Preparing for Discovery

Save to myBoK

In the October print edition, Kimberly A. Baldwin-Stried Reich describes the differences between traditional subpoenas and e-discovery requests in "Sorting out Discovery Requests" (AHIMA member log-in required). Here she continues that discussion, elaborating on the differences between paper and electronic records from a discovery perspective, offering a sample subpoena form, and describing steps in responding to a discovery request.

She also presents a scenario that led to discovery and recommends that organizations prepare for the changing world of discovery by developing similar use cases. Scenarios such as this, she writes, help organizations identify the types of data and systems that may require legal holds in response to or anticipation of discovery, and they illustrate the ever-widening scope of information that is discoverable.

Prior to the enactment of the amendments to the Federal Rules of Civil Procedure, case law played a key role in laying the foundation for the discoverability of electronically stored information for admission as evidence into a court of law. In *Linnen v. A.H. Robins Co., Inc.,* 10 Mass.L.Rptr. 189 (Mass. Super. Ct. 1999) the court held that a "discovery request aimed at the production of records retained in some electronic form is no different in principle from a request for documents contained in any office file cabinet."

Even though *Linnen* established that "in principle" there is no difference between the requests, there are indeed vast differences between the production of paper documents and electronic documents in response to a request. The fundamental differences are described below:

Volume and reproducibility

- Digital data exist in substantially greater volumes than paper-based information
- Digital data require a device such as computer to be read
- HIPAA Standards for Transmission for protected health information apply to electronic information

Dynamic content and nature of electronic data

- Information is easier to change in electronic systems than on paper
- Content of electronic information can change without human intervention
- Transmission and transfer of digital data are not fixed in final form

Metadata

- Digital data contain metadata, such as time stamps and audit logs
- System, application, and/or user metadata are not readily apparent
- Metadata require a new set of retention and preservation obligations

Lifespan and Persistence of Data

- Electronic information is much harder to dispose of—paper can be shredded, but electronic data are not easily deleted

Environment

- Electronically stored health information may be incomprehensible when separated from its environment
- Relevant digital data may exist in legacy systems that have not have been migrated into the organization's current systems, making the availability and accessibility to such information difficult

- Paper-based health information that exists as a scanned image or microfiche document will be complete and more easily accessible than data directly entered and distributed among various systems

Search and Retrieval of Electronic Data

- Paper documents are typically consolidated and maintained in single file folder
- Digital data may reside in numerous locations
- Electronic environment may obscure origin, completeness, or accuracy of information if it lacks proper controls

The Sedona Conference has been discussing the differences between paper documents and electronically stored information since it was established in 1997. In March 2008 the group released a commentary about the admissibility and authentication of electronically stored information. This document provides an excellent evaluation as to how the federal courts have begun to address and evaluate the differences between paper and electronically stored information as evidence that is submitted into a court of law.

Some general considerations that legal counsel will bear in mind when drafting a request for production of digital information is whether or not metadata will be requested and whether or not the information to be produced must be in native form. With regard to EHR systems, legal counsel will have to bear in mind that today's evolving systems often are not capable of recreating information as it appeared at the time of an incident; producing screen shots or duplicating events will not be possible. Therefore system metadata data and audit logs often will be useful tools in helping legal counsel recreate and evaluate a sequence of events.

Given the complexity of the systems, and the court's unfamiliarity with the data they produce as evidence, HIM and IT managers must understand these systems well in order to testify about the "good faith" operations of their organizations' information management practices.

HIM and IT managers should maintain good working knowledge of the uses, location, and system functionality of the EHR as well as any health information exchange networks in which the organization participates.

Organizations should determine how their information systems provide for the preservation of information that may be relevant to litigation. They must establish policies that describe how staff communicate the need for preservation in the face of impending litigation.

Sample Subpoena

HIM professionals are familiar with discovery requests in the form of subpoenas. A subpoena duces tecum is a written order issued by the court commanding a person to "appear and bring" all documents, media, books, and other records outlined in the subpoena. The form of the subpoena will vary by state statute, but generally a subpoena is valid when it contains the following elements:

- Name and jurisdiction of the court
- Names of the plaintiff and defendant
- Case docket number
- Date, time, and place of request appearance
- Description of specific documents sought
- Name of attorney who caused the subpoena to be issued
- Signature stamp or official seal
- Appropriate witness
- Mileage fees

The linked sample subpoena, issued by a local court, illustrates the basic document.

Key Steps and Considerations Responding to Subpoenas

The key to the continued success of the HIM profession in responding to subpoenas and e-discovery requests is to recognize that the process is changing and evolving. As the legal profession becomes more knowledgeable and experienced in the production of electronic documents, the process will become more straightforward and efficient.

In the meantime, however, organizations can follow these key considerations and steps in reviewing their policies and procedures regarding the processing of subpoenas and e-discovery requests:

- Clearly establish which individuals or departments will be authorized to accept and process subpoenas on behalf of the organization.
- Establish a practice that ensures all subpoenas served upon the organization are immediately reviewed to confirm their validity.
- If determined to be valid, identify the nature and type of subpoena (i.e., state, local, or federal) and review with legal counsel the associated duties and requirements for responding to it.
- Determine what (if any) risk there may be to the organization. Determine whether the subpoena is a third-party subpoena or whether the organization or its providers are (or may be) named in the lawsuit. Immediately notify the risk management department if the organization is or may be named in the litigation.
- Review the subpoena to determine if it appears that the preservation and production of electronically stored information is going to be a significant factor in the case. If it is, immediately identify the appropriate data custodians, as well as identify the forms, locations, and accessibility of other potentially relevant data.
- Ensure the organization maintains a well documented plan for the management of information and adequately describes the "good faith" operations of all information systems in place within the organization.
- Develop an organizational policy that defines the content, components, and form of the legal medical record that is released for disclosure purposes.
- Discuss and evaluate whether or not the organizational policy will define the minimum set of metadata that will be preserved and produced in response to litigation.
- Ensure all staff within the organization are knowledgeable about organizational policies and procedures regarding the individuals or departments that have been designated to accept and process subpoenas on behalf of the organization.

Preparing for the Challenges and Changes

As the nation works to adopt EHR systems and establish health information exchange, the roles and responsibilities of HIM professionals are changing. One day virtually all of a person's individually identifiable health information will be captured and exchanged electronically. EHRs and HIEs will provide the framework for a nationwide exchange of health information.

Given the impact the 2006 Amendments to the Federal Rules of Civil Procedure has had in redefining what information is relevant to a matter and how it may be used in litigation, today a record can be defined as anything recorded in written or electronic form that provides permanent evidence of past events. Whatever form EHRs and HIE ultimately take, one measure is certain—the courts are here to stay and they will continue to produce preservation orders, subpoenas, and requests for production.

To prepare for the changes and legal challenges that lie ahead, organizations and HIM and IT professionals, possibly collaborating with risk management staff and legal counsel, would be wise to develop use case scenarios to identify the types of data that may be discoverable and how the organization will respond to a subpoena or e-discovery request for such information.

Planning through Scenarios

Consider the following scenario. What information should the hospital immediately preserve, and what other information pertaining to the event will be discoverable through e-discovery?

Susie Smith is a 48-year-old female who presents to the emergency room with complaints of shortness of breath, nausea, abdominal pain, and intermittent chest pain. According to hospital records, Ms. Smith signed into the E/R at 12:01 a.m., was registered at 12:08 a.m. and was seen by the triage nurse at 12:28 a.m.

The triage nurse records the patients vitals as, BP 178/120, Respirations 92, Pulse Ox 98% on Room Air. The triage nurse asks Ms. Smith to rate her abdominal pain, which the patient rates as “6 out of 10.” The patient is placed into an examination room at 12:45 a.m. with a working diagnosis of abdominal pain and is informed, “There is going to be a slight wait, the emergency room is very busy tonight.”

At 12:46 a.m., four teenage victims from an automobile accident are brought to the emergency room. At 12:47 a.m. Susie sends a message via Twitter to family and friends: “Made it to the E/R… OMG mjr car acc teens, blood & activity everywhere, hope I won’t have to wait too long, chest hurts again.”

At 12:55 a.m., one of the teenagers is placed into the examination room next to Susie. A pull curtain is the only privacy barrier in place to separate the parties. Susie looks into the room next to her and thinks she may recognize the young woman as a close friend of her daughter. She snaps a picture of the girl and sends it to her daughter, asking if it is her friend from school.

At 1:46 a.m., the emergency room doctor enters the room to examine Susie. The doctor asks her to rate her abdominal pain. Susie, who is now sweating profusely and writhing in pain, describes her pain as “a 9 out of 10.”

She requests pain killers. The emergency room doctor informs Susie that she wants to “watch her a bit” and prescribes IV fluids and anti-emetics at 1:58 a.m.

At 2:05 a.m., the nurse administers the IV fluids and IV anti-emetics prescribed by the emergency room doctor. The nurse informs Susie that the fluids and anti-emetics may “make her drowsy” and informs her that she will “check back in on her in about a half an hour.”

At 2:42 a.m., the nurse enters the room to check on Susie. The nurse documents, “Patient asleep.” No vitals are recorded by the nurse.

At 2:56 a.m. the emergency room doctor enters the room to re-check Susie and notices that Susie looks “pale and ashen.” She tends to the patient and does not note obvious vital signs. The emergency doctor tries arousing the patient, but Susie is asystolic and unresponsive. The emergency doctor calls a code and the code team work diligently to try and revive the patient.

Susie Smith is pronounced dead at 3:32 a.m. by the emergency room doctor. Susie’s death is unexplained. The coroner is notified and begins an investigation into the cause of death.

Assessing the Situation

What went wrong? Certainly, the triage nurse failed to note, assess, and document the patient’s complaint of “intermittent chest pain.” The patient was never placed on an EKG monitor, and the ER doctor acted solely on the assessment of the triage nurse.

The hospital does not know this, of course. However, in anticipation of the coroner’s investigation, it should immediately establish a hold on any and all records and relevant information regarding Susie Smith’s care and treatment. This includes preserving system metadata, such as the audit trail indicating the names, dates, and times of all persons who accessed the record.

What other information about the event would be discoverable? The coroner will likely obtain the Twitter message and the cell phone photo from the patient’s family and friends and will likely be the first person to inform the hospital of their existence.

The Twitter message may be the only source that documents the patient’s complaint of chest pain. The photo and message are not relevant to the investigation, but they will reveal a violation of the teenage patient’s privacy that could lead to separate action.

Similarly, the hospital’s audit logs could reveal privacy-related complications if they reveal unauthorized access from curious staff who snooped in the record after the event. Even if this revelation did not lead to a complaint or action from the patient’s family, the hospital must respond to these violations.

What other questions, issues, or possibilities does the scenario raise?

Original source:
Baldwin-Stried, Kimberly A.. "Preparing for Discovery" (Journal of AHIMA website), October 21, 2010.