In the rush to meet meaningful use guidelines, physicians may have won the battle but lost the war as poor or faulty implementation of EHRs increases risk.

Source: Physicians Practice

Here are a couple areas of emerging risk we are seeing for EHRs – and areas physicians should take note of to address and correct.

1. **Partial implementation.** We are seeing a lot of smaller physician practices — and even some larger ones — who have not fully completed implementation. They may have gotten up to R or S in patient files, but aren’t done. Or they may have started with the new files but haven’t gotten to the old files yet. This can present a problem in the event of a claim involving a patient record that has not been fully transferred to an EHR or where there is only partial or lost data.

2. **Errors in implementation.** I’m sure someone has done the math, but consider the sheer amount of data America’s doctors have transferred from paper to electronic records over the past few years. Technology is only as good as the humans guiding it and understandably there are lost records, missing records, records that were illegible and didn’t transfer electronically, etc. The problem arises when there is a potential claim and data confirming a test was done or a call made to a patient) or some other action vital to the defense of a claim) … and the data to prove that action is not available or is incomplete. The burden is on the plaintiff and if proof isn’t there, it becomes more difficult to launch a defense.

3. **Know who is on first (and second and third).** As I noted in an earlier blog post, one area physicians need to understand if they have recently joined a large hospital or medical group is who is at risk in the event of a data breach or HIPAA error. In many cases, the physician will be held liable for staff errors. In a larger group setting where the physician has limited control over personnel, the physician is in a "Catch 22" situation. Understand ahead of time what data security policies are in place, who is responsible for training staff (and physicians), and the extent of the physicians’ liability.

4. **Remember what goes into the EHR, may not stay in the EHR.** Keep in mind that everything you put in the EHR becomes discoverable evidence in the event of a claim. If you add a comment that testing is needed — and it is not followed up on — you are at risk. If you note something potentially perceived as derogatory about a patient, it could become public. Be as complete as possible in your charting — because it can protect you — but always remember that anything and everything you put in the patient record has the potential to become public.

5. **Lack of a plan for data security and breaches.** Many physicians’ offices are just now becoming familiar with their EHR. And while some may have developed policies and procedures, for many because it is all so new, there are opportunities for mistakes. For example, someone leaves the computer on in an exam room and then next patient in the room can see the previous’ patient’s medical record. Or the more common mistake, someone takes a laptop home that contains patient records and it becomes lost or stolen. All of these actions while simple, can result in considerable exposure and cost to the practice.

6. **Invest in systems to back up and protect your data.** Physicians are facing considerable financial pressure these days. Cutting back on technology and services to store and protect data is not a way to save money. You could increase your risk not only of problems, but a zealous attorney might also look at your data storage and security provider and if there were problems in the past, bring those up in the event of a claim. For your own peace of mind and more importantly to protect your data, invest in security.

The above is meant to be cautionary — not predictive. By and large, EHRs can go a long way to
reduce malpractice risk by documenting what was communicated to whom, when, etc. They will increase efficiency, improve care coordination, and provide many other benefits. The key to EHR success is to recognize fully how they work, train staff on HIPAA and privacy guidelines often, and work to ensure you have done a stellar job of implementation.

Source URL: http://www.physicianspractice.com/blog/ehrs-can-be-risky-business-physicians

Links: