Risk Review
a Publication of Princeton Insurance

Princeton Insurance
Partnership. Prevention. Protection.

January 2008

Your Direct Link to Better Risk Management Practices

Is Your Electronic Health Record Structured to Provide You With Legal Protection?

Follow-Up to our Electronic Health Records Issue

James B. Couch, M.D., J.D., FACPE
Managing Partner & Chief Medical Officer
Patient Safety Solutions, LLC

The previous issue of *Risk Review* was dedicated to the basics of electronic health records (EHR) and other safety-enhancing technologies. In addition to establishing the differences between electronic health records and electronic medical records (EMR), as well as defining a host of other related terms and concepts, the articles in that issue explored the benefits and risks of these technologies and recounted the success story of at least one physician's experience in implementing EHRs.

This article delves more deeply into what EHRs (or EMRs) must be able to accomplish in order to be considered "legal." For the purposes of this article, to be "legal," an EHR or EMR must comply with the stipulations for business records on computers (which apply to any kind of electronic record compiled during the "ordinary course of business"). This does not mean that failure to comply makes an electronic record "illegal." However, as indicated in some of the examples in this article, noncompliance could subject physicians having such records to increased legal risk, including even fraud allegations – see the "**Billing and Clinical Systems Integrity**" section below.

What Constitutes a "Legal" Electronic Health or Medical Record?

The American Health Information Management Association's (AHIMA), which is dedicated to improving the standards for electronic health and medical records states on page 64A in its practice brief, *Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes; AHIMA; Chicago (2005)*:

> The legal health record is the documentation of healthcare services

continued on page 2

Vice President of Healthcare Risk Services
Tom Snyder x5852

Manager, Healthcare Risk Services
Phyllis DeCola x5897

Phone: 609.452.9404
www.RiskReviewOnline.com

We welcome your feedback, comments and suggestions. Please feel free to contact us if you have a question or to send us your ideas for improving this site.

Summary of Key Points

- The legal health record is the documentation of healthcare services provided to an individual during any aspect of healthcare delivery in any type of healthcare organization.
- There are three key functional requirements which electronic health and medical records must meet to be considered "legal": Authentication, Systems Integrity and Privacy/Security Protection. Use of systems failing to meet these functional requirements may result not only in greater malpractice liability, but also greater vulnerability to claims of fraud and violations of privacy, security and confidentiality according to HIPAA Rules.
- Authentication refers to an EHR or EMR's ability to demonstrate that the information is accurate and unaltered. Records of alterations are considered supportive data, which the user can, if needed, inspect for purposes of validation. This "data about data" is often referred to as "metadata."

- For physicians whose practice management and electronic health or electronic medical records interact, they should make sure that these systems don't automatically bill for services in advance of their actual occurrence. Otherwise, they may be vulnerable to charges of fraud, if those events in fact do not occur.
- The ability to perform or retrieve audits on the information entered; who entered, viewed or altered information; and what information has been retrieved or printed from the system is paramount to complying with the HIPAA Privacy and Security Rules, as well as to defend oneself or one's practice in a professional liability action. EHR systems need to have been certified at least according to the 2007 criteria of the Certification Commission for Healthcare Information Technology (CCHIT) to have any degree of assurance that they comply with these HIPAA rules. Even then, prospective buyers should make their own independent determinations of this compliance. ❖

provided to an individual during any aspect of healthcare delivery in any type of healthcare organization. It is consumer-or patient-centric. The legal health record contains individually identifiable data, stored on any medium, and collected and directly used in documenting healthcare or health status.

Legal health records are records of care in any health-related setting used by healthcare professionals while providing patient care service or for administrative, business, or payment purposes. Some types of documentation that comprise the legal health record may physically exist in separate and multiple paper-based or electronic or computer-based databases.

There are three key functional requirements which EHRs and EMRs must meet to be legal: authentication, systems interaction and privacy/security protection. Use of systems failing to meet these functional requirements may result not only in greater malpractice liability, but also leaves its users vulnerable to claims of fraud and violations of privacy, security and confidentiality according to HIPAA Rules.

Authentication Functional Requirement

This refers to an EHR or EMR's ability to demonstrate that the information is accurate and unaltered. In most systems, this function is handled in the background. Records of alterations, deletions or additions to a record are considered to be supportive data which the user can, if needed, inspect for purposes of validation. This "data about data" is often referred to as "metadata." The ability to properly show late entries in an EHR or EMR is another important functional requirement to authenticate. Although some older systems show all of the "before and after" versions of changes in a single version, some newer systems do just the opposite, showing only one version and giving few, if any, indications that an alteration took place or what exactly the prior version stated.

To identify previous versions may require the very skills which could permit undetectable alterations of the records, thereby further compromising their integrity, credibility and authenticity. This could lead to suspicions of electronic "cover-ups" in the context of medical litigation cases, further complicating their defense, even when there may be no strong claims for negligence.

These variations and their legal implications for users demonstrate why every user must have a basic understanding of how the EHR or EMR system works, and, more importantly, meticulous instructions regarding how the system is to be used correctly. Behind every EHR or EMR implementation there must be medical records policies and procedures that form the crosswalk from documentation compliance rules to system use rules. This will help ensure that all users routinely and habitually generate and use documentation systems in a manner that, since compliant with existing rules, regulations, and practice standards, serves all the intended uses of a legal medical record (*How to Evaluate Electronic Health Record (EHR) Systems;* Trites, Gelzer; pp. 2-3; AHIMA; Chicago,2008).

Billing and Clinical Systems Integrity

EHR or EMR systems must electronically interact either with their own fully integrated practice management system, or connect or transfer specific information between the EHR and a compatible practice management system through an interface. A major source of risk in integrated or linked EHR and practice management systems is how they manage tentative or incomplete actions, such as an encounter in progress that is left incomplete, or the ordering of a test usually performed in the office. Systems that generate a billing event in an incomplete action can inadvertently lead to claims of fraudulent billing. For example, a urinalysis is ordered, the patient cannot void, but the system dutifully bills for the ordered test anyway, and the medical practice gets paid for a service never delivered.

Now that a practice or organization has a computerized set of processes in place, an auditor can come to the physician's office or hospital facility and access all of the Medicare charge events from the practice management system (or access the explanations of benefits from the last few months) and proceed to review the documentation in the EHR and check the date and time stamps to verify when the physicians actually completed the documentation. This will also allow the auditor to inspect the documentation time stamps to verify when the providers actually completed the documentation and compare these documentation time stamps to the service submission dates in the billing system or explanation of benefits (EOBs). One EHR system actually shows on the face sheet of the system a list of all of the encounters that have been sent to billing, but which do not have closed or completed documentation. This is a government auditor's dream come true when identifying false claims *(Trites and Gelzer, pp. 3-4).*

Privacy and Security Safeguards Functional Requirement

The first two years (2005 and 2006) of certification criteria from the Certification Commission for Healthcare Information Technology (CCHIT—see our previous issue) did not ensure that those systems certified even complied with basic HIPAA Security and/or Privacy Rules. CCHIT Criteria for 2007 and projected for 2008 will address this to ensure that to be certified, systems must comply with basic HIPAA Security and Privacy Rules. However, if a user purchased a system in 2007 (or earlier) which was not certified according at least to 2007 criteria, then it is possible that such a system may not even ensure HIPAA compliance. The ability to perform or retrieve audits on the information entered; who entered, viewed, or altered information; and what information has been retrieved or printed from the system is paramount to complying with the HIPAA Privacy and Security Rules, as well as to defend oneself or one's practice in a professional liability action. This one element is significant to proving or disproving an allegation of misuse or malpractice. So just because a system is "certified," that doesn't mean that it will meet all of the requirements of existing laws or regulations, nor will that relieve prospective buyers and users of systems from undertaking thorough due diligence and compliant work processes (*Trites and Gelzer, p. 11).*

Conclusions and Recommendations

Physicians using an EHR must understand its functions and what it does or does not (or perhaps even *cannot*) do as an authenticating documentation system, as it interacts with an integrated or linked practice management system or as being protective (or not so protective) of patients' rights to privacy, confidentiality and security of their personally identifiable medical information.

The purpose of this brief article is certainly not to discourage the appropriate use of electronic records, but rather to ensure that those that are used meet these basic functional requirements to protect both physicians and their patients from a variety of avoidable legal risks, while facilitating the delivery of higher quality, safer and efficient care.❖