Potential Risks and Pitfalls of EHR Systems - Part II

By Jeffrey A. Woods, JD

In Part I last month, we discussed the potential risks and pitfall of EHR systems relative to digital assists and inconsistent processes. In this month's article, we will examine additional concerns unique to EHR systems that could create potential risks for the provider including the audit trail and alerts/pop-up warnings.

Every EHR system has an audit trail. The timeline is no longer a guessing game. Gone are the days of using handwriting experts to try to determine when and by whom an entry was made in a patient's chart. Forensic IT experts can now review the "metadata" contained within the EHR, which is basically the DNA of the EHR, to determine everything that occurred in that chart, including:

- Date and time stamp of records
- Who accessed the information
- On what occasion(s)
- For how long
- What records were accessed
- What records were available to the provider, but were NOT accessed

In the context of a claim or lawsuit, the audit trail does not play favorites. Unfortunately, for many providers, the audit trail is unforgiving. The record is what the record is, and the audit trail will either support the provider's position or sink it. If, for example, a radiology report or lab result was available to the provider prior to the patient's discharge, but the report/results were never reviewed, the audit trail will establish this fact. Similarly, if the standard of care (as established by expert testimony) requires a radiologist to spend a certain amount of time reviewing studies and the radiologist actually spent significantly less time performing that review than was typically required by the standard of care, this will be borne out by the audit trail.

Because every keystroke in an EHR is recorded with a time and date stamp, alterations should not be made to the EHR after a claim or lawsuit is asserted without first talking with an SVMIC Claims Attorney or defense counsel. Any amendments, supplementation, corrections, and/or addendums made after an adverse event will likely be viewed suspiciously and as self-serving. It should be remembered that the plaintiff's Forensic IT expert(s), who will be reviewing the metadata (audit trail), will do so at a much later time,

typically, during the discovery process prior to trial. If a correction to the EHR should be made for continuity of care purposes and there is no claim or lawsuit pending or threatened, these corrections should be made in the same manner as with paper charts, i.e. clearly identifying that it is a correction/supplementation, the reason necessitating the change, the date, and who made the change.

Additionally, EHR documentation should be performed contemporaneous with the event or as close thereto as possible. The audit trail will reveal the time differential between the event and the recording of the event. If significant time is allowed to elapse, the accuracy of the provider's documentation may be called into question.

Audit trails can also be used by hospital administration and law enforcement authorities to determine if a healthcare worker has improperly accessed a patient's records. Laws are firmly in place that protect patient confidentiality and guide healthcare administrators and staff as to the ethics and legality surrounding proper access and disclosure of medical records. Under HIPAA, generally, a covered entity may use and disclose protected health information ("PHI") for its own treatment, payment, and health care operations activities. If a healthcare worker has accessed a patient's records for any purpose other than one of these three authorized uses, and it is discovered through a review of the audit trail (whether it is discovered by routine audit or patient complaint), the potential consequences for the provider can include one or more of the following: employment termination, an ethics investigation, a civil lawsuit, and criminal prosecution.

If a provider shares his or her log-in information with a staff member or permits someone else to sign an EHR electronically using e-signature, it will appear from the audit trail that it was the provider who accessed the EHR or signed the record. This could be problematic in a claim where the record is in question. It could also be a violation of third-party payer contracts.

Alerts or pop-up warnings are also unique to EHRs and are utilized as a means of calling attention to something in the patient's record. These warnings can relate to such things as: allergies, medication dosages and interactions, follow-up needed, etc. Their purpose is to assist the provider and staff to deliver better, safer care by acting as a safety net to remind the provider/staff of important information regarding the patient. However, the number and frequency of these alerts/warnings can often become unduly burdensome. The result can be that the provider/staff develops "alert fatigue/numbness" and ignores the alert warning or deactivates the alerts altogether. The better practice is to manage the alert settings. In the event an alert is routinely disregarded, the practice should evaluate the purpose of the alert and, if appropriate, work with the EHR vendor to modify the alert as needed to make it more useful.

When a provider believes there is not a good medical justification for adhering to the recommendations of the alert, the provider's reasoning should be documented in the patient's chart. Alerts should be used to flag a patient's medical record to draw attention to needed follow-up in the event a different provider sees the patient at the time of the next visit.

An additional concern unique to electronic records is that printouts of the EHR can sometimes differ significantly from the image that is on the monitor screen being viewed by the provider. This can create problems and cause a record to be suspect when a patient or his/her attorney requests a hard copy printout of the medical record. Practitioners and staff should be familiar with what information is and is not printable from the EHR. If a patient, representative or attorney requests copies of the EHR, the hard copy should be reviewed to insure it is complete and any discrepancies noted prior to forwarding the information to the patient/representative/attorney. You should contact an SVMIC Claims Attorney prior to responding to any medical records request if you suspect that a claim or lawsuit may be forthcoming.

Finally, with respect to EHR systems, it is important to keep the focus on the patient and not on the screen. Many patients do not understand why their provider spends more time focused on the computer screen rather than on them and their condition. It is often beneficial to involve the patient in the documentation process by reviewing the prior notes in the EHR, allowing the patient to view the screen as new information learned from the visit is added and explaining how the system works. When the purpose and capabilities of an EHR system are explained to patients, it helps the patient who is attached to paper files become less apprehensive about the EHR and lessens the possibility that the patient will feel ignored.

While electronic communication has revolutionized the care provided within healthcare, it is important to remember the risks involved and how to mitigate them. Moreover, the primary focus should always be on the patient. Maintaining a good physician-patient relationship often will be the best defense to prevent a malpractice claim or lawsuit.
