Computers are everywhere, from the business world to the healthcare industry. Computer technology has, in many ways, facilitated processes that would otherwise be cumbersome; however, they also carry their own risks and hazards.

The American Recovery and Reinvestment Act of 2009 allocated $19 billion for incentivizing medical practices to adopt and implement electronic health records (EHR), also known as electronic medical records (EMR). To qualify for incentives, physicians and hospitals must use certified EHR technology in a "meaningful manner" in three defined stages in 2011, 2013 and 2015. Since the first deadline is quickly approaching, hospitals are now rushing to buy various EHR systems.

The Center for Medicare and Medicaid Services defines "meaningful use" as using an EHR for the objectives listed here [Ref. 1]:

- Improving quality, safety, efficiency, care coordination, population and public health
- Reducing health disparities
- Engaging patients and their families
- Ensuring adequate privacy and security protections for personal health information

What are the issues?

EMRs were created to supposedly increase efficiency and reduce medical errors. Medical records, such as discharge summaries, consultation reports and laboratory data, are readily accessible, even from many years back, without having to dig through multiple charts from the medical records department. During order entries, EMRs can provide automatic warnings for physicians about potential drug interactions, overdosing and allergies. Considering the numerous medications some patients are on, this is a valuable addition to reducing medical hazards.

However, EMR systems need to be regularly updated with new information and fine-tuned to carry over information from one part of a medical record to another to avoid multiple alerts for the same thing, which can actually delay medical care. A majority of alerts are overridden, according to Ross Koppel, faculty member at the University of Pennsylvania's School of Medicine. He claims that experienced physicians sometimes find alerts annoying and intrusive [Ref. 2]. Some programs also do not allow simultaneous access of patient information while entering orders, which can make this process time consuming. For example, if a drug can potentially cause elevated potassium levels, the system should allow easy data access to the patient's latest blood potassium level without having to abort the process.

60 at a second hospital treatment plans are not standardized, alerts are sometimes triggered differently at different hospitals, even for the same medications. Ross, who also works with many residents, adds: A resident will get an alert at 50 mg of a drug at one hospital, 60 at second hospital and no alert at all at a third hospital because staff turned it off. Sometimes, the residents don't even know if the alerts are on or off.

A new issue is hazards resulting from the interactions of new technologies. One major concern is cloud computing. Cloud computing is getting a lot of attention from EMR vendors. It is the ability to run applications, store data and access the applications and data from any computer that is connected to the Internet. Organizations utilizing cloud computing can run applications without having to worry about servers, installing software or upgrading the applications. They do not have to perform daily data back-ups, since backups are handled "in the cloud." When you look at this model, it has a lot of appeal [Ref. 3]. With cloud computing, all the software updates can be made in the cloud instead of on hospital computers. The hazard for hospitals is that they are helpless when an
application from the cloud becomes unavailable. Hospitals may not be equipped with back-up systems, and if a patient file is not available for hours, it can cause serious harm. Jeff Marion of Healthcare IT News and Healthcare Finance News [Ref. 4] says: “More and more health care providers are choosing cloud-based EHR models, opting to let hardware installation, data storage, and application hosting be someone else’s headache. The healthcare industry has long been uncertain as to whether confidential patient records should be stored centrally or in the cloud. Opponents challenge cloud computing as a new and unproven technology, warning that rapid adoption could result in disaster.”

There are also many other issues to consider, including reliability of EHRs [Ref. 5]. The failure rate of EHR implementation is close to 50 percent — 19 percent of EHRs have been uninstalled, and 30 percent are not being used by some physicians. The reasons are varied. Some EHR systems are not user-friendly. Some require multiple entries of the same patient information (e.g., patient allergies) instead of automatically carrying the information over, which delays care. Another barrier to reliability is the need to access different programs for the same patient. Some hospitals utilize one program to input vital signs and daily intakes and outputs, but then another program must be used to enter discharge summaries and progress notes. Yet another program may be used to access imaging studies such as X-rays and CT scans. Ideally, there should be a centralized information system that makes systems “talk” to each other and allows seamless access of patient information and provision of safety alerts as appropriate. Industry experts estimate that failure rates of EMR implementations range from 50 to 80 percent.
Examples of EMR Hazards

Scanned images of EKG charts and MRIs have resulted in misdiagnosis or delayed diagnosis. Dale Sanders, chief information officer at Cayman Island Health Authority, is an experienced user of EHRs, with 13 years in the trenches at various health organizations. He does not agree with the FDA’s estimate of only 44 HER-related deaths in the last two years. He believes that the number of deaths including undesired safety scenarios is at least 100 times the FDA estimate [Ref. 6]. He cites examples such as missed and inappropriate diagnosis of congestive heart failure, the death of an infant from a software error that caused the fetal monitor to stop generating local audible alarms, the death of a young mother because the radiology information system failed to file a cancer tissue report properly, and extensive kidney damage suffered by a patient because of lack of test results from the lab’s computers.

Sanders also offers the following response related to him by a physician as follows:

"One safety issue I struggle with on a daily basis is the integrity of my EMR medication list. Recently one of my patients was treated in the ER and admitted. When the nurse contacted a covering physician, she read from an obsolete EMR list of meds from a previous admission. Of course, they were wrong. The patient had an accurate list in his wallet but no one asked him. When he was discharged to rehab, the facility changed his meds again for formulary reasons. Several weeks later, the patient was discharged with a new med list and a computerized list of medications. Unfortunately, he was overdosing on medication because he was taking both the generic and the brand version of the same drugs. After much confusion, the med list was finally corrected in my office EMR. One month later I was asked to refill a prescription that was unknowingly changed by his cardiologist. I unknowingly filled the wrong dose. I still ask patients to bring in all their meds when they visit the office and I never trust the EMR med list."

Hospitals do need to evaluate the reliability and safety of EMRs. A knowledgeable and experienced team needs to proactively assess the reliability and safety of these EMR systems. We have covered several such tools in Journal of System Safety [Ref. 7, 8 and 9]. A cross-functional team can easily come up with over 100 hazards that need to be mitigated in EMR software as well as in the hospital’s own processes. Another approach a hospital can take is to collect failure modes found by other hospitals through professional networks and through Internet searches. This must be done before investing in the EMR.

An advisory panel of the Department of Health and Human Services has proposed creating a national database into which clinicians could report patient data errors and unsafe conditions they encountered in their use of electronic health records. Clinicians could use the system to report instances — noticeably inaccurate patient data or an EHR technical glitch, for example — that they believe might compromise patient safety [Ref. 10]. The group also suggested establishing an organization that could oversee a nationwide EHR safety system and provide other methods for reporting, analyzing and disseminating incident reports.

The solution is complex. Some of the following strategies below may be helpful:

- Have a cross-functional team perform hazard analysis for potential hazards
- Establish criteria for decision making
Analyze security breaches or failures that affect patient safety (e.g., HIPAA, wrong patient data, loss of data)
Analyze sources of downtime that affect patient safety
Question EHR vendors on safety functionalities. Establish the need for filters that will differentiate between high-severity alerts and low-severity alerts. Consider not allowing anyone to shut off high-severity alerts by design
Make sure technical support is readily available with a rapid turn-around time
Don't focus on price alone. If safety improvements are needed, be willing to pay now to save a lot more later
Include alerts as part of hand-offs

What can patients do?

Some patients’ medical histories are complex, and they often require visits to different specialists and hospitals. Medications need to be adjusted and diagnostic tests need to be performed. It can be difficult to track these changes; patients can take ownership of their own safety by taking a proactive role and carrying a current list of their medications at all times. During an emergency, they can end up in a different hospital that may not have prompt access to their medical records. One patient not only had a list of his medications but also his medical history and surgeries. Another patient had a list of all his physicians, including their contact information.

Computerized systems, such as electronic medical records or electronic health records, have revolutionized the healthcare system in some ways, but have created new headaches and problems in others. After all, the computer is not the healthcare provider, and it is limited by the quality of the data that it accumulates. These systems are not perfect and when they fail, serious hazards can occur. In some hospitals that don't have back-up systems in the event that the computer system crashes, serious consequences can occur. Healthcare delivery is a complex process, and we can all proactively contribute to making it safer.

References: