



## BUSINESS

# Is your EMR legal? A document can look like a medical record, but not meet the legal definition.

## System design and user error can contribute to vulnerabilities that increase your liability.

By [Pamela Lewis Dolan](#), AMNews staff. Oct. 13, 2008.

You might find your electronic medical record to be an efficient way to store patient data, but is that record legal? If it were subpoenaed, would it help you or hurt you in court?

These kinds of questions are emerging as more physicians go electronic. Federal Rules of Civil Procedure, approved by the U.S. Supreme Court in December 2006, not only make any electronically stored data discoverable in a trial, but also open up physicians to several new liabilities inherent in the detail electronic data provides.

- [Making it legal](#)
- [Before you buy](#)
- [See related content](#)
- Topic: [Electronic medical records](#)
- [E-mail](#) - [Print](#) - [Write a letter](#)

For example, if a nurse records information under your login and password, and that information is incorrect, you could be the one held liable. Or the record's metadata -- the time stamp of who entered what when -- can dispute a doctor's version of events.

While EMRs are touted as a way to make life easier for physicians, health IT and legal professionals say they can make life miserable for a doctor who buys the wrong system, or uses it in the wrong way.

"Where these issues can raise their heads is somewhat unpredictable," said Reed Gelzer, MD, co-founder of Advocates for Documentation Integrity and Compliance, an advocacy and consulting group that educates physicians and health care entities on the legal EMR.

## **CCHIT certification requires EMR amendments be recorded with date, time and author.**

Dr. Gelzer said electronic records can save you when the record-keeping combines with the metadata to provide an accurate picture. But, as some recent cases of snooping hospital employees have proven, EMRs can also detect when someone violates HIPAA. And, just because an EMR creates something that looks like a medical record doesn't mean that document fits the legal definition of a medical record.

### **Few protections exist**

Minneapolis health care attorney Gerald Deloss, vice chair of the American Health Lawyers Assn.'s Health Information and Technology Practice Group, says safeguards, including system certification, help vendors design systems that meet

certain legal criteria relating to the Health Insurance Portability and Accountability Act and the civil procedure laws. But as certification requirements evolve, safeguards can end up lacking.

"There are currently very few standards for EMRs, and the certification process is just now getting under way. ... [It] still allow[s] behavior that would disqualify the EMR as a legal record if challenged in court," said Jonathan Tomes, president of EMR Legal, a consultancy firm based in Overland Park, Kan.

The Certification Commission for Healthcare Information Technology, which declined comment for this story, is the most well-known and widely used certifying body. The organization, founded in 2004, was contracted by the U.S. Dept. of Health and Human Services in 2005 to help further its goal of widespread EMR adoption. It released its first set of certification criteria in 2006.

"CCHIT is absolutely invaluable. However, it still isn't comprehensive enough to relieve physicians of any due diligence responsibility [when searching for a system]. But it will be," said Dr. Gelzer, who has served on CCHIT work groups.

## **Electronically stored data are discoverable in trial.**

Dr. Gelzer noted that while CCHIT certification requires amendments to patient files be recorded with the date, time and author, there is no requirement to save a copy of the original document. HIPAA auditing would require retrieving all versions of a record. CCHIT does now require that certified systems track the identity of anyone who looks at or alters a patient's file, and include the date and time.

Barbara Drury, president of Pricare, a Larkspur, Colo.-based consultancy group that works with small practices and professional liability insurance carriers on health IT issues, said many older EMRs don't identify individual users.

In some small practices, she said, nurses use the physician's login to record data. Other systems allow multiple user logins, but aren't capable of self-auditing. With these EMRs, if a patient were to exercise HIPAA rights and request a list of everyone who accessed his file, the vendor would have to analyze the metadata.

"It's basically about recognizing that the EMR industry is still fairly new," Dr. Gelzer said. "If you went to a car dealer in 1955 and demanded seat belts and air bags, they would look at you like you were nuts. But knowing what you know now, you wouldn't buy a car without seat belts or airbags. People are being asked to buy EMRs without seat belts or air bags."

Dr. Gelzer said there are three areas to consider when shopping for a legal EMR:

- How well the system shows authorship. Does it clearly show who entered what portion of the record?
- How the system deals with changes. Does it track alterations to the record as well as who made each change and when? Does it save the original?
- How well the system's audit function supports the accuracy and validity of the record. Are there cross-checks in place?

"If they get those three things down, the likelihood that the system has a solid design gets much better," Dr. Gelzer said.

## **User error**

Stephen Fischer, MD, a solo family physician in Houston, said that if a system has basic security functions, like login names with passwords and the ability to record who opened what file at what time,

"that's really all that's necessary."

Dr. Fischer developed a home-grown EMR system about 10 years ago and has since commercialized it.

When Robert Anthony, MD, medical director of the emergency department of Frisbie Memorial Hospital in Rochester, N.H., was shopping for a hospital EMR, he found most systems do have the proper features. It was the users he worried about.

Drury agrees, saying there are no certification processes for users, but there should be. A system used incorrectly offers many ways to help a plaintiff prove the physician is negligent.

One doctor, she said, doesn't fill prescriptions with the EMR's electronic prescribing system but instead writes it on a prescription pad, then enters it into the EMR at the end of the day. Although the EMR generates safety alerts, the physician would see them only after the patient had the prescription. So if a patient has an adverse medication reaction, the doctor will have no defense.

Dr. Anthony said it all comes down to proper training and making sure the practice's policies for a paper-based system carry over into an electronic one, and are reinforced.

At Frisbie, each user was required to go through HIPAA training as it applied to an electronic system. Everybody was taught it would be a violation to share passwords or login information, for example, or to keep a patient's information visible on an unattended computer screen.

Another potential user error is turning off built-in decision-support systems such as drug interaction alerts and exam reminders. Deloss said there hasn't been much action by the courts in that area yet, but he suspects negligence claims could be filed against physicians who deactivate or ignore alerts.

Experts say while EMRs can make workflow faster and more efficient, physicians must be vigilant in making sure these efficiencies aren't short-cutting decision-making.

Attorney Lori-Ann Rickard, president of St. Clair Shores, Mich.-based Rickard & Associates, said there can be problems with systems that have click-box features, which allow physicians to select pre-formatted boxes to answer questions during the clinical exam. "When I am in litigation, they are always making the doctor look like this heartless guy that is trying to whip through patients, but 99% of the time that is not true."

She recommends systems provide an outlet for free text, so a doctor can click standard boxes, but still add notes to show the variations between each patient exam. "I want a doctor who is thinking and I want the medical record to show he is thinking."

Click-box features also can create inaccurate records through use of "auto-neg" features that insert negative responses for any box not checked. Deloss said if that record were called into court it would be difficult to determine if the question was ever really asked.

But even EMR notes that are written out come with risk. In the April 17 *New England Journal of Medicine*, Pamela Hartzband, MD, and Jerome Groopman, MD, a physician couple in Massachusetts, wrote about the dangers of errors being perpetuated when physicians cut and paste previous clinical notes written by colleagues. Similarly, cloned data -- copied boilerplate language -- is on the radar of insurers, and many are refusing to accept it as establishing medical necessity.

As the EMR industry matures, many more issues will be discovered, Dr. Gelzer said.

Physicians shouldn't give in to the pressures to go electronic until they have gone through a careful, deliberate selection process, he said.

"The idea that an EMR decision could actually be a step backwards is obviously not something the vendor is going to say," Dr. Gelzer said.

"And the government wants so badly for people to use these systems, but the government hasn't been forthright about the risk issue either."

[Back to top.](#)

---

## **ADDITIONAL INFORMATION:**

### **Making it legal**

Electronic medical records presented as evidence in court must have certain attributes.

- The record must be documented and kept in the normal course of business.
- The record has to be made at or near the time of the exam or event recorded.
- The record has to be made by a person with knowledge of the events. When dictation is used, the physician must review the report for accuracy and authenticate it.
- The computer used must be considered standard and efficient equipment.
- Authors and sources of information must be identified.
- Alterations must be noted and the original record preserved.
- Authors must be able to display the quality checks/audits used to ensure data integrity.

Sources: "The Legal EMR" presentation by Reed Gelzer, MD, and Patricia Trites; other resources

[Back to top.](#)

---

### **Before you buy**

Ask the vendor if and how an EMR will protect physicians and produce legally sound records.

- Does the system assign authors to each new entry in a document? The system should not overwrite a prior author.
- Does the system record the time and identity of each user and what he or she looked at or changed?
- Are alterations to records obvious?
- How easily can an audit be performed? How accurate is the audit? The audit trails should not be alterable or easily disabled.
- Does the EMR allow "documentation by exception," which allows the determined norms to be entered into the record unless otherwise changed?
- Does the EMR allow "open item billing," which automatically bills when an order is made? If so, can it be disabled?
- Does the system have controlled access that provides different views dependent on the user's job title or department?
- Does the system allow cut-and-paste functions? If so, is the original source identified?
- If the system has click-box features, does it also allow free-text entry?

Sources: "The Legal EMR" presentation by Reed Gelzer, MD, and Patricia Trites; other resources

[Back to top.](#)

---

Copyright 2008 American Medical Association. All rights reserved.

**RELATED CONTENT** *You may also be interested in reading:*

[Insurer finds EMRs won't pay off for its doctors](#) March 10

[AMA meeting: Delegates seek tax credit to help pay for EMRs](#) Dec. 3, 2007

[EMRs don't guarantee quality care, a review of 50,000 patient records shows](#) Aug. 13, 2007