



Health Information Technology: Understanding the Risks

Health information technology (HIT) and “converging technologies”—the interrelationship between medical devices and HIT—are increasingly being adopted by health care organizations. HIT is found almost everywhere in a health care organization, from medical devices, electronic health records (EHRs), medical billing, and scheduling software, laboratory test reporting, diagnostic imaging, and so on. Further, the information generated by HIT is increasingly interconnected to provide efficient, seamless care across the health care continuum (converging technologies).

“Those who have been working in patient safety have been waiting for IT to enter our world for many years,” says Robert M. Wachter, MD, author of the recent *New York Times* science bestseller *The Digital Doctor: Hope, Hype, and Harm at the Dawn of Medicine’s Computer Age*. Wachter is interim chair of the Department of Medicine and chief of the Division of

(continued on page 10)



Careful implementation of health information technology is essential to ensure patient safety.

Hospital Medicine, University of California, San Francisco. “Health IT has certainly improved certain things, and I believe care is generally better and safer than without it.”

Wachter explains that using HIT can help health care organizations avoid several common types of errors. First among them: Using a computer system can avoid errors that arise from misinterpreting a physician’s handwriting. Systems also can give alerts when a patient has a medication allergy. He says, “I can’t tell you the number of root cause analyses I’ve participated in where a computer system could have prevented an error.”

However, HIT also introduces a number of new safety risks and potential for preventable adverse events. Users and patient safety risk managers must be mindful of these.

The Joint Commission recently published a *Sentinel Event Alert* that directly addresses the implementation of HIT. This article will discuss the risks associated with HIT, as well as solutions to mitigate those risks, including compliance with Joint Commission standards. (A list of relevant Joint Commission standards, by accreditation program, is available at http://www.jointcommission.org/assets/1/6/SEA_HIT_Requirements.pdf.)

HIT–Related Adverse Events

Technology-related adverse events can be associated with any component of a comprehensive technology system and may involve errors of either commission or omission. For example, scanning a medication into the wrong patient’s record could result in the wrong patient receiving that medication. On the other hand, if a medication fails to scan

into a patient’s file due to a scanner error, the patient might not receive needed medication.

These unintended patient safety events typically arise from the design of the human–machine interfaces or processes and workflows associated with the technology. The overall safety and effectiveness of technology in health care ultimately depends on its human users, ideally working in close concert with properly designed and installed electronic systems.

Types of HIT Risks

Sentinel Event Alert #54: Safe Use of Information Technology identifies eight socio-technical dimensions that affect HIT. They include, in order of their frequency, the following ¹:

1. Human–computer interface (ergonomics and usability issues resulting in data-related errors), such as selecting the wrong option from a drop-down menu
 2. Workflow and communication (issues related to HIT support of communication and teamwork), such as the integration of a system into the process of care
 3. Clinical content (design or data issues relating to clinical content or decision support), such as nurses and physicians not having access to the same parts of the medical record
 4. Internal organizational policies, procedures, and culture
 5. People, such as lack of training or failure to follow established processes
 6. Hardware and software
 7. External factors, such as those originating from the vendor
 8. System measurement and monitoring
-

All of these are important to consider when assessing HIT risks, and in some cases they can interact to create a risk. For example, a pharmacist may have two patient records open simultaneously, get distracted, and enter a medication order into the wrong file. This case might involve a combination of human–computer interface, internal policies and procedures, and failure to follow established processes.

HIT risks can be roughly divided into two sources: human or process related and technology related.

Human- or process-related errors can take many forms. Data may be entered incorrectly, such as into the wrong file or due to a typographical error, or not at all. Alerts may be ignored or overridden. The wrong bar code might be scanned, or the right bar code scanned into the wrong place, or the wrong choice selected from a menu. Test results or images may be sent to the wrong provider, resulting in delay of care. A user may not know to scroll down to see vital information. Some of these problems occur because the user is not familiar with the technology, others as a result of the user being distracted or interrupted.

“One major risk is alert fatigue,” Wachter says. “There can be thousands of alerts, and people learn to tune them out, which negates their purpose.”

Technology failure includes those events that originate with the machines themselves. Software may be out of date or have glitches. Data may not display properly or be difficult to read. Network connections may be slow or down completely, resulting in lost data or delay in care. Security breaches, such as viruses or malware, can not only compromise the system integrity, but require services to be off-line while security is reestablished. Even a keyboard with a sticky key or a mouse that is set to move the cursor too fast can result in errors. Technology failures may be caused by power interruptions, connectivity and data transfer issues, and/or faulty software or hardware.

Recommended Actions

In *Sentinel Event Alert #54*, The Joint Commission suggests approaching HIT risks from three angles: safety culture, process improvement, and leadership.

Safety Culture

Joint Commission standards require organizations and their leaders to operate in a safety culture. This includes an organizationwide awareness of and shared responsibility for HIT-related risks. Staff should feel safe to report any HIT-related concerns without fear of retaliation or censure. For example, if a particular software program is confusing to use, staff should be encouraged to ask for help and/or bring the issue to leaders’ attention.

Wachter explains that this can be very difficult. IHT

systems involve large investments of time and money to purchase, implement, and train staff to use them. These factors can get in the way of objective analyses of a system’s real-world functionality, which can impact patient safety.

An established reporting system is crucial to a safety culture. Staff should be familiar with the process for reporting instances of HIT-related hazardous conditions, close calls, or errors. Reporting systems should include both internal and external reporting, as appropriate. External reporting, which can include patient safety organizations, governmental agencies, and vendors, contributes to data aggregation efforts that aim to improve safety on a large scale. All reports should be recorded for data analysis and performance improvement purposes.

Instances of adverse events related to HIT should be treated as opportunities for learning and problem solving. In cases in which patient harm occurs, a comprehensive systematic analysis should include HIT issues as a potential contributing factor. Because HIT factors may not be readily apparent, the analysis should include all eight dimensions as described earlier in this article.

Process Improvement

Ideally, HIT risks should be identified and addressed before they result in patient harm. Health care organizations are required by Joint Commission standards to have plans in place to manage clinical information and support patient safety through performance improvement activities. Proactive identification of HIT risks and development of process improvements might use a failure mode and effects analysis (FMEA), the SAFER Guides created by the Office of the National Coordinator for Health Information Technology [ONC]), or other methods.

HIT risk assessments should include analysis of three areas. First, HIT hardware and software must be free from malfunctions. This includes analyzing processes such as the following:

- Backing up data
- Using standardized coded data elements
- Creating evidence-based standard order sets for common conditions, procedures, and services
- Training and testing of staff on use of a system before it goes live, and afterward as appropriate to ensure consistently high performance.

Second, clinicians, staff, and patients should be able to use HIT safely, as appropriate to their role in the health care process. Processes to consider include the following:

- Displaying patient identity clearly and accurately

(continued on page 15)

Health Information Technology

(continued from page 11)

on all screens and printouts

- Limiting the number of patient records displayed on a computer screen
- Providing clinicians with the ability to easily correct accidental clicks, typos, or incorrect drop-down choices
- Allowing patient access to their EHR via portals to help ensure the accuracy of their clinical information

Finally, HIT should be used to monitor and improve safety. This might include review of the following processes:

- Monitoring metrics such as help desk use, system uptime and downtime, and alert overrides
- Engaging both users and vendors in decisions regarding how to improve safety and efficiency of HIT systems


Gerard Castro, PhD, MPH, project director for Patient Safety Initiatives at The Joint Commission, gives an example of a system design that put patients at risk. In this situation, a critical piece of clinical data was not seen by staff because it did not fit on the display screen. In other words, the staff member would have to know to scroll down to see this important information.

“Difficulty in finding critical information is a common complaint,” Castro says. “In this case, the system would benefit from a redesign that puts the most important information at the top of the display.”

Wachter agrees. He says physician notes have become more legible but less useful, because the tendency is to copy and paste large blocks of text that are not conducive to reading on a screen. “It can be very difficult to figure out the essence of what’s going on with a patient.”

Leadership

Organization leaders are responsible for creating the safety culture described earlier, but their involvement in ensuring HIT safety does not stop there. Because HIT involves every functional area of a health care organization, and requires the transfer of data among providers in different departments, organization leaders must provide oversight. Leaders should create and use multidisciplinary teams to gather relevant information that informs decisions on HIT planning, implementation, and evaluation.

“Health information technology is so integral to what we do today,” says Castro, “that leadership must play a role in ensuring that it is working efficiently and safely.” 

Reference

1. The Joint Commission. Safe use of health information technology. *Sentinel Event Alert*, Issue 54. Mar 31, 2015. Accessed Aug 10, 2015. http://www.jointcommission.org/assets/1/18/SEA_54.pdf.