Dev Raheja & Maria C. Escano, M.D.

Electronic Health Records: Dangers for Patient Safety

Electronic health records (EHR) are critical to precision medicine. They provide greater patient access to medical history data and are available quickly. But there are many inherent risks in using these records.

According to a new study, even in long-standing EHR systems such as the one used by the Department of Veterans Affairs (VA) health care system, many significant EHR-related safety concerns remain. In a study of investigations of EHR-related safety violations launched through the VA's Informatics Patient Safety office (IPS) from 2009 to 2013, researchers looked at 100 closed cases at 55 VA facilities. Of those cases, 74 involved unsafe technology, and 25 involved unsafe use of technology, which the researchers of the study wrote "most commonly involved the dimensions of people, clinical content, workflow and communication, and human interface." A majority of cases (70 percent) involved both unsafe technology and unsafe use [Ref. 1].

This particular study points out many risks, including:

- Risks related to software modifications. These issues center on the intended and unintended consequences of software upgrades or improper software configuration.
- Risks related to system-to-system interfaces. Concerns in this area have to do with the ways systems communicate with each other, and the possibility of one patient's records being mixed up with another's.
- Risks of hidden dependencies. Seemingly unrelated components of an EHR affect each other, such as the re-assignment of a patient from outpatient to inpatient status, resulting in the removal of certain medications from the patient's active medication list.

The study suggests that technology-based solutions alone will only partially mitigate concerns, and that interventions to improve EHR-related safety should encompass the people, organizations, systems and policies that influence how EHRs are used.

There are many other risks that need to be understood, as well, including cases where data entered into the opening screen may fail to populate the fields of other screens correctly, or authorized software upgrades may alter the presentation of historical data that was entered [Ref. 2].

The Health Insurance Portability and Accountability Act (HIPAA) states that the healthcare provider is the covered entity responsible for maintaining the integrity of the patient's medical record. If a doctor finds bugs or flaws, he or she should contact the vendor and insist that the glitches be fixed. Vendors may be more responsive than many doctors assume.

Many doctors complain that an EHR slows them down. To regain some of that lost time, they may use shortcuts, such as "cutting and pasting" lengthy patient histories from one electronic chart to another. The problem with that practice, however, is that incorrect or outdated patient information may be copied from one record to another. Sharona Hoffman, J.D., Professor of Law & Bioethics at Case Western Reserve University School of Law in Cleveland, Ohio and an expert on the potential pitfalls of EHR use in liability suits, has said that copying and pasting information from one electronic record to another is among the worst things you can do, both clinically and legally. "It seems to be happening at a fever pitch today," she said.

Physicians can expect criminals to increasingly target their EHRs for patient information that they can sell on the black market. Identity thieves can use patient data to obtain free medical care, including prescription drugs, or to open new credit accounts. They also can use pilfered information about a physician to file bogus insurance claims.

Clinical decision support (CDS), which includes drug/drug alerts and drug-allergy alerts, can be annoying to many physicians. Too many unending streams of alerts, many unnecessary, can be irritating. As a result, some doctors click through alerts with barely a glance, override them or set higher thresholds that trigger a

reduction in the number of alerts. Most EHRs can be customized, which has its own risks. A doctor can bypass the way the EHR is designed to have information entered. Instead of checking off a box that indicates that the patient is allergic to penicillin, he or she puts that into a note. The system may not be smart enough to figure out the note indicating that the patient is allergic to penicillin.

What Needs to be Done?

Healthcare is a system of systems, and should be treated as such. It is a collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new, more complex system offering more functionality and performance than simply the sum of the constituent systems. A matrix of which resources affect other resources helps in monitoring the effects of changes anywhere. In addition, system safety analysis methods can be used to identify many unknown risks [Ref. 3].

Robert Rowley, M.D. [Ref. 4] has suggested some fixes, which include:

- Brainstorm how to create safe chart notes
- Brainstorm problems and solutions on medication refill handling
- Brainstorm problems and solutions referrals to outside practices
- Brainstorm problems and solutions on scanned document management

References

1. American Physical Therapy Association. "EHR and Patient Safety: A Real Danger, Even for Experienced Users," *PT in Motion News*, June 24, 2014, http://www.apta.org/PTinMotion/NewsNow/2014/6/24/EHRPatientSafety/.
2. Chesanow, Neil. "8 Malpractice Dangers in Your EHR," *Medscape News and Perspective*, August 26, 2014, http://www.medscape.com/viewarticle/828403.
3. Raheja, Dev. *Safer Hospital Care: Strategies for Continuous Innovation*, CRC Press, 2011.
4. Rowly, Robert, M.D. "Explore Fixes to Your EHR System Before Deciding to Replace It," *Medical Economics*, April 10, 2013, http://medicaleconomics.modernmedicine.com/medical-economics/RC/tags/ehr/explore-fixes-your-ehr-system-deciding-replace-it?page=full.