POTENTIAL PITFALLS OF EHRs: A LAWYER'S PERSPECTIVE

Electronic health records can be a boon for medical practices, but their use is not without hazards.

BY VICTORIA M. WALLACE, JD

The days of walking into a physician's office and seeing rows of color-coded files behind the receptionist's desk are long gone. Electronic health records (EHRs) have become the preferred choice for record-keeping in many practices. It is clear that EHRs have many benefits, including the capacity to improve quality of care, facilitate better transitions of care, and enable patients to easily access their own health information. However, it is important to recognize that EHRs can also be misused. An understanding of common EHR pitfalls can help physicians and their staff members implement policies and procedures to ensure appropriate EHR use.

POTENTIAL PITFALL NO. 1: CARRY FORWARD AND COPY-AND-PASTE FEATURES

Unlike paper records, which require manual data entry for each page of the record, many EHRs include *copy* and *paste* functions that allow users to carry forward demographics and other information from a patient's prior visit. These features help save time and ensure accuracy from one record to the next. However, as with paper records, it is not always appropriate to carry forward certain medical information.

For example, documentation of certain components of an examination that are required in order to bill a certain code should not be brought forward from a prior record. Similarly, it would be problematic to copy and paste a patient's refraction from a prior visit when those tests are required to be performed again. Government agencies are picking up on these issues, and blatant copy-and-paste jobs in EHRs have been cited to uphold postpayment denials and support allegations of false claims.

POTENTIAL PITFALL NO. 2: THE ERRANT EMPLOYEE LAPTOP

Because EHRs allow the capability to store thousands of patient records on a single laptop, the risk of a data breach is much higher today than in

85.9

Percent of office-based physicians using any electronic medical record or EHR system.

Source: Percentage of office-based physicians using any electronic health record (HER)/electronic medical record (EMR) system and physicians that have a certified HER/EMR system, by U.S. state: National Electronic Health Records Survey, 2017. www.cdc.gov/nchs/data/nehrs/2017_NEHRS_Web_Table_EHR_State.pdf. Accessed November 14, 2019.

the past. For example, a nurse who has his or her practice-issued laptop stolen can potentially expose the protected health information of many patients, leaving the practice vulnerable to privacy violations.

It is important to establish policies that dictate when computers with access to patient records can be removed from the practice and to implement requirements that ensure the security of patient information in the event a laptop is lost or stolen. Access controls, such as passwords, encryption, and audit trail features, are helpful tools to minimize the impact of such a breach.

POTENTIAL PITFALL NO. 3: FALSIFIED RECORDS

It is not a new phenomenon for unethical individuals to justify payments through the falsification of medical records. What is new is the ability of EHR software to track and monitor changes to an electronic record, potentially helping to detect the originator of such changes. EHRs often track *who* enters or changes information in a record, *when* it is entered or changed, and *what* is entered or changed.

When a claim is investigated, EHR software metadata could be used to prove that records were altered to bill for services that were not actually provided. This function may also help investigators detect improper use of an EHR to make it appear as though payment criteria have been satisfied when they were not.

CONCLUSION

Despite these pitfalls, having strong policies, procedures, and employee training on the appropriate use of EHR can help prevent improper use of the technology and associated legal risks. Conducting regular self-assessments to identify vulnerabilities related to EHR use is crucial to prevent such misuse. ■

VICTORIA M. WALLACE, JD
- Associate, Arnold & Porter, Washington, DC
- victoria.wallace@arnoldporter.com
- Financial disclosure: None