physician connection

PSIC | Professional Solutions INSURANCE COMPANY

Protecting Reputations ... One Doctor at a Time®

PROFESSIONAL SOLUTIONS INSURANCE COMPANY BRINGS YOU PRACTICAL TIPS FOR AVOIDING A MALPRACTICE ALLEGATION ISSUE 2 • 2013

E-Communications Can Be E-Discovered

The last issue of *Physician Connection* included a discussion about the malpractice risks associated with e-communication. Closely related is the topic of e-discovery, which can have equally serious risk implications for your practice.

A practice that finds itself involved in litigation and unable to comply with e-discovery rules can jeopardize the defense of the case. The physicians and staff of the practice also will waste valuable time, effort and money trying to recover e-data in response to a subpoena for electronically stored information. What's more, if those attempts are unsuccessful, the physician faces court sanctions.

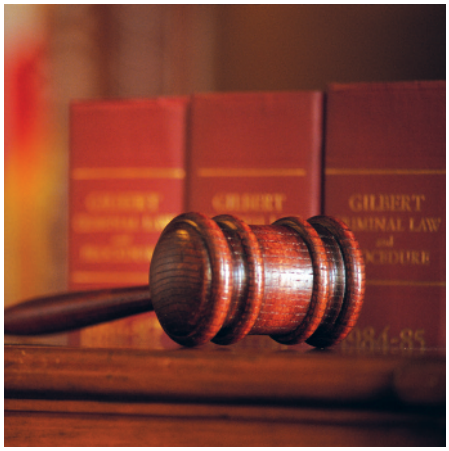
Yet many physicians are not aware of the e-discovery rule. And, unless the practice or its physicians have been defendants in a recent lawsuit, they probably have not thought about how e-discovery could affect their IT network or EHR systems.

Consider the following scenarios:

Scenario 1

An internist received notice of being named in a lawsuit alleging the inappropriate prescription of an antibiotic to a patient who had a known and documented allergy to that drug. At her deposition, the physician denied knowing about the allergy and claimed there was no allergy of the drug noted in the patient's medical history or the patient's electronic medical record.

On e-discovery, the plaintiff's expert was able to find metadata[1] in the patient's electronic record. This metadata confirmed the allergy information had existed in several places in the system



and had been deleted by the physician/defendant on the same day the practice received notice of the lawsuit.

In addition to losing her medical malpractice lawsuit, the physician was fined by the courts under the e-discovery rules. Not only was she cited for the destruction of electronically stored information with the intention of preventing e-discovery by the plaintiff, she was also sanctioned by her state medical board for unprofessional behavior.

Scenario 2

A medical assistant in a family practice group filed a sexual harassment claim against its business manager. She alleged the business manager made persistent, inappropriate sexual advances to her. What's more, the medical assistant contended that after she rejected these advances, the business manager threatened to fire her.

After she reported the business manager's behavior to the lead practice physician, the business manager reportedly professed his innocence. He claimed it was a case of "he said/she said," and her accusations were ridiculous and completely unfounded. The physician

INSIDE THIS ISSUE:

[1]Metadata describes other data. It provides information about a certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document.

Continued on Page 2

Continued from Page 1

told the medical assistant that she must have misinterpreted the situation, and the matter was essentially dropped as far as he was concerned.

The employee then hired an attorney to file an action against the business manager and the practice. When the lead physician received a subpoena for internal emails between the business manager and the medical assistant, he denied their existence other than an initial "new employee" email sent on the medical assistant's first day of employment. This email was turned over to the plaintiff's attorney.

Is everyone who uses the practice's EHR system aware that anything they document, review and delete will remain in the system?

That was not the end of things, as the employee had printed out every incriminating email the business manager had sent to her during office hours over a four-month period. It was later determined that, upon receiving notice of the claim, the business manager had accessed the practice's computer system and deleted all emails he had sent to her, as well as her responses.

It was further discovered that the business manager knew that merely deleting an email was not sufficient to prevent its recovery from the hard drive. He had contracted with the practice's IT consultant to "clean" the main hard drive.

In addition to losing the sexual harassment case, the business manager ***and the practice*** were hit with a significant monetary sanction for attempting to thwart the e-discovery of evidence.

How E-Discovery Began

In civil litigation, discovery is the fact-finding process undertaken before trial by the parties involved in the lawsuit. This includes bringing forth any necessary titles, documents or other items in the parties' possession necessary to the cause or action pending.[2]

The discovery process is regulated by federal Rules of Civil Procedure, which were expanded in 2006 to include requests for digitally or electronically stored information. Thus began the use of electronic discovery, or "e-discovery," for gathering evidence in a civil or criminal trial.

These rules were borne out of technological advances and societal changes in how individuals and businesses communicate and store information. The federal government also sought to reduce the high costs of collecting and reviewing paper documents in a lawsuit. Some experts believe that "following the paper trail" during litigation will go the way of watching a program on a VHS.

E-Discovery Impacts All Healthcare Providers

The changes to the Rules of Civil Procedure apply to any organization that might be involved in a lawsuit in which electronic data from any source might be used as evidence. In other words, all healthcare organizations and facilities—including physician practices—are directly affected.

Since 2006, a majority of states have enacted their own version of the e-discovery rule. Most of these are in keeping with the federal rules, but a few (e.g., Idaho, Mississippi, Oregon and Texas) have enacted their own models of e-discovery or have not addressed e-discovery at all.

Physicians should determine the e-discovery requirements in their own states and develop practice policies and procedures accordingly.

As the scenarios described earlier demonstrate, a practice must be prepared to comply with electronic data and e-PHI retention, security and destruction regulations/requirements. To get started, it can be helpful to consider the following questions:

- Could your practice easily comply with a subpoena for intra-office emails relating to a specific employee or patient?
- Could it comply with such a subpoena several years after the fact?
- Is everyone who uses the practice's EHR system aware that it keeps retrievable "metadata"? In other words, anything they document, review and/or delete will remain in the system, along with the exact date and time the actions were performed.
- Can the practice easily produce digitally stored radiographs or a specific electronic claim submitted to a third-party payer upon request?
- Can the practice produce these items and remain in compliance with HIPAA and HITECH privacy requirements regarding electronic PHI?

[2]The Law Dictionary: Featuring Black's Law Dictionary Free Online Legal Dictionary 2nd Ed. Accessed January 7, 2013: http://thelawdictionary.org/discovery/

The practice must also develop a retrieval procedure for the event of an e-discovery request. Ideally, the practice should proactively assess its existing systems, policies and procedures. It should ensure the practice is able to retrieve and produce electronic information on request in a timely and efficient manner.

To obtain the maximum benefit from the assessment usually requires involving several members of the practice team, including its business manager, legal counsel, IT consultants, in-house IT manager, medical record managers and billing personnel. By involving several people in this process, it is more likely the physician will identify the locations and formats of all practice e-data that may be subject to the e-discovery rules.

E-Discovery Readiness Recommendations

Here are some tips to help your practice become e-discovery ready:

- **Implement a record retention and storage policy** that's in compliance with existing regulatory and statutory requirements regarding record retention and release. Typically, a record retention and storage policy would include procedures and schedules for retention, retrieval and destruction of all practice records. The policy should identify what types of electronic records and data the practice should not release or that would require special consent to release, e.g., records containing protected information on HIV, AIDS or substance abuse. The practice's system can use "metadata" to tag or flag such e-records to help prevent their inadvertent or unauthorized release, as well as unauthorized or inadvertent record modification, loss, or destruction.
- **Develop specific policies and procedures for records that could be involved in litigation.** This includes protecting both electronic and hard-copy records from regularly scheduled retention, automatic off-site storage and destruction procedures until litigation resolves. Staff should know what to do if the practice receives a subpoena for records or an e-discovery request.
- **Implement a policy and procedure for email retention and archiving of information.** Include a system that facilitates accessibility and retrieval, if needed (e.g., an indexing system).
- **Develop policies and procedures to address the security, retention and accessibility** of other electronic devices and technologies used in the practice. These may include voicemail messages, text messages, e-prescribing, smart phones, tablets, laptops, websites and blogs. Be careful about the destruction or recycling of portable electronic devices and equipment that contain practice information.
- **Consider HIPAA Security requirements and put in place protections** to provide for record integrity and security of any electronic data received, transmitted or stored. These may include implementing a secure network, data encryption, data back-up and off-premise storage.
- **Educate staff about practice records policies and enforce compliance.** This includes business records, third-party payer claims and records, practice employment records, and patient health information. Hold staff in-service education programs to review the practice's policies and procedures and to provide updates. Make physicians and staff aware that anytime they access a patient's e-record, their actions will be tracked and documented—all of which is discoverable.
- **Stay alert for changes, modifications, and amendments to the e-discovery rules** that could require updating or modifying the practice's policies and procedures. Some aspects of e-discovery are currently vague, and

Staff should know what to do if the practice receives a subpoena for records or an e-discovery request.

Continued on Page 4

because technology is evolving rapidly, the rules will likely change. For example, existing record retention laws and regulations do not specifically address retention of e-information in emails, text messages or smart phones.

With today's changing technology, it is essential that your practice become e-discovery ready. Being knowledgeable about e-discovery will help you develop policies and procedures that will enable your practice to comply with these changing rules and regulations, while protecting your practice and patient information.

Resources

Federal Rules of Civil Procedure. E-Discovery Rules: Rules 16, 26, 33, 34, 37 and 45. The Cornell University Law School Legal Information Institute. www.law.cornell.edu/rules/frcp/

E-Discovery in Federal and State Courts after the 2006 Federal Amendments. Thomas Y. Allman (2012). www.ediscoverylaw.com/.../2012FedStateEDiscoveryRules(May3).pdf

The Sedona Principles: Helpful Guidelines for e-Records Management. The Sedona Principles, the Sedona Guidelines, and other useful e-discovery and e-records management publications are available free to the public. www.thesedonaconference.org

Scan to visit the risk management section of psicinsurance.com

Highlights of the Federal E-Discovery Rule

- **Establishes electronically stored information (ESI) as a separate class** of discoverable information.
- **Requires mandatory "meet-and-confer" sessions** to specifically address e-discovery issues that occur early in the discovery process—within 120 days of the filing of litigation and at least 21 days prior to the scheduling conference.
- **Addresses the format of production of ESI.** It permits the requesting party to designate the form desired for electronically stored information. The requesting party is not required to choose a form of production, and the rule provides a framework for resolving disputes over the form of production, if the responding party objects to the requested format.
- **Recognizes that some ESI may be "reasonably inaccessible"** because of undue burden or cost and clarifies the obligation to produce this information. If the requesting party can demonstrate good cause, the "reasonably inaccessible" information may later be determined to be discoverable and required to be made available by court order and under court supervision.
- **Establishes "claims of privilege" and "claw-back agreements"** in cases of inadvertent production of privileged ESI during initial discovery. After appropriate notification, the receiving party may not use or further disclose information deemed privileged or protected. Further, the receiving party must return, sequester or destroy this information. The producing party is then required to protect and preserve that information until the case is closed.
- **Establishes "safe harbors" that provide protection for organizations** that inadvertently destroy potentially discoverable records in the course of normal, "good faith" records management operations and "absent exceptional circumstances."

PSIC | Professional Solutions INSURANCE COMPANY

Send all inquiries, address changes and correspondence to:
Physician Connection, P.O. Box 9118, Des Moines, IA 50306
Toll-Free 1-888-336-2642
Internet – www.psicinsurance.com
Email – riskmanagement@psicinsurance.com