Pharmacy Automation and Technology

Health Information Technology Risks, Errors, External Threats, and Human Complacency

Bill G. Felkey, MS,* and Brent I. Fox, PharmD, PhD†

It may seem that our position is one of unwavering support for all things health information technology (HIT). However, we like to believe that we are cautious and deliberate in our evaluation of HIT. This month, we explore some of the common overt and covert challenges to optimal use of HIT.

We admit to being unabashed technology enthusiasts. We try to be found in the group known as early adopters and want to be known as the Underwriter Laboratories evaluators of all things health care technology. Here is the other side of the coin that we don't always take the time to think about. To err may be human, but we have to remember that the information technology (IT) systems designed to make our patient care processes safer, more efficient, and effective can also pose serious risks and actually be the cause of errors. The Joint Commission has just issued a second alert about potential health IT risks.

All technology requires appropriate operation within a safe workflow that acknowledges the risks that are present in any machine–human interface. Errors that are traced back to technology still fall within an error of omission or commission category. An error of commission (doing something wrong) can unwittingly occur because, for example, an order entry software application happens to transmit orders literally rather than ascertaining what the prescriber intended. For example, the order of several medications was begun by a prescriber at 11:52 p.m. One of the medications was intended to be administered at 8:00 the next morning. The prescriber selected the proper instructions from the pulldown windows provided by the software but executed the order at 12:03 a.m. This created a wrong time error by delaying the medication administration by an additional 24 hours. An error of omission (failing to do the right thing) can be perpetuated by technology when, for example,

an automated dispensing cabinet opens a drawer and presents a single injectable product that is, in fact, the wrong strength because the cabinet was improperly stocked by a pharmacy technician.

We used to say that if we are able to read it in print, you can believe it. Today, technology sometimes gets the same halo effect when health care clinicians assume that the technology eliminates the need for human verification. We call this complacency, and errors related to the use of technology can multiply a single opportunity for an error into a much broader and potentially deadly situation in which a thousand errors can take place before being discovered. System errors that might include an improper coding of a barcode, corrupted data files, corrupted software coding, and corrupted calculation formula can create a ripple effect of errors through an organization when clinicians fail to use their higher level judgment along with the health IT they employ. One example of a calculation error that we encountered involved a pharmacy operation that used a flawed pricing formula over a 3-month period. This calculation error resulted in a \$4.3 million shortfall of revenues for the pharmacy.

It's not surprising that computerized provider order entry (CPOE) can be designed in such a way that it promotes better safety or opens the door for error. For example, when prescribers search for a drug product directly by name, it is possible for them to order a medication that is contraindicated and/or not indicated for the condition being treated. One interface option would be to begin the drug search

*Professor Emeritus, Auburn University, Auburn, Alabama; †Associate Professor, Department of Health Outcomes Research and Policy, Harrison School of Pharmacy, Auburn University, Auburn, Alabama

with the indication being treated, and then only those medications that are appropriate for that indication would be displayed as a prescribing choice in the CPOE system. We also know that clinical decision support systems (CDSS) can alert prescribers of inappropriate behaviors within focused categories that are contained in 21 decision support modules. Unfortunately, false positive flagging and too frequent generation of alerts creates an irritating situation called flag fatigue. Flag fatigue can prompt the deactivation of many levels of CDSS alerts by prescribers. We have physician friends who inform us that they count the number of “clicks” they have to perform to complete a transaction and judge the quality of every clinical software by this count.

We’ve already mentioned automated dispensing cabinets and CDSS that pose risks when they are managed inappropriately or receive inaccurate data entry. We also need to be on guard for virus and malware threats to the information security of the automation we use. This is a battle that will probably never be completely won. Information security is more like a tennis match. The chief information officer and IT team beef up the security of the health IT system and then hit the ball over the net. The barbarians at the gate receive the ball and modify or alter it until it becomes a threat and then head it back over the net. And so the game goes on, with ever-increasing levels of protection needing to be added to systems.

The newest push with technology is the effort to produce a connection with patients and their caregivers in such a way that self-care management and patient engagement takes place. The ironic part of this desirable goal is that each portal, personal health record app, social media venue, and mobile device creates new threats to health IT systems. Health information exchange initiatives and interoperability demand for each patient handoff in the continuum of care come with system vulnerability issues. Before you believe that all is lost, we can tell you that this is all part of the health IT adoption process. The use of technology will always bring inherent risks. We believe that the benefits that can be achieved by this process outweigh these risks.

We invite you to be the squeaky wheel in this process. Make sure your technology vendors are made aware of system vulnerabilities, and always keep your high-level judgment and verification processes churning. We believe that most clinicians, after going through the growing pains involved with health care becoming a digital field, will not desire to go back to a paper-based system. We hope that your old processes are already positioned as being the “Stone Age” way of doing things. We invite you to let us know your thoughts and comments and welcome any questions you might have. You can reach Bill at felkebg@auburn.edu or Brent at foxbren@auburn.edu. ■