Toward safer EHR use and documentation

Tips for reducing malpractice risk

BY TRISH LUGTU, BS, CPHIMS, CHP

The launch of the Medicare and Medicaid Electronic Health Records (EHR) Incentive Programs in 2009 triggered a surge of health information technology implementations, most of which were undertaken with little consideration of their potential to contribute to malpractice risk. When designing EHR systems, vendors remained neutral on risk management practices in order to avoid liability. This left physicians vulnerable. Predictably, technology-related safety events have occurred, and management of technology-related malpractice risk has emerged as a concern.

In the years since the launch of the incentive programs, we have amassed a growing base of EHR-related malpractice claims data. Analysis of that data is yielding lessons that will help physicians produce better EHR documentation and more effectively manage risk related to health information technology.

A sea change in medical practice

It is important to understand that the EHR is more than just a tool for documentation. The EHR-enabled medical practice represents a “huge change in the way health care is delivered,” according to Dean F. Sittig, PhD, a professor in the School of Biomedical Informatics at the University of Texas Health Science Center at Houston. EHRs enable clinicians to communicate with each other about patients and to view patient data in ways that can affect the quality of care as well as the way in which they work.

Sittig describes EHR-enabled health care as having a number of components, only some of which are technical in nature but all of which must be managed in order to avoid negative consequences. Thus, in designing an EHR system, it is essential to not only consider technical concerns but also how people will interface with the technology and how it will affect workflow, care, policies and procedures.

A recent example that shows how problems can arise as a result of these factors not being well-managed was the missed Ebola diagnosis at Texas Health Presbyterian Hospital in Dallas last fall. When Thomas Duncan was admitted to the emergency department, a nurse recorded his recent travel to West Africa. But the workflow was not configured so that this crucial information was communicated to other clinicians caring for him. This delayed Duncan’s diagnosis and treatment. One wonders if the outcome would have been different had risk managers, clinicians and health IT staff considered both the human and the technical factors in the initial EHR design.

Although this story made the national news, many more remain out of the spotlight. Claims analysis is uncovering more and more evidence on the risks generated by EHRs. One study by Boston-based CRICO Strategies, a division of the Risk Management Foundation of Harvard Medical Institutions, involved analysis of 147 malpractice claims in which the use of EHRs was a contributing factor. In 9% of those claims, the problem was attributed to “failure of system design”—much like what occurred in the case of Thomas Duncan.

Making EHR documentation safer

The EHR may have introduced compelling new ways to manage patient health; however, it is primarily used to document the care that is delivered. Documentation deficiencies (lack of consistency, coordination, accuracy, timeliness and objectivity) can lead to significant consequences including patient injury. And many malpractice cases hinge on these deficiencies, as the medical record is the primary source of evidence used to determine whether a physician or health care facility is liable for malpractice. Our experts estimate that the defense of 35 to 40 percent of malpractice claims filed is jeopardized by documentation problems within the medical record.

Faulty data entry is alarmingly common. In a study of EHR documentation in the Veterans Affairs health system, 84 percent of progress notes analyzed contained at least one documentation error; on average, the notes contained 7.8 documentation errors. However, not all errors are created equal. Through analysis of
malpractice claims data, incorrect information was found in 20 percent of all cases studied, making it the leading EHR-related risk factor.\(^3\) Adding to the risk is the proliferation of EHR data—whether accurate or not. Copies of information exist in backups, patient portals and other clinical systems. To avoid the risk of incorrect information finding its way into the EHR, consider these best practices:

**Double-check information.** In the CRICO analysis, faulty data entry led to the selection of incorrect units that distorted dosing calculations; unanticipated autoconversion of numbers (eg, 2.5 becomes 25); and information being entered into the wrong patient record when the user accidently opens the wrong file. Although template design can reduce the likelihood of faulty data entry, even with all their checks and balances, EHRs simply do not eliminate human error. Therefore, double-checking remains the best defense.

**Avoid pre-populating templates.** A significant contributor to incorrect information is pre-populated workflow templates—ie, templates that default patient assessments to “normal” or which require clinicians to “uncheck” normal findings. Such templates have high potential not only for contributing to diagnostic errors but also to billing fraud, as every system marked “normal” may not actually have been assessed.

**Avoid cut-and-paste/copy forward.** Although this function may seem like a great timesaver, it can contribute to incorrect information proliferating across many notes and even across other systems as records are exchanged. Use of the cut-and-paste or copy-forward functions should be limited to demographic information only. Do not cut and paste information that has not been independently obtained or verified, as patients’ histories and recollections may change depending on who is asking the questions, how questions are asked, the patient’s pain or anxiety levels, their current medications, and the presence of family members at the time of questioning.

**Be cautious when amending documentation.** Amendments describe a range of alterations that are intended to clarify information. The processes for amending documentation are more complex with EHRs than with scanned, imported or transcribed notes, as the nuances are captured behind the scenes in metadata, which increases the importance of clarifying how each is defined. The following definitions of amendment types are adapted from the American Health Information Management Association’s Amendments in the Electronic Health Record Toolkit:\(^4\)

- **Addendums.** An addendum is used to add information to a completed entry. Methods to attach or connect addendums to an original document depend on the EHR’s capabilities, so it is important to design them so they are visible and to implement processes for filing and viewing them. Addendums must include the date of documentation and be completed according to your organization’s documentation completion policy. (Each practice must have documented processes for completing an entry and define when an entry is completed.)

- **Corrections.** Corrections are intended to fix an inaccuracy in an entry. Information may be corrected before or after an entry is completed. Your organization’s policies should specify the procedure for making corrections to a completed entry and identify who is allowed to make such corrections. When correcting comingled records (moving an entry from one patient to another), steps must be taken to avoid a privacy breach. For example, simply striking through misplaced patient information is not sufficient enough to hide it and prevent unauthorized disclosures.

- **Retractions.** Retractions are used to correct invalid information or documentation made in error by hiding it from general viewing. Keep in mind, the original information remains archived and is not completely erased from the system. It is crucial to be able to hide incorrect information that may lead to an inappropriate medical judgment.

- **Deletions.** Deletions completely eliminate information from an EHR. Only with some EHRs is it possible to perform true deletions. If at all possible, deletions should be avoided. If they are allowed, your practice should have a clear policy about when they can be used; monitor and audit their use; document them in a log outside of the EHR; and control who is able to perform deletions.

**Late entries.** Late entries relate to an original entry but are created at a later date. Late entries also may be defined by type of documentation, such as direct template entry outside the point of care. It is important to clarify when a late entry must be included as an addendum.

**Final considerations**

Electronic health records have changed the way physicians and other clinicians work. However, they are primarily used to document the care doctors, nurses and others provide. In the end, when memories fade, it is this documentation that physicians rely on to manage a patient’s health. That same documentation is what stands in your defense of a medical malpractice claim or lawsuit. It is ultimately the physician’s responsibility to understand the ins and outs of the documentation their EHR creates, along with the risks that come with poor-quality documentation. Remember, it is your signature, albeit digital, that completes the entry.

Trish Lugtu is associate director of research for MMIC’s Patient Safety Solutions team.

**REFERENCES**

2. Ruder DB. Malpractice claims analysis confirms risks in EHRs. PSHQ. January/February 2014;20-3.