Patient Safety and Liability Concerns in the Era of Electronic Records

Laura M. Cascella, MA

Electronic health records (EHRs) — once a fairly cutting-edge concept — have become a standard fixture in healthcare. Data show that the adoption of EHRs continues to grow. The Office of the National Coordinator for Health Information Technology (ONC) notes a 62 percent increase in EHR use from 2004 to 2014 among office-based physicians. Research also shows that the number of dentists using EHR systems is rising.¹,²

These increases undoubtedly are driven by the Centers for Medicare & Medicaid Services’ (CMS’) EHR Incentive Programs, as well as a natural progression toward more technological processes.

Although doctors and other healthcare professionals have seen the benefits of EHR systems, they also have noted numerous challenges with EHR functions, capabilities, and overall effect. Similarly, EHRs have presented new issues in relation to malpractice. A PIAA survey found that 53 percent of member companies had EHR-related malpractice litigation.³ Major contributing factors in this litigation included problems with documentation, system functionality, metadata, record format, vendor support, and more.

This article focuses on a number of areas in which EHR-related risks may occur due to time constraints, inexperience, oversight, or other factors. Risk strategies also are presented for each area covered, with the hope that they will lay the groundwork for more thorough discussions within medical and dental practices about how to manage risks associated with these complex systems.

Implementation

Implementing or upgrading an EHR system requires thorough research, careful planning, and ongoing assessment and adjustment once the system is in place. According to Ted Passineau, a senior patient safety and risk consultant at MedPro Group, “the implementation phase is a time when errors commonly occur because of lost data, process and workflow changes, and other inconsistencies.”

To minimize the risks associated with implementation, medical and dental practices should develop clear policies for transitioning data between systems and for reconciling new electronic records with older paper records, so as not to misplace data or overlook critical health information.
Additionally, careful evaluation and an open dialogue with staff about workflow processes may help identify potential issues early, so effective strategies can be developed.

Staff cooperation and compliance also are critical during the implementation phase. Although some providers may welcome the new technology, others might be resistant to change.

In some instances, staff resistance has led practices to maintain both paper and electronic systems to meet the preferences of all providers. However, research has shown that dual systems decrease efficiency and increase the risk of errors.4

Although it might be tempting to try to satisfy everyone’s preferences, it also can be counterproductive and, ultimately, it does not support an environment of cohesive teamwork.

**What Can You Do?**

- Include staff members who will be using the EHR system in initial research and planning activities.
- Develop a plan for how the practice will handle paper records once the EHR system is in place. Will paper records be scanned into the new system? If not, what are the expectations for providers to reconcile old records with new ones during patient encounters?
- Seek staff input on developing policies and workflow procedures that align with the new system.
- Support staff throughout the implementation phase by including them in the decision-making process, maintaining transparent communication, and establishing firm expectations related to EHR use.
- Provide training and education during implementation and after to help staff (a) acclimate to the new system, (b) recognize potential process or system problems, and (c) work toward reasonable solutions.

---

**CASE EXAMPLE**

A patient’s orthodontist referred her to an oral surgeon for elective extraction of several teeth. The surgeon met with the patient to discuss the procedure and obtain consent.

The night before the extraction, the surgeon reviewed the patient’s electronic record, and the procedure commenced the next day without complications. However, following the procedure, the surgeon noticed a separate paper chart for the patient. In the chart was a letter from the orthodontist with a new, updated treatment plan that was never entered into the EHR. The new plan recommended removal of different teeth than the original plan specified.
Documentation

Accurate and thorough documentation is the backbone of risk management; it provides essential patient information, historical details about the course of patient care, and a record of services provided.

EHRs are intended to streamline the documentation process, while at the same time capturing more information than was previously possible with paper records. Although this may result in more substantive patient information, it also presents new opportunities for error.

Copy and Paste

The practice of “copy and paste” is perhaps one of the most common and egregious missteps in EHR use. In PIAA's survey, this practice was listed as the top trend in EHR-related allegations.5

Copy and paste — also called cut and paste, cloning, or carrying forward — refers to electronically lifting information from a previous entry in a patient’s record and placing it in the current entry. It also refers to copying information from one patient record to paste into another, such as through the use of boilerplate language.

Automated functions within EHR systems facilitate the cloning of information because of the ease with which the user can grab and move content.

Practitioners who feel crunched for time may find the copy and paste function enticing because it’s quick and easy. Yet, as noted in an article from HealthLeaders Media, “quick” doesn’t necessarily equal “efficient.” Copying and pasting content can result in the proliferation of incorrect or nonapplicable information throughout electronic records, which can be “detrimental to . . . patient care”6 if, for example, treatment decisions are based on inaccurate or old information.

CASE EXAMPLE

A patient who had a history of smoking, high cholesterol, and borderline hypertension presented to his primary care office complaining of intermittent numbness in his left hand and mild neck pain.

The patient expressed concern that his symptoms were cardiac related because his brother had recently had a heart attack. The patient’s electrocardiogram was normal, and the provider diagnosed the patient with nerve compression.

Several months later, the patient presented to urgent care for gout and an ongoing cough. Although the urgent care provider had access to the patient’s EHR, it did not reflect his recent symptoms or family history of heart attack because it was a duplicate of an older record. The patient was given medication for gout and cough and sent on his way.

Nine days later, the patient was found dead. The death certificate indicated atherosclerotic disease and heart attack as the cause of death.
The use of copy and paste also can have serious consequences for corporate compliance. When information is carried forward from encounter to encounter without careful review by the healthcare provider, the practice might end up billing for services that did not occur. Even though this type of billing error might be a simple oversight, it could lead to allegations of fraud, which may jeopardize reimbursement from Medicare and other payers.

Copy and paste also can have a negative effect on data integrity. One of the goals of EHR use is to facilitate the electronic exchange of health information and collection and submission of clinical quality measures. Inaccurate data that results from poor practices like cloning may have long-term implications for population health studies, disease tracking, and data mining.

What Can You Do?

- Establish guidelines for when copy and paste is prohibited and when it may be used with extreme care (if ever).
- If copy and paste is allowed in any circumstances, ensure that the practice’s policy stipulates the need for providers to carefully review any information carried forward records. Copied information should be updated/revised as appropriate, and providers should electronically sign the record indicating their review and approval of the information.
- Routinely audit records to check for errors that may have resulted from copying and pasting patient information.
- Educate staff about the dangers and consequences of using poor documentation practices and shortcuts, such as misinformed treatment decisions and fraudulent billing.

Data Entry Fields, Check Boxes, and Templates

One of the proposed benefits of EHRs is structure and standardization. When used appropriately, data entry fields, check boxes, and templates help generate consistent documentation across providers. However, standardization also presents new dilemmas. For example, inaccuracies in the records might occur if:

- The data entry fields don’t match the clinical situation.
- The system automatically defaults to a selection of “normal.” If all options are not carefully reviewed, the record might indicate a normal value for a condition that was never evaluated.

RESOURCE

• Providers select the wrong template or check box, which can easily happen when multiple options are presented and time is of the essence.
• Providers are unaware of how taking an action within the EHR ultimately affects the physical output of the record.

Also, although data entry fields, check boxes, and templates can save time, over-reliance on these functions can result in records that lack specificity. Without the unique patient narratives that were customary in paper records, it may be difficult to distinguish one patient encounter from the next.

What Can You Do?
✓ Ensure that the EHR product you select can be tailored to the clinical situations that are relevant to your practice.
✓ Be aware of whether your system automatically defaults to a normal setting. If so, carefully review the record at each encounter to ensure it doesn’t misrepresent clinical information.
✓ Provide a final quality control review of all data you enter and boxes you select in the EHR.
✓ Occasionally print out records to ensure information is presented in a logical, accurate format.
✓ In addition to using data entry fields and check boxes, provide patient-specific notes and comments in the record, as appropriate and necessary.

Metadata
As mentioned previously, EHRs present an opportunity to collect more documentation and data than was ever possible with paper records. A distinguishing characteristic of EHRs is their ability to collect metadata, or “data about data.” The metadata generated by an EHR might show:

• Who accessed a record and when they accessed it
• The date and time that test results were reviewed
• The data and time that a record was modified
• How long a provider had a record open and how quickly he or she selected various options

Simply stated, metadata provide “a permanent electronic footprint”8 that tracks healthcare provider activity. For some doctors, metadata might necessitate a change in workflow. For example, providers who have typically entered some information into patient records prior to the actual patient encounters will need to adjust their processes. Otherwise, metadata might show inconsistencies in the timing of events.
The implications of metadata on malpractice litigation are still evolving. In 2006, e-discovery amendments were introduced to the Federal Rules of Civil Procedure (FRCP). These amendments apply to litigation in federal courts; however, various states also have partially or fully adopted the FRCP’s approach or implemented their own e-discovery statutes or rules.

In theory, metadata could work for or against the defense — either by confirming the doctor’s recollection of events or showing discrepancies in the doctor’s statements.

**What Can You Do?**

- Learn how your system’s metadata function works, and develop documentation policies around that knowledge.
- Ensure that providers in your practice are mindful of the type of metadata that your EHR system collects.
- Adjust workflow processes as necessary to eliminate inconsistencies in metadata.
- Develop guidance for how to appropriately amend or update electronic records. Without a defined policy, changes to a record may raise questions about the validity of information.
- Be aware of your state’s laws or rules related to e-discovery. Consider hiring an outside party to perform an annual audit of your EHR and provide feedback about the quality of documentation, adherence to regulatory standards, and billing/coding compliance.

**Alert Fatigue**

Perhaps one of the most powerful patient safety capabilities of EHR systems is their potential to analyze patient data, provide clinical decision support, and send providers alerts about possible contraindications (such as dangerous drug–allergy interactions). These tools are valuable, but only if they’re utilized in an efficient way.

Systems that bombard providers with an overabundance of alerts can be frustrating and lead to a phenomenon known as “alert fatigue,” in which providers automatically ignore or override alerts without verifying their content.

An *American Medical News* article attributes alert fatigue to the “frequency and often lack of necessity” of alerts. A survey of primary care providers from the Department of Veterans Affairs showed that almost one-third of those using EHRs reported that they missed or did not follow up on alerts about patient test results, and almost 87 percent thought the quantity of EHR alerts was excessive.

These study results suggest that when providers are inundated with massive numbers of noncritical or nonrelevant notices, the likelihood that important information will be overlooked increases. After receiving a number of unhelpful
alerts, a doctor might bypass the next alert based on the assumption that it is another “false alarm” — when in fact, it might contain critical information.

To complicate matters, not all alerts that are overridden are the result of providers ignoring the system. Many times, alerts are overridden for valid clinical reasons. But metadata that capture overrides likely won’t distinguish between the two. If metadata are used as evidence in a malpractice lawsuit, a doctor might have to defend why he or she overrode a system alert.

**What Can You Do?**

- Determine whether your EHR system’s alert function can be tailored for your practice/specialty.
- If your practice is in the process of purchasing an EHR system, include questions about the alert capabilities in your initial research and assessment of products.
- Ask your vendor whether the system’s alerts can be classified based on severity or other factors.
- Provide documentation and support for overriding clinically significant alerts.

**Privacy/Security**

Privacy and security of patients’ protected health information (PHI) have been at the forefront of healthcare for a number of years. Most doctors are well aware of their obligations to protect PHI under state and federal regulations.

Yet, as information has gone digital, new questions and concerns about privacy and security have arisen. In PIAA’s EHR survey, allegations of HIPAA violations were in the top 5 EHR claims trends. Some of the issues noted included data breaches due to inappropriate access, shared passwords, confidentiality breaches, and stolen data that lack encryption.14

Factors that were never relevant to paper records now must be considered with electronic records. For example, PHI is much more mobile in electronic format. It can easily be transmitted or taken out of the office on laptops, flash drives, etc. Without safeguards in place, the risk of lost, stolen, or unauthorized access to data increases.

**CASE EXAMPLE**

An employee at a healthcare practice had tapes containing EHR backup data and staff information in a laptop bag in his car. The car was broken into, and the bag and tapes were stolen. Although the files were password protected, they were not encrypted, causing a security breach.

As a result of the breach, the practice had to report the incident to the U.S. Department of Health and Human Services and the state’s Attorney General — as well as retain consulting firms to investigate the situation and send notification letters to approximately 55,000 patients.
Other privacy and security considerations with electronic health information include:

- **System platform.** Some EHRs are stand-alone systems that exist within a single practice, while others are accessed through the Internet. Both types of systems offer security features not available with paper records, but both also involve risks. For example, with an office-based system, a disaster — such as a fire or tornado — could damage the system and destroy patients’ PHI. With an Internet-based EHR, vendors manage many security settings, and their standards might be difficult to assess.¹⁵

- **Password security.** To help prevent data breaches, individuals who are authorized to access the EHR system need unique passwords or passcodes to help the system authenticate their identities. Protocols for logging in and out of the system should be strict, but not overly time-consuming.¹⁶

- **Data encryption.** Encryption refers to coding information in a way that prevents unauthorized users from reading it. This technology can protect PHI when it is stored on a device or transmitted electronically.

- **Time-outs and record locks.** Even the most cognizant provider can forget to close a record or log out of a system. A system that shuts down or locks records after a certain period of inactivity can add an extra layer of security that helps prevent unauthorized access to PHI. Record locks also can be used to prevent providers from inappropriately modifying records (per your practice’s medical record policy).

- **Email communication.** Although EHR systems can make electronic communication among providers and between providers and patients a viable and convenient option, doctors should exercise caution when using email. Sending health information electronically might violate patient privacy if the information is not properly protected. Additionally, although providers’ email systems might be secure, they cannot attest to the security of their patients’ systems.

This list certainly is not exhaustive, but it does provide some broad considerations related to privacy and security of electronic health information. For more comprehensive and detailed guidance, please visit [http://www.healthit.gov/providers-professionals/ehr-privacy-security](http://www.healthit.gov/providers-professionals/ehr-privacy-security).

**What Can You Do?**

- ✔ When evaluating EHR systems, carefully research their privacy and security features.
- ✔ If your practice is considering an Internet-based EHR system, ask the vendor about its compliance with HIPAA and HITECH privacy regulations.
Ensure that the Business Associate Agreement your practice has with its EHR vendor requires HIPAA/HITECH compliance and details how access to data is obtained, how information is secured, and how the vendor ensures privacy and security.

Issue unique usernames and passwords to each individual who will access the system. Strictly prohibit password sharing and placing written passwords in an easily accessible location (e.g., taped to a computer monitor).

Enable system time-outs and record locks to prevent unauthorized access to patient data.

Use encryption technology to protect stored and transmitted data.

Develop a practice policy for the appropriate use of email communication with patients and other providers.

Ensure the practice has a process in place for handling security breaches and noncompliance with privacy and security policies.

Provide ongoing staff training on privacy and security policies and breach notification protocols.

Conclusion

EHR systems have increasingly become the norm in medical and dental practices. When used properly and with careful consideration, EHRs offer opportunities to streamline processes, enhance quality of care, and support patient safety efforts.

However, like all types of technology, EHR systems aren’t without risk. Changes in workflow, poor understanding of the system and its capabilities, user errors, and lack of defined protocols can all lead to process breakdowns and errors.

Awareness of the potential risks that EHRs present can help healthcare providers and staff proactively counter them through ongoing staff training, workflow evaluation, and development of comprehensive policies and procedures.

Endnotes


8 Mangalmurti, et al. Medical malpractice liability, 2063.


This document should not be construed as medical or legal advice. Because the facts applicable to your situation may vary, or the laws applicable in your jurisdiction may differ, please contact your attorney or other professional advisors if you have any questions related to your legal or medical obligations or rights, state or federal laws, contract interpretation, or other legal questions.

MedPro Group is the marketing name used to refer to the insurance operations of The Medical Protective Company, Princeton Insurance Company, PLICO Inc., and MedPro RRG Risk Retention Group. All insurance products are underwritten and administered by these and other Berkshire Hathaway affiliates. Product availability is based upon business and regulatory approval and may differ between companies.

© MedPro Group. All Rights Reserved.