MedPro Group
a Berkshire Hathaway company

EHR Liability and Risk Management Strategies

Graham Billingham, MD, FACEP, FAAEM

For many physicians, electronic health records (EHRs) have been somewhat of a failed promise. The proposed benefits of these systems — e.g., enhanced communication, broader research capabilities, standardized practice patterns, improved patient outcomes, and streamlined costs — often remain elusive or only partially realized. Clearly, EHR implementation has both pros and cons, and much has been written about the potential risks that these systems present.

As we approach a decade of EHR use, issues related to electronic records also have found their way into the courts. A recent PIAA study found that 53 percent of member companies had malpractice litigation directly related to EHRs. Top issues noted in these cases include inappropriate use of copy and paste, failure to review available data, HIPAA violations, and inability of systems to interface.[2] Others have pointed out the difficulty of defending cases in which electronic records include unexplained additions or deletions, late entries, subjective remarks, data entry errors, or alert overrides.

EHRS AND E-DISCOVERY

In 2006, e-discovery amendments were introduced to the Federal Rules of Civil Procedure. These amendments require production of electronically stored data and metadata if requested.[1] Metadata is the "hidden" data in electronic files, such as author of the entry, timestamp, changes to the record, etc. Metadata may not be easily accessible, and physicians and other providers may not always be aware of the content contained within metadata.

To address these issues, medical practices should develop policy statements that specifically define what each practice considers a "legal patient record." These policies will help practices track, preserve, and retain electronic records for business, legal, and compliance purposes. Each practice's policy should align with its respective hospital policy. Important considerations include the following:

- When are patient records considered complete for accreditation/compliance purposes?
- What data are disclosed upon request for medical records?
- What authorizations are required for release of protected health information?

Establishing a clear definition of the legal patient record and specific policies related to documentation will help medical practices respond to requests for disclosure, comply with state and federal medical record retention schedules, and safeguard records against breaches, tampering, and destruction.

Additionally, keep in mind that printed electronic records may look entirely different from the user interface that the practitioner sees. Knowing what the printed copy of the legal EHR record looks like will help raise awareness about the types of information available in print format and how it might appear to patients, legal counsel, and juries.

As EHR systems continue to mature and evolve, it is incumbent on physicians to identify emerging risks and put effective risk-prevention strategies in place to reduce liability exposure.

Top EHR Emerging Risks

Metadata

Requests for the production of electronic records will include large amounts of hidden data, such as time stamps, record authors, and changes to the record. Be aware of the information contained within metadata and its implication for workflow practices.

Audit Trails

Every keystroke leaves an electronic footprint for potential audit and discovery. Medical practices should consider hiring an outside party to perform an annual audit and provide feedback about the quality of EHR documentation, adherence to regulatory standards, and billing/coding compliance.

Paper

Discovery requests for printed copies of electronic records can be problematic if the treating physician is unaware of what these records look like in print format. Further, cases have occurred in which multiple versions of the same record appear different due to software upgrades and time synchronization issues (e.g., if patient care is documented before the actual provision of treatment). Review printed records on a quarterly basis to ensure familiarity with the print format. Does the record accurately reflect the care the patient received?

Definition of the Legal Record

Both physicians and hospitals should work together with legal counsel to define what constitutes the actual legal medical record. Written policies and procedures should address the following questions: When does the record begin and end? Who has access to the record? What should be disclosed during discovery? Consistency in the definition of the legal medical record is essential across the practice and the institution.

Big Data

A common question since the widespread adoption of EHRs is who is responsible for the large volume of data? Data overload is a legitimate concern, and the ability to decipher meaningful information out of vast quantities of unstructured data is challenging. Recent court cases have held that physicians are *not* responsible for knowing the entire medical record of their patients. Grasping the breadth of electronic patient data is even

more cumbersome when the patient has received care at multiple organizations within a healthcare system. The issue of big data should be closely monitored, as it is a moving target that continues to increase in complexity.

Record Preservation and Retention

Medical practices and hospitals have a clear-cut duty to preserve and maintain patients' medical records. Any modifications, tampering, or destruction of records can have both regulatory and legal ramifications. Practices and hospitals should develop written policies and procedures to address documentation best practices and record retention requirements.

Embedded Guidelines

The practice of embedding guidelines, such as Choosing Wisely®, in EHR systems is a common concern among physicians. As a general rule, reducing practice deviation — particularly for high-risk diagnoses — by adopting best practices is both good medicine and sound risk management. The key is to follow and practice these guidelines in both principle and documentation. Adopting best practices that are not implemented, documented in the record, or followed in practice markedly increases legal exposure.

Medical Errors

Adverse events, such as administering the wrong medication dosage or failing to document an allergy, can lead to poor patient outcomes and allegations of malpractice. Although human error cannot be completely prevented, EHR design is evolving to incorporate human factors engineering that both anticipates and mitigates the risk of errors.

Data Breach

Data breach, both intentional and unintentional, is a serious concern with EHRs. As technology continues to progress and becomes more sophisticated, so do malicious attempts to steal data. Physicians and medical staff should seek education and training so they are aware of cyber risks, and they should implement safeguards to protect medical records from breach. Increasingly risky areas include email, texts, passwords, social media, and hardware (e.g., stolen smartphones, tablets, and laptops). Annual security audits and strategies, such as secure encryption, will help address this area of risk.

Patient Portals

The intent of patient portals is to engage and empower patients, promote communication, increase transparency, and improve patient outcomes. To meet these objectives, medical practices should develop policies and procedures that address both the operational and legal aspects of portal use. Some important areas that polices should cover include terms of use, the physician–patient relationship, response times to queries and requests, emergency situations, and privacy/security.

Conclusion

Although EHRs have created new opportunities in healthcare, they are not without risk. Issues related to documentation, data overload, and privacy/security of health information represent some of the main concerns.

Physicians and healthcare organizations can mitigate EHR risks by (a) developing policies and procedures that address top concerns and emerging issues, (b) gaining familiarity with the concept of metadata and both the electronic and printed format of records, and (c) conducting regular audits to identify potential problems or gaps in policy.

Taking proactive steps can help physicians feel more comfortable with, and confident in, taking action if they receive a request for discovery of electronic data.

Endnotes

[1] Federal Rules of Civil Procedure. (2006, December 1). U.S. Government Printing Office. Retrieved from https://www.gpo.gov/fdsys/pkg/CPRT-109HPRT31308/pdf/CPRT-109HPRT31308.pdf

[2] PIAA. (2015, January). Part 1 of 2: Electronic health records and a summary analysis on the 2012 PIAA EHR Survey. *Research Notes, 1*(1), 3.