The Office of the National Coordinator for Health Information Technology

Anticipating Unintended Consequences of Health Information Technology and Health Information Exchange

How to Identify and Address Unsafe Conditions Associated with Health IT

November 15, 2013

Authors

ECRI Institute:

Cynthia Wallace, CPHRM

Karen P. Zimmer, MD, MPH, FAAP

Lorraine Possanza, DPM, JD, MBE

Robert Giannini, NHA, CHTS-IM/CP

Ronni Solomon, JD

Prepared for

The Office of the National Coordinator for Health Information Technology

Washington, DC

Prepared by

Westat

1600 Research Boulevard

Rockville, MD 20850-3129

(301) 251-1500

Contract No: HHSP23320095655WC

Task Order: HHSP23337003T

Table of Contents

Chapter	Page
Introduction	1
Health IT Overview	3
Socio-Technical Model	5
Common Health IT-Related Problems	6
Computer-Related Issues	9
Human-Computer Issues	10
Identifying Health IT's Unintended Consequences	11
High-Reliability Organizations' Commitment to Health IT Safety	12
Event Reporting within a Safety Culture	13
How to Collect Health IT Event Data	14
Educating Staff About Health IT Event Reporting	14
What to Include in a Health IT-Related Event Report	14
AHRQ Common Formats for Health IT Event Data	15
Beyond the Common Formats: Hazard Manager	16
Health IT Event and Hazard Analysis	17
Staff Feedback and Monitoring	20
Other Sources of Information for Health IT-Related Issues	20
Reporting Health IT Events to PSOs	20
EHR Developers' Role in Assuring Patient Safety	22
Teaming Up With PSOs	24
Conclusion	25
Resources	26
References	27

Table of Contents (continued)

Tables **Page**

1 What is Health IT? 4

2 Examples of Health IT-Related Incidents 7

Figures

1 Health IT Safety: A Shared Responsibility 2

2 Socio-Technical Model for Health IT 5

3 ECRI Institute PSO Deep Dive Identifies Top Five Safety Issues from Health IT Events 8

4 Continuous Feedback Approach to Health IT System Safety 12

5 Sample Screenshot from AHRQ's Hazard Manager 17

6 Case Study of a Laboratory Event Involving Health IT 19

7 Intended Flow of Patient Safety Event Data and Feedback 23

Introduction

Health information technology (IT) can provide multiple benefits to enhance patient care if the technology is optimally designed by the system developer, thoughtfully implemented by the healthcare organization, and appropriately used by the organization's staff.

Health IT's potential can also be undermined by the hazards created when a health IT system operates in unintended and unanticipated ways.

For example, studies have found that the same health IT systems can have varied results when implemented in different facilities. In its 2011 report *Health IT and Patient Safety: Building Safer Systems for Better Care*, the Institute of Medicine (IOM) cites three studies conducted at different children's hospitals that adopted the same computerized provider order entry (CPOE) system. In one hospital, the mortality rate did not change (Del Beccaro, Jeffries, Eisenberg, & Harry, 2006); however, in the other hospital, CPOE implementation led to a significant increase in mortality (Han et al., 2008). And when that same system was used in several other hospitals, mortality rates either did not change or dropped (Longhurst et al., 2010). According to IOM's report (IOM, 2011), "The differing impact on mortality rates may be due to the hospitals' differences in the implementation and use of the CPOE system."

"Designed and applied inappropriately, health IT can add an additional layer of complexity to the already complex delivery of health care, which can lead to unintended adverse consequences," says IOM.

Adding to the complexity is the challenge of recognizing the technology's involvement in patient safety incidents and near misses—i.e., patient safety issues that are caught before they reach the patient. An electronic health record (EHR) system developer recently notified its customers that a software glitch in its emergency department module prevented emergency physicians' notes about medications from transferring to the patients' charts (U.S. Food and Drug Administration [FDA], 2013). Healthcare organizations may have viewed any incidents that occurred as a result of the bug as a medication omission, unaware that a software defect in the health IT system was at fault.

A recent analysis of health IT-related events submitted by healthcare organizations to a federally certified patient safety organization (PSO) identified many of the common problems that can arise with health IT systems. The challenge for healthcare organizations is to detect the problems before the system is fully implemented. If a particular defect escapes detection, the organization must also have processes in place to identify those problems as soon as possible after the system is brought online.

In short, healthcare organizations must operate as high-reliability organizations to ensure the safety of their health IT systems. Their safety culture should foster a willingness to learn about unsafe conditions with their health IT systems that can lead to patient harm and to make improvements to the systems before accidents do occur.

To achieve their goals as high-reliability organizations in an increasingly wired healthcare environment, organizations must sharpen their internal processes to identify health IT flaws and

make improvements. These processes must be ongoing because new safety risks can arise as software is upgraded and new interfaces are built.

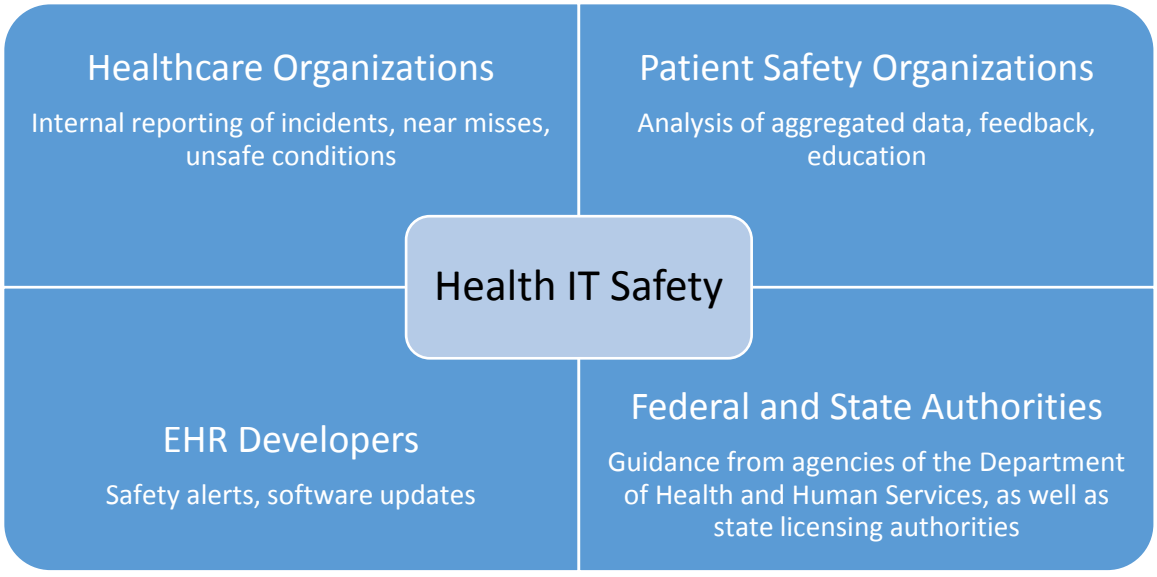
Organizations must also be able to call upon their EHR developers for assistance in addressing unanticipated system faults. As their customers expose the systems to the busy, complex healthcare environment, developers may find that their systems function within that environment in unexpected ways. They must be prepared to work with their customers to correct those bugs.

But organizations should also be prepared to turn to other outside experts as the healthcare sector, collectively, gains experience with health IT and learns about the issues that can arise with the technology, as well as ways to ensure that health IT fulfills its promise of improved patient care. Within the protected and confidential framework offered by PSOs, healthcare organizations can also share with others their experiences with health IT systems to better understand problems that can occur with health IT systems and identify solutions.

Additional guidance on health IT safety is available from federal and state healthcare safety oversight authorities, including various agencies of the U.S. Department of Health and Human Services—the Office of the National Coordinator for Health Information Technology (ONC), the Centers for Medicare and Medicaid Services, the Office for Civil Rights, and the FDA—and state licensing authorities.

Ultimately, a healthcare organization's approach to health IT safety relies on the collective guidance provided by internal and external experts (see Figure 1). Working together, healthcare organizations, PSOs, EHR developers, and policymakers can learn how to achieve the full potential of health IT.

Figure 1. Health IT Safety: A Shared Responsibility



This White Paper is intended to help healthcare organizations lay the foundation for a process to identify health IT hazards, using both internal and external resources. It covers the following:

1. Describes health IT systems and addresses their operation within a complex healthcare environment.

2. Identifies five common health IT problems that can occur within the context of this complex environment and contribute to the unsafe use of health IT systems, leading to potential and actual patient harm.

3. Examines the role of organization's internal reporting systems to identify and address unsafe scenarios for health IT systems and to continually monitor health IT systems' safety and make improvements.

4. Discusses the role of external reporting programs, such as PSOs, in helping to identify areas for health IT system improvements.

5. Reviews the role of EHR developers in working with healthcare providers and external reporting programs to identify and manage health IT system improvements.

Health IT Overview

Broadly defined, health IT systems comprise the hardware and software that are used to electronically create, maintain, analyze, store, or receive information to help in the diagnosis, cure, mitigation, treatment, or prevention of disease (AHRQ, 2013a). For many healthcare organizations, health IT is synonymous with EHR, but it also includes various other components as depicted in Table 1.

Numerous studies support health IT's important role in patient safety. For example, CPOE systems can improve patient safety by eliminating transcription errors for illegible handwriting, providing clinical decision support, and alerting clinicians to potentially dangerous orders, such as a patient allergy to a selected medication (Kaushal, Shojania, & Bates, 2003).

But studies also point to the so-called "unintended consequences" of health IT (Ash, Berg, & Coiera, 2004). Continuing with the CPOE example, studies have documented that, among several possible hazards with the systems, clinicians can mistakenly select the wrong patient file when placing an order in a CPOE system if the computer display is confusing, resulting in a medication order for the wrong patient.

Table 1. What is Health IT?

Health IT involves the exchange of health information in an electronic environment as in the following examples.

Health IT System	Example
Administrative (e.g., medical billing and scheduling, practice management system)	• Coding/billing system • Master patient index • Registration/appointment scheduling system
Automated dispensing system	• Medication dispensing cabinet
Computerized medical devices	• Infusion pumps with dose-error-reduction capability (i.e., "smart" pumps) • Patient monitoring systems (e.g., cardiac, respiratory, fetal)
Electronic health record (EHR) or EHR component	• Bar-coded medication administration • Clinical decision support system • Clinical documentation system (e.g., progress notes) • Computerized provider order entry • Electronic medication administration record • Pharmacy system
Human interface device	• Keyboard • Monitor/display • Mouse • Printer • Speech recognition system • Touchscreen
Laboratory information system (including microbiology and pathology systems)	• Microbiology system • Pathology system • Test results reporting
Radiology/diagnostic imaging system	• Picture archiving and communication system

Adapted from "Device or Medical/Surgical Supply, Including Health Information Technology (HIT)." In Hospital Common Formats—Version 1.2: Event Descriptions, Sample Reports, and Forms, April 24, 2013. Rockville, MD: Agency for Healthcare Research and Quality. Retrieved August 20, 2013 from https://www.psoppc.org/web/patientsafety/version-1.2_documents.

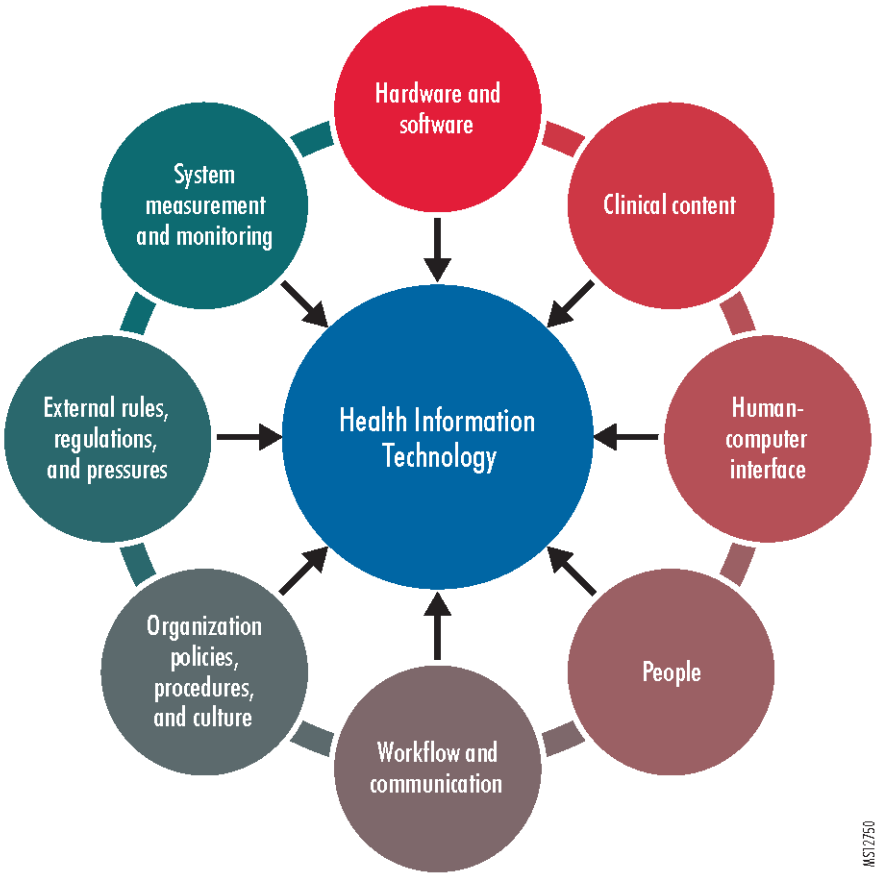
Indeed, health IT-related incidents can occur under any of the following circumstances (Sittig & Singh, 2011):

- The system is unavailable for use.
- The system malfunctions during its use.
- The system is used incorrectly.
- The system interacts incorrectly with another and causes the loss of data or data being incorrectly entered, displayed, or transmitted.

Socio-Technical Model

As with many events involving medical technology, health IT-related incidents, such as those described above, do not occur in isolation. The technology operates within a complex environment, and health IT must be considered in the context of that environment. In trying to understand why an event occurs, researchers have developed a socio-technical model for evaluating health IT within the context of eight dimensions (Sittig & Singh, 2010), as illustrated in Figure 2.

Figure 2. Socio-Technical Model for Health IT



Adapted by permission from BMJ Publishing Group Limited. Sitting DF and Singh H. A new socio-technical model for studying health information technology in complex adaptive healthcare systems. *Quality and Safety in Health Care.* 19(Supplement 3): i68-74, October 2010; doi: 10.1136/qshc.2010.042085

The eight dimensions of a socio-technical model for evaluating health IT are as follows:

1. Hardware and software (e.g., computers, keyboards, data storage, software to run health IT applications);

2. Clinical content (data, information, and knowledge stored in the system);

3. Human-computer interface (hardware and software interfaces that allow users to interact with the system);

4. People (software developers, IT department personnel, clinicians, healthcare staff, patients, and others involved in health IT development, implementation, and use);

5. Workflow and communication (steps followed to ensure patients receive the care they need at the time they need it);

6. Internal organizational policies, procedures, environment, and culture (internal organizational factors, such as capital budgets, IT policies, and event reporting systems, which affect all aspects of health IT development, implementation, use, and monitoring);

7. External rules, regulations, and pressures (external forces, such as federal and state rules to ensure privacy and security protections and federal payment incentives to spur health IT adoption); and

8. System measurement and monitoring (processes to measure and monitor health IT features and functions).

In short, examining health IT incidents within the context of the socio-technical model enables organizations to look beyond the incident to understand it in the context of the people who use the system and the other technologies and processes affected by health IT. Understanding these interactions enables high-reliability organizations to make improvements to their health IT systems when flaws in the systems are identified that can lead to patient harm.

Common Health IT-Related Problems

What are the most common problems that can occur with health IT systems? At the most basic level, there are two general areas. First, problems can occur at the interface between a computer user and the health IT system, causing a person to use the system incorrectly. Second, glitches can occur in how the equipment and software functions; for example, if software designed to connect one system to another has faulty coding, it could cause unexpected gaps in the transmitted data. Sample scenarios from each of these two categories, human-computer interface and computer-specific, are listed in Table 2.

As organizations try to understand why a particular problem arose with their health IT systems, they can dissect these two general categories in greater detail. Did a problem at the human-computer interface occur when data was entered into the health IT system or when it was retrieved? Did the problem arise because the computer user was interrupted or distracted from a task? For computer-specific issues, the organization can explore an array of questions that could have caused the incident. Was there a power interruption to the healthcare facility's computer network? Did information fail to display on the computer monitor? Was there a problem with the particular system's software, hardware, or both?

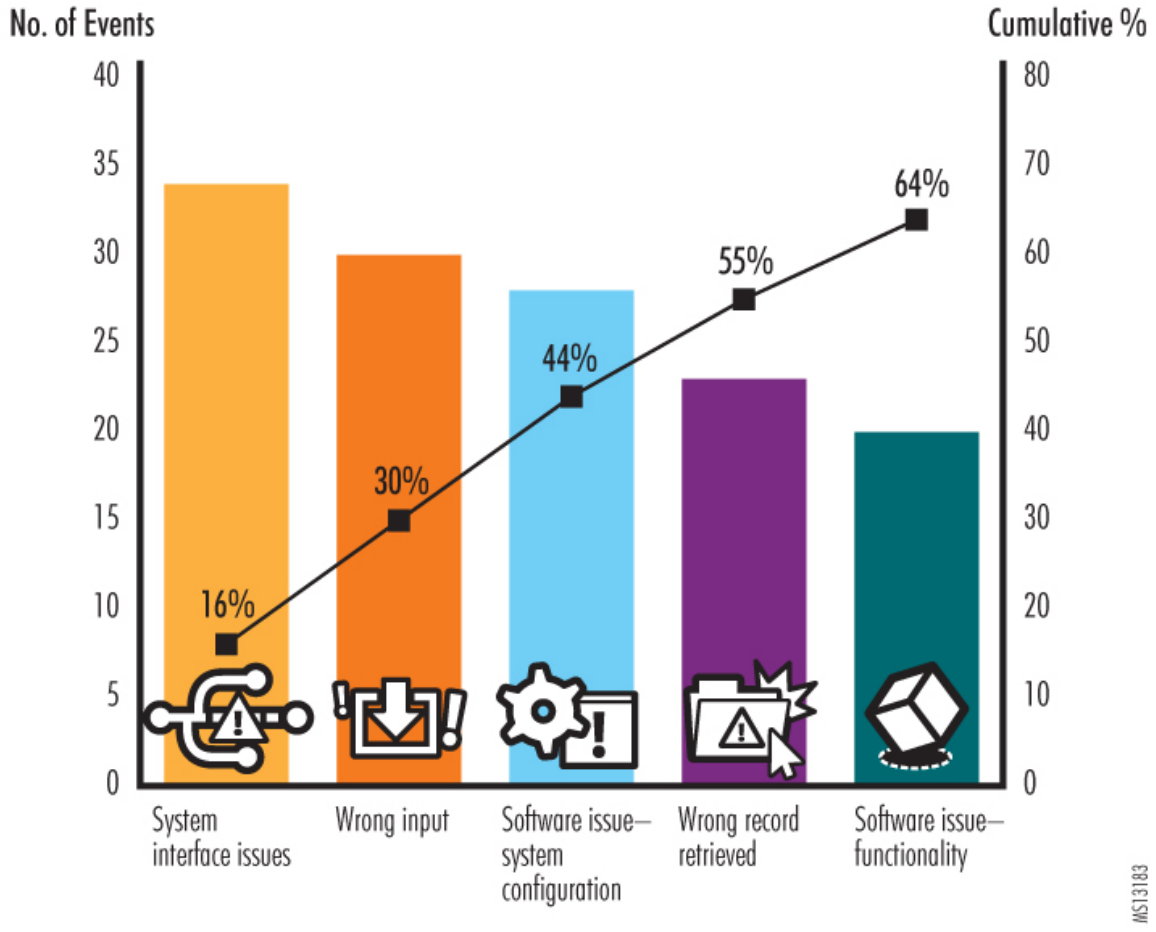
Table 2. Examples of Health IT-Related Incidents

Human-Computer Related	Computer Related
▪ A patient was not identified properly, and all clinical information was entered into the wrong record. ▪ Data were entered incorrectly into the electronic record due to multiple records being open. ▪ The system failed to alert the user of an identified concern with a flag or pop up. ▪ The user ignored or overrode an alert. ▪ Data were not entered into the system. ▪ Data were incomplete and missing from the entry. ▪ There was not enough equipment/devices for providers, causing delay in data entry. ▪ Lab test results were not reviewed in a timely manner. ▪ An item from an outside source was scanned into the wrong patient record. ▪ There was no evidence in the patient record of a written order or the care provided. ▪ Data from the archived paper record were not available at the time of the patient visit. ▪ Test results were sent to the wrong provider causing a delay in action. ▪ There were gaps in training among staff causing processes to be missed or done incorrectly. ▪ Text entries were not shared due to poorly designed interfaces between systems. ▪ Reasons for not using clinical decision support were not documented.	▪ Data were not displaying properly in the system. ▪ The network was down or slow. ▪ Interface issues with the laboratory system caused delays in the ability to retrieve data. ▪ The software was not up to date. ▪ Software did not meet the needs of the specialty provider. ▪ The software was not functioning properly. ▪ Data were lost. ▪ Internet or server connectivity issues prevented real-time data entry. ▪ There was a breach in the security of the system (e.g., virus or malware). ▪ Unapproved data-entry devices were used. ▪ The hardware malfunctioned (e.g., mouse, keyboard, monitor, or touchscreen).

Using a taxonomy designed for in-depth analysis of health IT-related incidents (Magrabi, Ong, Runciman, & Coiera, 2012), ECRI Institute PSO, one of the first PSOs to be federally certified, conducted an evaluation of health IT-related events and unsafe conditions to advance the healthcare sector's understanding of the technology and its impact on healthcare delivery.*

In its report *ECRI Institute PSO Deep Dive: Health Information Technology*, the PSO shared information learned from the events, as well as strategies to ensure health IT is appropriately implemented and used to improve healthcare quality without jeopardizing patient safety (ECRI Institute PSO, 2012). Figure 3 presents a summary of the five most frequently identified health IT-related problems found by the analysis.

Figure 3. ECRI Institute PSO Deep Dive Identifies Top Five Safety Issues from Health IT Events



The percentage identified with each event type represents the accumulative total of that event type and any preceding event types as a portion of the 211 safety events.

* ECRI Institute PSO's Deep Dive analysis evaluated more than 170 health IT-related events reported by 36 healthcare organizations over a nine-week period. The events ranged from data entries in the wrong patient records to gaps in reporting critical test results because the results could not be relayed electronically from one system to another. Some events involved more than one safety issue; consequently, the analysis identified 211 patient safety issues that were grouped into 22 event categories.

ECRI Institute PSO's analysis reinforces findings in the clinical literature and reports from policymakers, such as ONC and IOM, about the unintended consequences of the technology (ONC, 2013; IOM, 2011). A statewide analysis of health IT events in Pennsylvania reported to the state also reached similar conclusions about common health IT-related incidents (Sparnon & Marella, 2012).

Computer-Related Issues

Three of the five categories—system interface, system/software configuration, and software function—are considered computer-related events that occur, for example, as a result of design issues (e.g., difficult-to-read screen displays) or software interfaces that jeopardize the exchange of data between separate health IT systems. There can be numerous other reasons for these glitches. Identifying these reasons starts with understanding the type of problem associated with the incident.

System Interface

System interface problems were the most commonly identified health IT concern in ECRI Institute PSO's analysis. These problems arise if there are failures with the system interfaces, often resulting in missed orders for medications and various other types of tests, as in the following example:

> *The physician ordered the patient's anticoagulation medication be discontinued after reviewing results for the patient's prothrombin time. The order did not cross over to the pharmacy system, and the patient received eight extra doses of the medication before it was discontinued.*

System/Software Configuration

A large percentage of computer-related safety issues were also associated with the configuration of a system's hardware and software as in the following event:

> *Following the wound team consult, the nurse tried to enter instructions and comments in the patient's record, but the system prevented the nurse from typing more than five letters in the comment field.*

Software Function

Computer-related problems also occurred when a health IT system's software failed to function as intended. Examples of software problems affecting the system's function include the following:

- Inability to order a particular item, such as a specific magnetic resonance imaging study.
- Failure to record the correct medication dose when the medication label is scanned into the medication administration record.
- The system does not alert when a pregnancy test is ordered for a male patient.

Human-Computer Issues

Two of the five common health IT problem categories—wrong data input and wrong record retrieved—involved user interactions with the health IT system, or the so-called "human-computer interface." In these cases, a user's mistake in entering data or retrieving a record may have been prompted by the design features of the health IT system or the way in which the IT system was implemented. For example, an organization may choose to display drug names in a drop-down list by alphabetical order based on the premise that the drug names will be easier for users to find. But once the system is put into operation, the organization finds that users make frequent errors in selecting drugs with similar names.

Wrong Data Input

The most common problem encountered with the human-computer interface in ECRI Institute PSO's analysis occurred when a computer user entered incorrect data about the patient, such as weight, drug allergies, or an identification number. While incorrect data entry errors are not unique to the EHR (i.e., they also occur with paper records), the entry might auto-populate other fields, thereby multiplying the risks associated with the incorrect entry. Typical of such data entry errors is the following:

> *The nurse entered an incorrect patient identification number and recorded the blood glucose results from the bedside glucose meter for the wrong patient. The correct patient was still treated appropriately because the blood glucose results were immediately available at the bedside.*

Wrong Record Retrieved

Another common problem at the human-computer interface occurred when the wrong record was retrieved by the computer user, often resulting in a medication order for an incorrect patient as in the following event:

> *The pharmacist entered medication orders, written and intended for one patient, for the incorrect patient. There is no system validation that the correct patient record is pulled up.*

In another event, the medication management system allowed users to open two patient records at the same time, increasing the risk of entering orders for the wrong patient:

> *The medication management system allows the pharmacist to navigate off one patient profile and pull up another patient profile. An incorrect medication order was placed in the wrong patient's profile. The patient received incorrect medications as a result.*

The last two examples show how health IT risks may not be readily detectable or reported as a health IT-related event. In both scenarios, a patient almost received a medication intended for another patient, and, thus, the incident report was categorized as a medication error. But the underlying cause for both incidents was a suboptimal design in how pharmacists interacted with the health IT systems available to them.

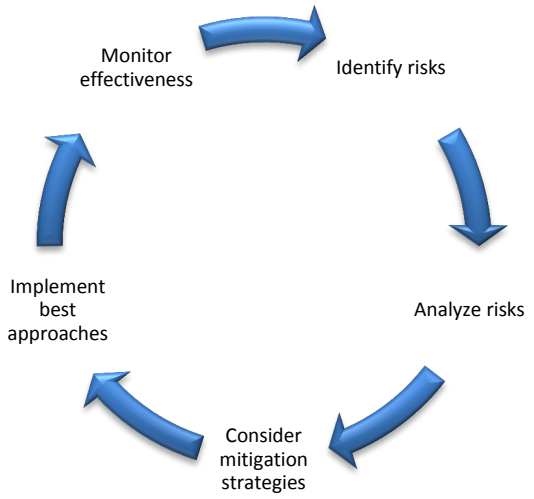
To be able to make improvements to these systems, healthcare organizations must be alert to the possible role of health IT in incidents. The next section examines how healthcare organizations can identify health IT-related incidents.

Identifying Health IT's Unintended Consequences

As healthcare organizations build a new foundation for care delivery with their health IT systems, they must not presume that the systems will always operate as planned, nor that patient safety is assured with these systems. Indeed, high-reliability organizations make safety their number one priority and approach safety systematically.

The high-reliability organization must maintain a never-ending, closed-loop approach to health IT system safety. As depicted in Figure 4, this approach requires continually monitoring for possible unintended consequences of health IT from the time the technology is first tested in the organization and throughout its full implementation and operation. If any safety risks are identified, the organization must examine the causes of these risks, consider strategies to eliminate the risks, select and implement the most effective risk-reduction strategies, and monitor these strategies to ensure they are working as intended.

Figure 4. Continuous Feedback Approach to Health IT System Safety



The goal for healthcare organizations in tracking and addressing the unintended consequences of health IT systems is to design robust processes to capture the problems that users encounter with the systems so that they can be addressed before any patients are harmed. The organization must, therefore, have processes in place to identify problems that can occur with the technology when it is first tested and implemented, as well as capture important information about health IT-related vulnerabilities throughout the system's operation in the organization.

The organization's patient safety adverse event reporting system provides a readily available tracking process. Given that event reporting systems are primarily designed to keep patient safety, risk, and quality staff informed of incidents and near misses that affect patients, the organization must have a process to involve its IT department and others with related expertise in addressing reports submitted to the event reporting system that require those departments' knowledge for resolution.

High-Reliability Organizations' Commitment to Health IT Safety

Of course, for the organization's approach to health IT safety to be successful, the high-reliability organization must build a safety culture that supports staff reporting of problems that they encounter.

The foundation for this culture is leadership commitment. Leaders can establish a safety culture with the following actions:

- Educate staff about health IT safety.
- Advocate health IT safety as everyone's responsibility.
- Promote open communication about health IT safety concerns.

- Empower staff to identify, report, and ameliorate hazards and risks from health IT systems.
- Establish a blame-free environment for reporting any health IT-related problems (including errors and near misses) without fear of punishment or reprisal.
- Allocate adequate resources to ensure health IT safety.

Event Reporting within a Safety Culture

Event reporting programs are integral to a continuous feedback approach to health IT safety because they allow organizations to identify health IT system breakdowns and failures. Operated within a blame-free safety culture established by the high-reliability organization, event reporting programs enable staff to report actual events, unsafe conditions, and near misses so the organization can examine the event, identify the causes of the event, and implement measures to prevent similar events from occurring and to lessen any injury to the patient if a similar event does recur. The reporting programs are typically overseen by the risk management department. (Later sections of this White Paper will discuss the value of reporting these events to PSOs to spread the lessons learned from the event to many institutions.)

As an example, refer to "Case Study: Health IT Event Report Leads to Safety Improvements" to learn how one organization used information reported about a serious health IT-related event to improve the electronic information display for drugs being administered to patients.

The case study describes a health IT incident that occurred after the system was fully deployed to patient care units. Equally important to monitoring the health IT system's ongoing performance is tracking system performance during their

Case Study: Health IT Event Report Leads to Safety Improvements

A hospital's electronic medication administration record (eMAR) shortened the display for morphine orders by cutting off the information indicating whether the drug is delivered as an extended-release formulation for long-term control of pain or as an immediate-release formulation for breakthrough pain. The organization had made the transition to eMAR from paper MARs, which clearly indicated the drug formulation ordered and administered.

A cancer patient's physician ordered extended-release morphine to be given to the patient every 12 hours to control cancer pain. The patient could also receive a smaller dose of the immediate-release formulation as needed for breakthrough pain. In the eMAR, each order was displayed as "morphine"; the dosing information about the regularly scheduled and as-needed doses was cut off in the display.

When one patient complained of pain, the patient was mistakenly given both formulations of the drug at the same time, causing the patient to suffer a respiratory arrest. An overdose of morphine, which is a high-alert medication, can cause serious patient harm. The patient was successfully intubated and resuscitated.

The event was reported to the organization's event reporting program. After reviewing the event, the organization worked with its health IT developer to ensure that the eMAR display for "morphine" included information about the drug formulation. Additionally, the organization identified other same-drug-name displays that cut off information about the drug dose in the eMAR and requested that the developer correct the display to show the dosing information.

early stages of implementation. Errors are likely to occur in the early phases of adoption as users adjust to the system and as bugs are identified that were not found during testing. "The period of initial use [of a health IT system] in an operational environment is fraught with patient safety risks, because it is during this period that many problems are likely to appear," IOM commented in its report *Health IT and Patient Safety: Building Safer Systems for Better Care* (IOM, 2011).

How to Collect Health IT Event Data

Educating Staff About Health IT Event Reporting

Healthcare staff should report health IT system-related hazards to the facility's event reporting program as they would report any other incident and near-miss affecting patient care and safety. In the health IT arena, however, frontline staff, who report a majority of events, may be unaware that the health IT system contributed to an incident. While some health IT-related events, such as a network failure causing the health IT system to be unavailable, are easily identified as health IT-specific, others may not be so readily identifiable. For example, what was first attributed to a medication dosing error may actually be a health IT system error if the default option from the drop-down menu of drug dose choices is unclear to clinicians entering a medication order.

To foster health IT event reporting, organizations must educate staff by providing examples of health IT-related incidents. The point to emphasize with staff is that the organization is collecting information not just on computer-related failures (e.g., the screen display was flickering; the clinician did not receive the patient's lab test results) but on situations that made the health IT system difficult to use at the human-computer interface (e.g., information was difficult to find; the system required too many clicks to get to a standard order set).

Additionally, organizations must underscore for staff the importance of reporting by illustrating how the information from these events can be used to improve the health IT system's function, as well as to minimize the likelihood that people using the system will make mistakes by using it incorrectly.

What to Include in a Health IT-Related Event Report

Most event reporting systems are designed so staff can provide certain essential information about the event, such as the date and time of the event, the location, and a brief, factual description of the event. But how does this information help to convey the involvement of health IT? Unfortunately, not all event reports are ideally structured for collecting information about health IT problems. To identify any health IT related factors in an event, healthcare organizations will need to modify their event reporting systems to collect information about the health IT system's involvement. One healthcare system, for example, redesigned its electronic event reporting system to add a drop-down box to capture specific information about problems with the health IT system if the reporter indicated the health IT system was involved in the incident (ECRI Institute PSO, 2012). Any modifications to the reporting system should enable reporters to provide sufficient information, in a standardized format, to identify the problems they encountered, such as the system was down, the

wrong record was retrieved, an alert did not display, results were posted to the wrong record, or the drug library was unavailable.

The event reporting system should capture enough information so that those analyzing the event can pinpoint specific health IT-related issues and answer such questions as:

- What health IT system (e.g., scheduling system, CPOE, Picture Archiving and Communication Systtem (PACS), monitor) was in use at the time of the event?
- What software version was used with the system?
- What display screen was the user looking at when trying to enter or transmit data?
- Who are the developers of the health IT system hardware and software associated with the event?
- Was the event the result of a user error, health IT system error, or a combination of both?

Fortunately, there are resources available from AHRQ that can help an organization reconfigure their event report systems to collect health IT-specific data in a standardized and robust format. These resources include the AHRQ Common Formats and a prototype system called Hazard Manager. Both are described below.

AHRQ Common Formats for Health IT Event Data

AHRQ has developed event report forms that can collect health IT event data in a structured format to provide important information for meaningful analysis. These forms, called the Common Formats for event reporting, were developed by AHRQ to enable PSOs to collect all event data in a standardized format. To date, these Common Formats have been developed for hospitals and long-term care facilities; another version will be released for ambulatory care settings.

The latest version of the hospital Common Formats includes health IT-specific questions to prompt staff to report pertinent health IT event data that will be helpful to the organization in reviewing and understanding the event in order to identify strategies to prevent the event from recurring. These questions have been incorporated into the event report form, "Device or Medical/Surgical Supply, Including Health Information Technology (HIT)" (AHRQ, 2013a). Refer to "Resources" to access the form online.

In addition to collecting specific information about the health IT system involved as well as important data about the type of error (i.e., user error or device error), the form prompts the individual reporting the event to identify factors contributing to the incident. If some cases, frontline staff reporting the event may not have access to all the information to complete the form. Those within the organization tasked with reviewing and analyzing health IT events may need to obtain that information. Refer to "Common Formats Identify Circumstances for Health IT-Related Events" for a list of those circumstances identified on the event report form.

Beyond the Common Formats: Hazard Manager

Organizations may choose to supplement the data collected from the AHRQ Common Formats with an additional narrative field for those submitting incident reports to describe their concerns in detail. Organizations may also choose to enhance the reports with additional questions to get to the underlying reasons for the reporter's concerns, although the organization's event review team will likely need to obtain the answers to these additional questions. More than likely, frontline staff will not have the information at hand when they report the event.

For example, while the Common Formats enable a computer user to indicate that a health IT safety concern is related to the display of information on the computer, organizations may want to collect additional detail about that concern to better identify corrective measures. Additional questions for the event review team to explore include:

- Was the information on the computer screen organized and clear?
- Was critical information available and observable?
- Was the text on the screen easily readable?
- Did the processes charted by the health IT system match the user's workflow?
- Did the user interface reduce short-term memory load (i.e., the user was not required to remember information from one screen when working in another screen)?

Examples of these and other questions to consider are contained in AHRQ's Health IT Hazard Manager, a prototype tool for healthcare organizations, EHR developers, and researchers to report and systematically analyze health IT-related hazards and safety concerns (Walker, Hassol, Bradshaw, & Rezaee, 2012). Refer to "Resources" to access a report about the tool. The report contains sample questions to ask about a particular health IT safety concern, as well as a lengthy list of possible underlying causes for the problem so that the organization can begin to identify corrective measures.

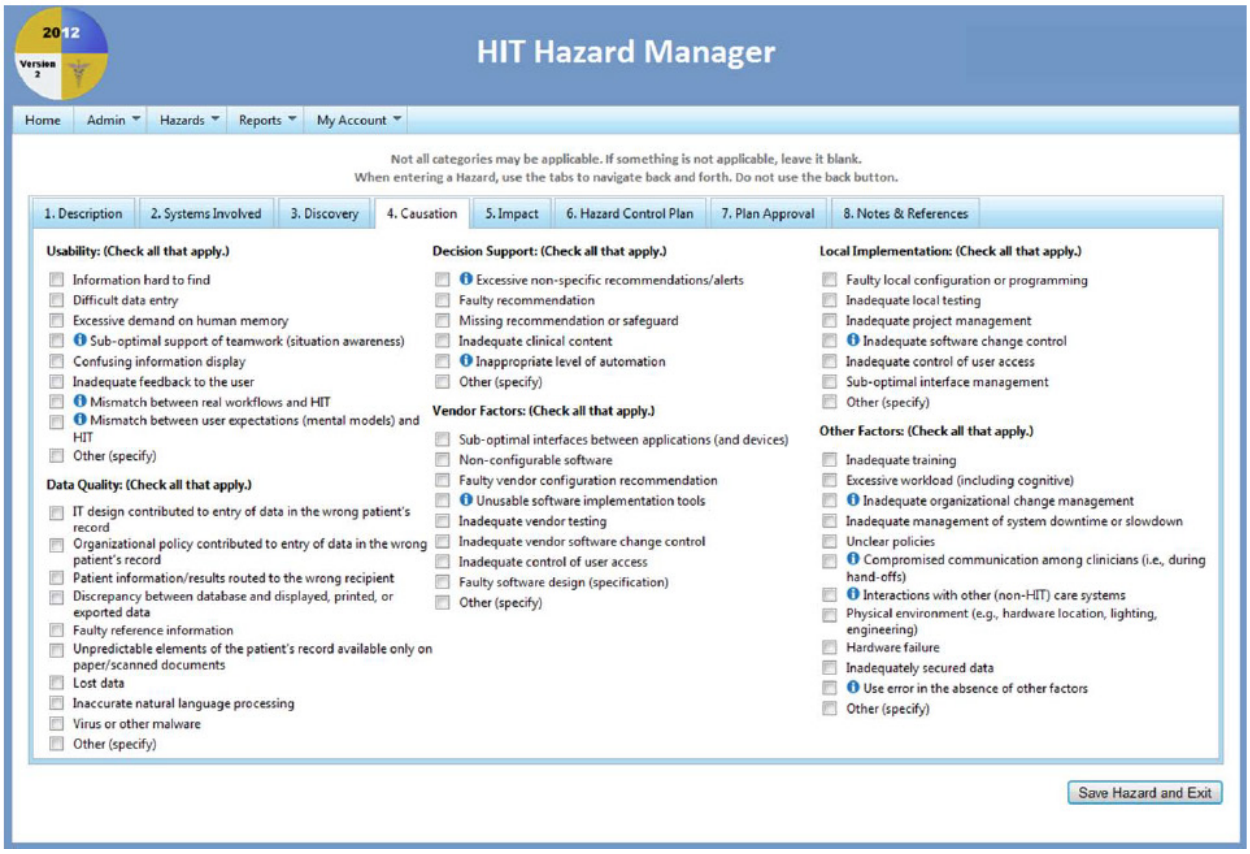
Common Formats Identify Circumstances for Health IT-Related Events

- Incompatibility between devices
- Equipment/device function
  - Loss or delay of data
  - System returns or stores data that does not match patient
  - Image measurement/corruption issue
  - Image orientation incorrect
  - Incorrect test results
  - Incorrect software programming calculation
  - Incorrect or inappropriate alert
- Equipment/device maintenance
- Hardware failure or problem
- Failure of, or problem with, wired or wireless network
- Ergonomics, including human/device interface issue
  - Hardware location
  - Data entry or selection
  - Information display or interpretation
  - Alert fatigue/alarm fatigue
- Security, virus or other malware issue
- Unexpected software design issue

Source: Adapted from "Device or Medical/Surgical Supply, Including Health Information Technology (HIT)." In *Hospital Common Formats—Version 1.2: Event Descriptions, Sample Reports, and Forms, April 24, 2013*. Rockville, MD: Agency for Healthcare Research and Quality. Retrieved August 20, 2013 from https://www.psoppc.org/web/patientsafety/version-1.2_documents.

A snapshot of some of the information that the tool collects is reprinted in Figure 5.

Figure 5. Sample Screenshot from AHRQ's Hazard Manager



Source: Adapted from "Health IT Hazard Manager Beta-Test: Final Report," by J. M. Walker, A. Hassol, B. Bradshaw, and M. E. Rezaee, 2012, (AHRQ Publication No. 12-0058-EF). Rockville, MD: Agency for Healthcare Research and Quality. Retrieved from http://healthit.ahrq.gov/sites/default/files/docs/citation/HealthITHazardManagerFinalReport.pdf.

Health IT Event and Hazard Analysis

Incidents identified by event reporting should be analyzed in a structured, step-by-step manner. It is particularly important to examine incidents that reach the patient and to determine why the event happened, as well as the underlying causes. Event analysis tools, such as failure mode and effects analysis and root-cause analysis, can be used to better understand where failures can or do occur.

Consider the following poorly designed health IT system interface that hindered the reporting of critical laboratory results to patients' physicians and eventually led to a fatal event:

- The interface between the hospital's laboratory information system and its transplant surgery database only allowed certain laboratory test results to reach the transplant database.

- The transplant team had to access the laboratory system and the organization's EHR for additional test result information.
- Transplant staff created a paper-based workaround. Using a printed list of transplant patients, patient care coordinators would review physicians' inboxes within the organization's EHR to find the laboratory results that could not be reported electronically to the transplant database.
- Once results were reviewed, the coordinator would sign off on the result, delete the notification from the inbox, and enter an "action item" about the results in the transplant database.
- When a particular transplant patient underwent laboratory testing, critical results indicating possible transplant rejection were reported to the laboratory information system but not to the transplant surgery database because of the incomplete interface between the two systems.
- In this particular event, the coordinator deleted the notification but did not enter an action item in the transplant database.
- Several months after the laboratory tests were conducted, the patient died as a result of organ transplant rejection.
- Upon the patient's admission to the hospital for treatment for the failing transplant, staff discovered the original test result in the organization's EHR, which had indicated pending organ failure. The physician had never seen the test result to act on its findings.

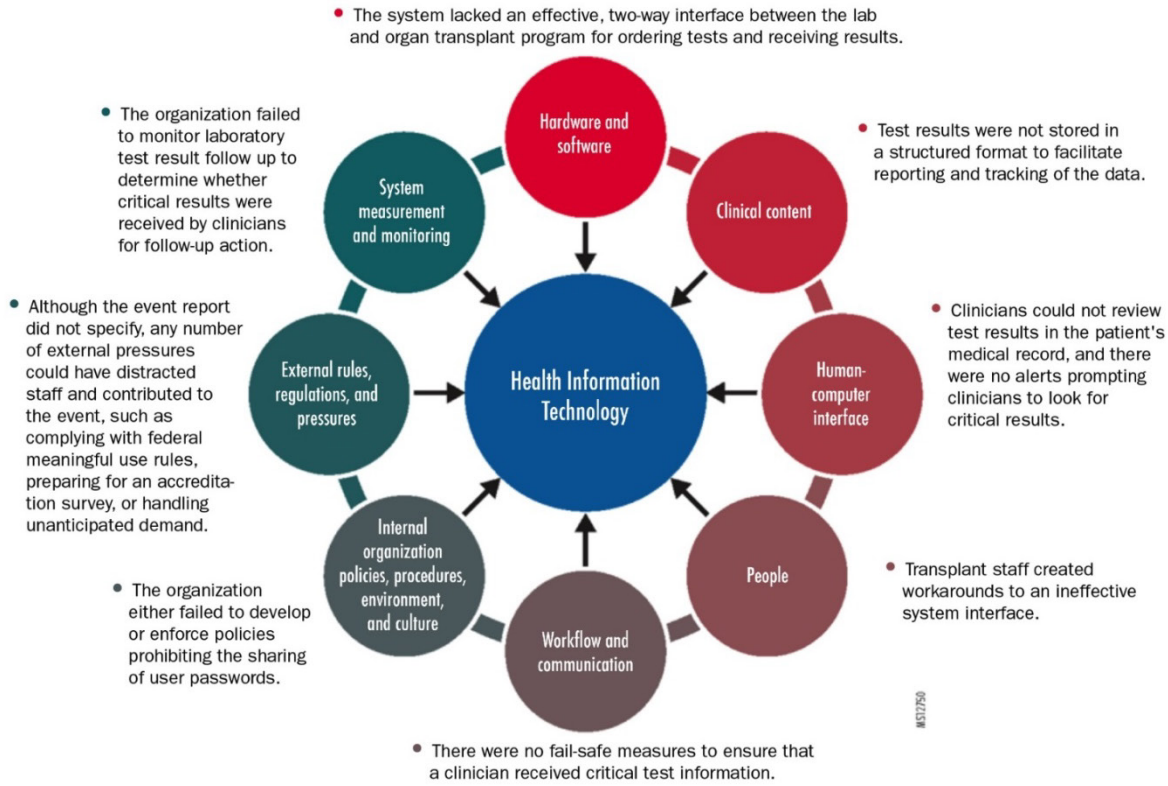
Using the eight dimensions of the socio-technical model, the organization can begin to conduct an in-depth examination of the event to understand how and why the health IT event occurred and, ultimately, to identify and design strategies to prevent similar events. Here is a partial look at what each dimension might reveal about the particular event:

- **Hardware and software.** The system lacked an effective, two-way interface between the lab and organ transplant program for ordering tests and receiving results.
- **Clinical content.** Test results were not stored in a structured format to facilitate reporting and tracking of the data.
- **Human-computer interface.** Clinicians could not review test results in the patient's medical record, and there were no alerts prompting clinicians to look for critical results.
- **People.** Transplant staff created workarounds to an ineffective system interface.
- **Workflow and communication.** There were no fail-safe measures to ensure that a clinician received critical test information.
- **Internal organizational policies, procedures, environment, and culture.** The organization either failed to develop or enforce policies prohibiting the sharing of user passwords.

- **External rules, regulations, and pressures.** Any number of external pressures could have contributed to the event. For example, if the transplant center was preparing for an inspection, the care coordinator may have been distracted and forgot to record the test results.
- **System measurement and monitoring.** The organization failed to monitor laboratory test result follow up to determine whether critical results were received by clinicians for follow-up action.

Using the socio-technical model, Figure 6 depicts the analysis for each of the eight dimensions for a laboratory event involving Health IT.

Figure 6. Case Study of a Laboratory Event Involving Health IT



Adapted by permission from BMJ Publishing Group Limited. Sitting DF and Singh H. A new socio-technical model for studying health information technology in complex adaptive healthcare systems. *Quality and Safety in Health Care.* 19(Supplement 3): i68-74, October 2010; doi: 10.1136/qshc.2010.042085

Just as James Reason's "Swiss cheese model" for system failure illustrates that accidents are the result of multiple faults within a system that occur together in an unanticipated interaction, the socio-technical model illustrates the multiple facets within an organization that affect health IT safety.

The in-depth analysis of a health IT incident must be conducted by a multidisciplinary team of health IT system stakeholders, as well as those familiar with the particular hazard or incident. While

organizations' event analyses have typically involved representatives from the clinical departments affected, incidents that involve health IT must include the IT department and other departments, such as biomedical engineering, familiar with the technology.

Staff Feedback and Monitoring

Following the incident investigation, staff should be provided with feedback about the analysis—and the error-prevention strategies put in place—so that they understand that their reporting leads to safer patient care and continue to participate in the process. And, of course, the organization must monitor the effectiveness of the new strategies and solutions to ensure they are working as intended. To reiterate, attention to health IT safety is continuous in a high-reliability organization.

Additionally, organizations must monitor the effectiveness of their event reporting programs to ensure that staff know how to use the program and that the program is capturing the necessary data for continuous improvement. Refer to "Issues for Managers: Questions to Evaluate Health IT Incident Reporting Effectiveness" for sample questions to consider when assessing the effectiveness of an organization's event reporting program in capturing health IT-related occurrences.

Other Sources of Information for Health IT-Related Issues

An organization's event reporting program should not be the only source for collecting data about an organization's health IT events. Throughout the health IT system lifecycle, it is important to talk to users and seek their feedback on the system's ease of use and to determine what problems, if any, they have encountered. Other information sources for potential health IT-related problems include helpdesk logs maintained by the IT department, medical chart reviews, claims data, and executive staff walkarounds on patient care units to inquire about staff concerns about the health IT system.

Reporting Health IT Events to PSOs

PSOs serve as a source of external advice for healthcare providers seeking to improve the safety of health IT, as well as patient safety more broadly. Federal law provides that hospitals, doctors, and other healthcare providers may voluntarily report patient safety events to PSOs, on a privileged and confidential basis, for aggregation and analysis. By reporting health IT events to a PSO, healthcare providers enhance their ability to make health IT system improvements. No one organization's incident data is likely to contain a sufficient number of health IT-related events to detect trends and gain insights about health IT hazards as would be accomplished when organizations share their data.

Issues for Managers: Questions to Evaluate Health IT Event Reporting Effectiveness

1. Are health IT system users instructed on using the organization's patient safety adverse event reporting system to report events, near misses, and hazardous conditions involving health IT?
2. Has a patient safety, risk, and/or quality professional reviewed the event report form to ensure that information pertinent to health IT-related events is collected in the report?
3. Does the event report use common language and terminology to prompt the sharing of data about events associated with health IT systems?
4. Do patient safety, risk, and/or quality staff have a process in place to forward any event reports raising health IT issues to the IT department for resolution?
5. Do patient safety, risk, and/or quality staff have a process in place to identify health IT events requiring additional analysis in order to understand the systems issues that may have contributed to the event and to identify measures to prevent recurrence of similar events?
6. Does a representative from the IT department, in addition to other appropriate stakeholders, participate in all follow-up systems analyses of health IT-related events?
7. Is a process in place to track corrective actions identified as a result of a systems analysis of health IT-related events (e.g., identify the corrective actions, designate responsible department or individual, specify time frame for implementation)?
8. Are the findings from the event analysis reported to appropriate departments and individuals within the organization?
9. Does the organization have a process to identify health IT-related events that will be reported to external organizations or entities (e.g., ECRI Institute, PSOs, Institute for Safe Medication Practices, the Joint Commission)?
10. Does the organization have a process to determine whether adverse events involving health IT systems must be reported to the U.S. Food and Drug Administration under the mandatory reporting provisions of the Safe Medical Devices Act as applicable?
11. Does the organization set aside funds in its capital budget for ongoing maintenance and improvements to the health IT system?
12. Does the organization have policies and procedures for change management (i.e., a structured approach for ensuring that system modifications, such as software upgrades and scheduled maintenance, are performed in a controlled manner)?
13. Does the organization assess, approve, and implement changes (e.g., hardware and software upgrades, security changes, new applications, new work processes, new input devices, planned maintenance) to interfaced medical devices and IT systems in a controlled manner to evaluate their impact on the various components of the networked devices and IT system?
14. If any concerns are identified during testing of changes and updates to interfaced medical devices and IT systems, are they addressed before any changes are fully implemented?

Source: Adapted from "ECRI Institute PSO Deep Dive: Health Information Technology," by ECRI Institute PSO, 2012. Plymouth Meeting, PA: Author.

Several organizations—including IOM and ONC—are calling for federally certified PSOs to monitor safety events involving health IT to better identify the types of errors that can occur from using the technology and to guide improvements (IOM, 2011; ONC, 2013). ONC's 2013 *Health Information Technology Patient Safety Action and Surveillance Plan*, underscores the important role of PSOs in identifying, aggregating, and analyzing health IT safety event and hazard reports. This plan builds on recommendations from the IOM's 2011 *Health IT and Patient Safety: Building Safer Systems for Better Care*. Refer to "Resources" to download the organizations' reports.

PSO activities are established under the Patient Safety and Quality Improvement Act of 2005 (PSQIA), which creates a framework for healthcare providers to collect and share patient safety data in a nonthreatening, confidential, and protected legal environment. Within the protected environment, PSOs provide analysis and feedback about the events to help organizations make patient safety improvements, including improvements to assure health IT safety. Additionally, PSOs can collect the information in a standardized format, using the Common Formats, in order to aggregate the data, identify trends that might not be detected from an organization's more limited event data, and gain patient safety insights to share with the healthcare community.

ECRI Institute PSO's Deep Dive analysis of health IT events is an example of the shared learning that can be achieved with PSOs. The analysis benefited from PSOs' capability to collect multiple events from multiple organizations in a standardized format and to share the lessons learned from analyzing those events without identifying any organization or individual identified in an event.

Further learning can occur when multiple PSOs share aggregated data about health IT events reported to them. Because the Common Formats promote collection of this data in a standardized format, multiple PSOs could combine their health IT event data to spot trends, suggest health IT safety solutions, and ensure health IT is effectively used for safe patient care. As data becomes available from PSOs, AHRQ intends to oversee a national network of patient safety database, which can analyze nonidentified and aggregated patient safety event information, including health IT events.

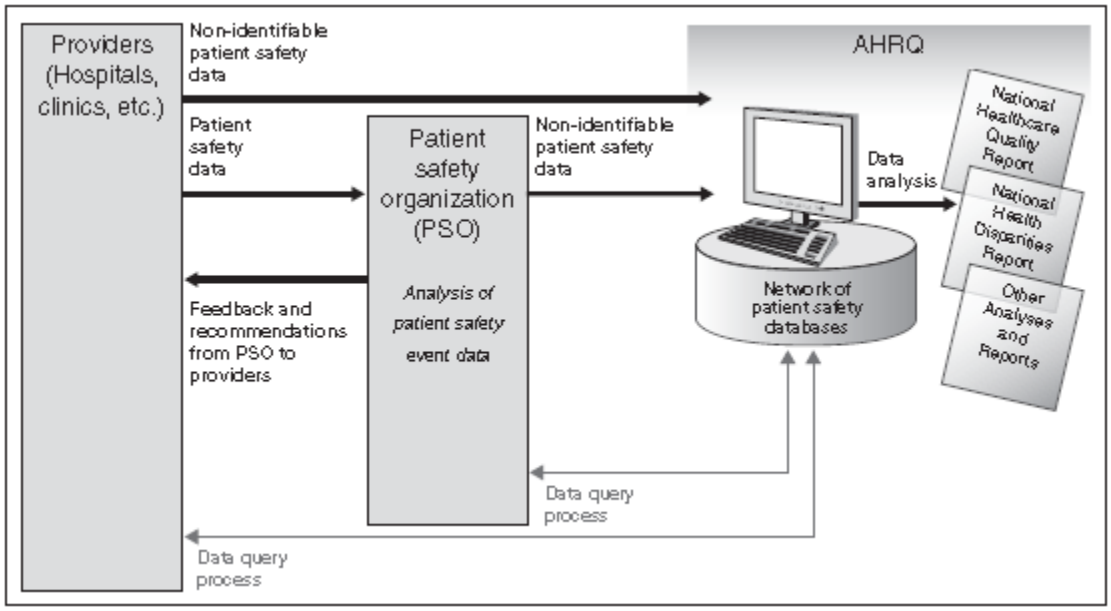
The flow of patient safety information from healthcare providers to PSOs and AHRQ's national database and back to healthcare providers is depicted in Figure 7.

EHR Developers' Role in Assuring Patient Safety

The case study described earlier about one hospital's initiative to engage its health IT system developer in improvements for an eMAR display following a serious patient safety event underscores the important role of EHR developers in assuring patient safety. Health IT safety hinges on the cooperation between health IT customers and their systems' developers.

In fact, EHR developers have a shared responsibility with healthcare facilities and health IT system users to ensure the technology's safety, as summarized by IOM in *Health IT and Patient Safety: Building Safer Systems for Better Care*. "Vendors, care providers, provider organizations and their IT departments . . . are all partners in building a safer system in which IT is used," the report says.

Figure 7. Intended Flow of Patient Safety Event Data and Feedback



Source: Adapted from "Patient Safety Act: HHS Is in the Process of Implementing the Act, So Its Effectiveness Cannot Yet Be Evaluated," by *the* U.S. Government Accountability Office (GAO), 2010, GAO-10-281. Washington, DC: Author. Retrieved from http://www.gao.gov/assets/310/300382.pdf.

EHR developers, represented by the Electronic Health Record Association (EHRA), acknowledge their responsibility to ensure patient safety with their products and, in June 2013, issued the EHR Developer Code of Conduct, outlining their patient safety responsibilities. Refer to "Resources" to download the document.

Any EHR developer that wishes to promote its adoption of the code must agree to adhere to the following principles regarding patient safety (EHRA, 2013):

- Support patient safety in their product design, development, and deployment.
- Share best practices with customers for safe deployment, implementation, maintenance, and use of their products.
- Participate with one or more PSOs for reporting, reviewing, and analyzing health IT-related patient safety events.
- Notify customers when they identify or become aware of software issues that could materially affect patient safety and to offer solutions.
- Recognize the value of their customers' participation in discussions about patient safety and not contractually limit their customers from discussing patient safety issues in appropriate venues.

The EHRA's Code of Conduct reinforces what healthcare organizations should expect and demand from their EHR developers. As a customer, the organization should be able to contact the developer about hardware and software problems to identify possible solutions to the issue—just like the hospital that was able to remedy the truncated drug dose display by reporting the problem to the system developer. Similarly, healthcare organizations should expect and demand that their developer report known hazards and software bugs that could contribute to health IT safety events and to offer solutions to the problems.

While a health IT developer's adoption of the EHRA Code of Conduct is an important indication of the company's commitment to health IT safety, healthcare organizations must ensure that these assurances are spelled out in their contracts with EHR developers. Additional guidance on health IT developer contracts is available from ONC. Refer to "Resources" to access ONC's report, "EHR Contracts: Key Contract Terms for Users to Understand."

Teaming Up With PSOs

Sometimes, the problems that healthcare organizations encounter with their health IT systems may require more investigation and analysis than can be provided by the systems' developers and healthcare providers. What are the best strategies to reduce distracting alerts to clinicians? What measures have other organizations adopted to prevent sharing of computer user passwords? What redundancies can be built into the health IT system to ensure critical test results are received by the ordering physician or the designated back-up clinician? Answers to these and similar questions are not always within the developer's domain and may require the input of other healthcare providers, researchers, and patient safety experts.

Importantly, the EHRA Code of Conduct recognizes the value of healthcare organizations discussing safety issues involving health IT in appropriate venues, such as the confidential and protected environment provided by PSOs. And, in fact, EHR developers can also participate with PSOs, within the limits allowed by law, to provide insights about the safety issues identified. PSQIA permits EHR developers to work with PSOs and, as such, to participate in analyses of events involving their products and view certain identifiable data. AHRQ provides information on engaging system developers in these patient safety activities on its website. In its Frequently Asked Questions (FAQs) about PSOs, AHRQ addresses three ways in which EHR developers can work with providers and PSOs within the framework of the PSQIA (Refer to "Resources" for accessing the FAQs online). In brief, these three approaches are as follows (AHRQ, 2013b):

1. Serve as a contractor to a PSO. PSQIA permits a PSO to contract with another entity, such as an EHR technology developer, to disclose patient safety information about health IT systems that is classified as patient safety work product (PSWP). Under the law, PSWP is given confidentiality and privilege protections, so the contracting entity is not permitted to disclose the information unless the disclosure is deemed permissible.

2. Serve as a contractor to a provider. The provider can contract with another entity, such as a health IT developer, to submit patient safety reports to a PSO on behalf of the provider working with the PSO.

3. Create a component organization to seek listing and serve as a PSO. While a EHR technology or software developer cannot become federally certified as a PSO, it can create a component organization that can become a PSO. Operating under the requirements that apply to all PSOs, the component PSO could receive and analyze patient safety events and hazards involving health IT.

Conclusion

Health IT can reshape healthcare delivery by fostering patient safety and healthcare quality if it is thoughtfully developed and implemented and used as intended. Providers, EHR developers, and policymakers recognize that problems can occur with the technology and, if unaddressed, can lead to patient harm and undermine the goal to use health IT to improve patient care. Together, they have a shared responsibility to ensure health IT can be used to promote patient safety.

This White Paper explored the wide array of problems that can arise with health IT and the role of incident and hazard reporting within healthcare organizations to address these issues. While the safety focus of high-reliability organizations enables these organizations to continually monitor and address health IT safety, they cannot achieve the goal of health IT safety alone.

In addition to using their internal event reporting systems, providers, system developers, and policymakers must harness the information reported to external groups such as PSOs, which have the capability to identify trends and patterns that can lead to patient safety events from data submitted in a standardized format by multiple providers. EHR developers, in particular, must support such initiatives, recognizing that they can still protect innovation while working with their customers to meet the higher priority of protecting patient safety.

Through initiatives to monitor the unintended consequences of health IT and share their findings, healthcare organizations and their health IT users, as well as policymakers and EHR developers, can foster the development, adoption, and use of the safest systems for the best care.

Resources

AHRQ Common Format: Device or Medical/Surgical Supply, Including Health Information Technology (HIT) Form

AHRQ's FAQs about PSOs

EHR Contracts: Key Contract Terms for Users to Understand

Electronic Health Record Association's EHR Developer Code of Conduct Principles

Health IT Hazard Manager Beta-Test: Final Report

ONC's Health Information Technology: Patient Safety Action & Surveillance Plan

Institute of Medicine's report, *Health IT and Patient Safety: Building Safer Systems for Better Care*

References

Agency for Healthcare Research and Quality (AHRQ). (2013a). Device or medical/surgical supply, including health information technology (HIT). In *Hospital common formats—version 1.2: Event descriptions, sample reports, and forms, April 24, 2013*. Retrieved August 20, 2013 from https://www.psoppc.org/web/patientsafety/version-1.2_documents.

Agency for Healthcare Research and Quality (AHRQ). (2013b). Patient safety organization (PSO) FAQs. Retrieved August 27, 2013 from http://www.pso.ahrq.gov/psos/fastfacts.htm.

Ash, J. S., Berg, M., & Coiera, E. (2004). Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. *Journal of American Medical Informatics Association,* 11(2), 104-112.

Del Beccaro, M. A., Jeffries, H. E., Eisenberg, M. A., & Harry, E. D. (2006). Computerized provider order entry implementation: No association with increased mortality rates in an intensive care unit. *Pediatrics,* 118(1), 290-295.

ECRI Institute PSO. (2012). *ECRI Institute PSO deep dive: health information technology*. Plymouth Meeting, PA: Author.

Electronic Health Record Association (EHRA). (2013). EHR developer code of conduct (June 11, 2013). Retrieved August 27, 2013 from http://www.himssehra.org/docs/EHR%20Developer%20Code%20of%20Conduct%20Final.pdf.

Han, Y. Y., Carcillo, J. A., Venkataraman, S .T., Clark, R. S. B., Watson, R. S., Nguyen, T. C., Bayir, H., & Orr, R. A. (2005). Unexpected increased mortality after implementation of a commercially sold computerized provider order entry system. *Pediatrics,* 116(6), 1506-1512.

Institute of Medicine (IOM). (2011). *Health IT and patient safety: building safer systems for better care.* Washington, DC: National Academies Press.

Kaushal, R., Shojania, K. G., & Bates, D. W. (2003). Effects of computerized physician order entry and clinical decision support systems on medication safety: a systematic review. *Archives of Internal Medicine,*, 163(12), 1409-1416.

Koppel, R., Metlay, J. P., Cohen, A., Abaluck, B., Localio, A. R., Kimmel, S. E., & Strom, B. L. (2005). Role of computerized physician order entry systems in facilitating medication errors. *Journal of the American Medical Association,* 293(10), 1197-1203.

Longhurst, C. A., Parast, L., Sandborg, C. I., Widen, E., Sullivan, J., Hahn, J. S., Dawes, C. G., & Sharek, P .J. (2010). Decrease in hospital-wide mortality rate after implementation of a commercially sold computerized physician order entry system. *Pediatrics,* 126(1), 14-21.

Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E. (2012). Using FDA reports to inform a classification for health information technology safety problems. *Journal of American Medical Informatics Association,* 19(1), 45-53.

Office of the National Coordinator for Health Information Technology (ONC). (2013). Health information technology: patient safety action & surveillance plan. Retrieved August 26, 2013 from http://www.healthit.gov/sites/default/files/safety_plan_master.pdf.

Sittig, D. F., & Singh, H. (2011). Defining health information technology-related errors. *Archives of Internal Medicine,* 171(14), 1281-1284.

Sitting, D. F., & Singh, H. (2010). A new socio-technical model for studying health information technology in complex adaptive healthcare systems. *Quality and Safety in Health Care*, Supplement 3, October 19, 2010, i68-74. doi: 10.1136/qshc.2010.042085

Sparnon, E., & Marella, W. M. (2012). The role of the electronic health record in patient safety events. *Pennsylvania Patient Safety Advisory,* 9(4), 113-121.

U.S. Food and Drug Administration (FDA). (2013). Class 2 recall: ED PulseCheck, July 29, 2013. Retrieved September 15, 2013 from http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRes/res.cfm?ID=119832.

U.S. Government Accountability Office (GAO). (2010). *Patient Safety Act: HHS is in the process of implementing the Act, so its effectiveness cannot yet be evaluated.* GAO-10-281. Washington, DC: Author. Retrieved from http://www.gao.gov/assets/310/300382.pdf.

Walker, J. M., Hassol, A., Bradshaw, B., & Rezaee, M. E. (2012). *Health IT hazard manager beta-test: Final report* (AHRQ Publication No. 12-0058-EF). Rockville, MD: Agency for Healthcare Research and Quality. Retrieved from http://healthit.ahrq.gov/sites/default/files/docs/citation/HealthITHazardManagerFinalReport.pdf.