The Audit Trail and How It Affects You

Like most technology, it can help or harm you.

BY LAWRENCE F. KOBAK, DPM, JD

What is an "audit trail"? This refers to electronic health records. These records permit the preparation of when the record was accessed, who accessed it, and what actions that person performed concerning the integrity of the records. In short, the audit trail is the "digital fingerprint" of everything that occurred with your EMR. This would include the time the healthcare provider accessed the x-ray results or blood test results, and the exact time that the surgeon prepared the operative report.

Think of the audit trail as a sort of body camera that records the work you do and everyone else in your practice with access to protected health information. Either Big Brother is watching, or you can use this technology to protect yourself.

HIPAA and the Audit Trail

Under 45 C.F.R. §164.312(b), healthcare providers must provide a means that "record and examine activity in information systems that contain or use electronic protected health information". Yes, HIPAA is describing your EMR! Your EMRs generally can provide audit trails for tracking your orders, such as prescriptions, your patient notes, patient vital signs such as pulses, access to who viewed whatever module of your EMR or what patient record was externally released to. The implications are profound.

Malpractice Implications

During the discovery phase of a medical malpractice suit, the attorney may demand copies of the audit trails that can be generated by your EMR for the patient in question. The judge will likely require it. However, the request must be specific and must not be too broad. Not producing this information can result in serious sanctions or loss of the case.

The audit trail is the "digital fingerprint" of everything that occurred with your EMR.

Having a HIPAA-compliant audit trail should allow you to catch security breaches. Your IT people should have access to this trail. They should alert you immediately if any untoward access occurs. Your EMR should allow you to work with compliance management software, if you do not already have that as part of your EMR. Data breaches of personal health information can be expensive and very time-consuming. Like most things, preventing or catching it early is highly preferable. How to handle a data breach is beyond the scope of this article.

Let's look at some examples of how this can play out. You are being sued for professional negligence. They are alleging that something was changed in the patient records report to reflect that a particular post-operative event occurred that was not reflected in the records, when the final

Continued on page 44

Audit Trail *(from page 43)*

"version" of the records was provided. The audit trail will be able to show precisely who accessed those records, the actual date they were accessed, and what the patient's chart said or did not say on the date in question. If the chart was changed, a record of that change will show. It will also reveal who accessed the chart to change it and what verbiage was added or subtracted.

Remember, this is a two-edged sword. It will prove the record was changed or it will substantiate the content of the original, unchanged record. Alternatively, it might substantiate a legitimate change made at a later date, known as an addendum.

Let's vary the situation. The gist of the medical malpractice action involved the allegation that the healthcare provider ignored the implications of a blood test that revealed that the patient had a substantially elevated blood glucose level. The audit trail will reveal the date the result was logged into the EMR. It will also reveal the date and time that the healthcare provider added any notation as to what occurred because of that elevated blood glucose level. It will also reveal which provider provided the relevant content of the notes. If a detailed paragraph concerning the diet restrictions and possible dire consequences of ignoring the blood test results first appears to have been inserted later without an appropriate justification, that may be considered fraudulent.

Medicare and Medicaid can validate your medical records.

The patient is claiming that they called your office one week after the surgical procedure to tell you that the incision was oozing and smelled terrible. Your records reveal no such phone call. While your phone log/audit trail might reveal the patient's phone number, short of the phone call being recorded, we cannot know the content of the call. Of course, if the call was simply about rescheduling an appointment, somewhere in the electronic appointment book, the log would demonstrate an appointment change was made and the date that the change was made, and by whom. This can get far down in the weeds.

In every one of these situations, a well written and reasoned medical record would serve to protect you.

Insurance Audit Implications

Medicare and Medicaid can validate your medical records. If you

Continued on page 46

Audit Trail (from page 44)

claim that your patient's chart was signed contemporaneously, the audit log will show that it was signed by you (or not). It will also show exactly when it was signed. If it was signed a year later, that will not go well. Of course, most EMR programs will not allow you to close/complete an unsigned note. If proven by the audit trail that you often signed your charts only after you were being audited, the Medicare audit could have more implications than just asking for money back.

If your patient gives private insurance permission, they should also be able to gain access to your audit log. They could use this as a tool to prove fraud and abuse. Do not make it worse than it is.

Professional Discipline

Your patient can always ask for their audit trail. They can use this information to hurt you with your state's board of professional discipline. Also, your state board should be able to access the audit trail of a complaint that involves your patient. So far, most states, to my knowledge, have not done that. They have limited resources. In an egregious allegation, I imagine, they would. As an example, a state board is tipped off that a practice is billing for EDGs without performing them. The results appear to be the same exact numbers, a statistical improbability. The practice submits copies of the EMGs and the numbers are all different. The state board is still suspicious as the source appears to be very reliable and in a position to know (a disgruntled former employee). If they access the audit log of a sample number of patients, they will see that the numbers were tampered with. They will also see who tampered with them.

Often the complaint against the provider involves information that the "doctor never told me." Again, a complete medical record, including noting the implications of lab results, radiology, the reasons for prescriptions, etc. will allow the audit trail to protect you.

Common Problems

Many medical practices do not make known to their staff what needs logging. Neglecting to record a patient phone call, abnormal lab results, another provider's prescription, a patient's hospital admission, a missed appointment, a patient failing to follow instructions, can make a tremendous difference in the continued success and viability of your practice. A phone call from a patient involving a social matter such as an invitation to a community picnic may not need to be logged into your system.

Neglecting monthly or quarterly reviews of medical records is asking for trouble. There are professional charting auditors who will review charts at regular intervals to find areas that need improvement. They are generally very cost-effective. Alternatively, the providers in your practice can review each other's charts periodically. Remember, a longer chart is not necessarily a better chart. Also remember, stating you do not have enough time to prepare complete charts is not an excuse that will fly with any of the authorities.

Conclusion

Electronic medical records give you the ability to generate audit trails of your practice. You have the option of ignoring its implications, or you can diligently use it to protect your practice. Like most technology, it can be destructive, or it can be quite useful to you. The choice is yours! PM

5 "No-Nos"

1 Forgetting or declining to update your EMR software can lead to data compromise. As poaching of data continues to become more sophisticated, your software must be updated to keep pace. Continued training on that software for your staff is also very important. All the improvements go to naught if your staff has no idea how to make use of it.

2 Inadvertently turning off the audit trail during an update will result in lost data during the time of the shutoff. The lost data could be crucial to your defense in an insurance audit or medical malpractice case.

3 Manual data edits, such as an addendum or correction of a mistaken observation, performed in administrative override mode, will result in lost data. This can be looked upon with suspicion by the investigation authority.

4 Correcting clinical data without giving the reason for the change.

5 Giving unlimited access to the audit trail. An example of this is the failure to remove access to former employees. Besides the HIPAA implications, do you really want a "disgruntled former employee" access to personal health information and practice data? Think of the harm that could be done. PM

Dr. Kobak is Senior Counsel in Frier Levitt's Healthcare Department in New York. Larry has extensive experience representing physicians in connection with licensure issues, as well as successfully defending physicians before Medical Boards, OPMC, OPD investigations, as well as Medicare Fraud, Fraud & Abuse, Hospital Actions, RAC Audits, Medicare Audits, OIG Fraud, Healthcare Fraud, Medical Audits, and Health Plan Billing Audits. As a licensed podiatrist prior to becoming an attorney, he served as the international president of the Academy of Ambulatory Foot and Ankle Surgery.