			
5. *Does the organization have a formal business continuity plan* to minimize disruption of discovery response following an emergency or system outage?			
6. *Have steps been taken to protect against security breaches* and other threats to data integrity?			

COMPLIANCE MEASUREMENT	YES/NO	IS THIS INITIATIVE SUPPORTED BY A WRITTEN POLICY OR DEPARTMENTAL PROCEDURE? (IF SO, WHEN WAS IT APPROVED AND REVIEWED?)	COMMENTS/ REVISIONS/ ENHANCEMENTS NEEDED
E-DISCOVERY RESPONSE			
1. *Do health information management or information technology personnel assist defense counsel/risk management with e-discovery duties*, including the search, retrieval, preservation and production of responsive e-documents?			
2. *Is there a written subpoena response plan*, which addresses the need to: ▪ Identify the date of the subpoena? ▪ Assess the validity of the document (e.g., fees paid, court seal present, proper jurisdiction)? ▪ Determine if the requested information is relevant to the underlying case? ▪ Verify if requested information is under legal hold? ▪ Ascertain whether any confidentiality protections apply?			
3. *Is there a mechanism in place for estimating e-discovery expenses*, including the cost of producing electronically stored information in an acceptable format?			
4. *Is the organization prepared to object to unreasonable data production requests*, based upon such factors as relevance, technical obstacles and cost?			
5. *In the event of a pretrial conference, are guidelines in place* to help administrators: ▪ Provide defense counsel with a current copy of the organization's record management plan? ▪ Answer potential questions about the organization's information system and record management policies? ▪ Explain where the data reside or when and why they were deleted, using information flow diagrams? ▪ Describe the formats in which the requested data can reasonably be produced? ▪ Demonstrate the organization's good-faith efforts to comply with record retention guidelines?			
6. *Does the e-discovery team communicate regularly with defense counsel* concerning the status of the e-discovery response?			

CNA Risk Control Services

ONGOING SUPPORT FOR YOUR RISK MANAGEMENT PROGRAM

CNA School of Risk Control Excellence

This year-round series of courses, featuring information and insights about important risk-related issues, is available on a complimentary basis to our agents and policyholders. Classes are led by experienced CNA Risk Control consultants.

CNA Risk Control Web Site

Visit our Web site (**www.cna.com/riskcontrol**), which includes a monthly series of Exposure Guides on selected risk topics, as well as the schedule and course catalog of the CNA School of Risk Control Excellence. Also available for downloading are our Client Use Bulletins, which cover ergonomics, industrial hygiene, construction, medical professional liability and more. In addition, the site has links to industry Web sites offering news and information, online courses and training materials. When it comes to understanding the risks faced by healthcare providers … **we can show you more.®**

CNA

For more information, please call us at 888-600-4776 or visit www.cna.com/healthcare.