

# ECRI INSTITUTE PSO DEEP DIVE: HEALTH INFORMATION TECHNOLOGY

ECRI<sup>Institute</sup>  
**PSO**  
*Share Learn Protect™*

- ▷ In-depth look at health information technology
- ▷ Systems-focused learning
- ▷ Leadership strategies
- ▷ Online resources

## ECRI INSTITUTE PSO

**Ronni P. Solomon, J.D.**, Executive Vice President and General Counsel; **Karen P. Zimmer, M.D., M.P.H.**, FAAP, Editor, *PSO Navigator*, Medical Director; **Amy Goldberg-Alberts, M.B.A.**, FASHRM, CPHRM, Program Director; **Barbara G. Rebold, B.S.N., M.S., R.N.**, CPHQ, Director, PSO Operations

**Paul A. Anderson**, Director, Risk Management Publications; **Theresa V. Arnold, D.P.M.**, Manager, Clinical Analysis; **Sharon Bradley, R.N., CIC**, Infection Preventionist; **Maura N. Crossen-Luba, M.P.H.**, CPH, Healthcare Writer; **Andrea Fenton**, Web Editor; **Robert C. Giannini, NHA**, Patient Safety Analyst and Consultant; **Ambily Gracebaby, M.S.**, Clinical Informatics Analyst and Consultant; **Kelly C. Graham, B.S.N., R.N.**, Patient Safety Analyst and Consultant; **Gail M. Horvath, M.S.N., R.N.**, CNOR, CRCST, Patient Safety Analyst and Consultant; **Ruth Ison, M.Div., S.T.M.**, Patient Safety Analyst and Consultant; **Jane Kelly, B.S., RN, CPHQ**, Senior Risk Management Analyst and Consultant; **William M. Marella, M.B.A.**, **Barbara (BJ) McAdams**, Administrative Coordinator; **Patricia Neumann, R.N., M.S.**, Senior Patient Safety Analyst and Consultant; **Luke A. Petosa, M.Sc.**, HEM, HEM-CC, Director, Center for Education and Training; **Catherine Pusey, R.N., M.B.A.**, Manager, Clinical Analysts; **Madelyn S. Quattrone, Esq.**, Legal Editor, Risk Management Publications; **Sheila Rossi, M.H.A.**, Senior Patient Safety Analyst and Consultant; **Melva Sanzon**, Reporting and Business Analyst; **Cynthia Wallace, CPHRM**, Senior Risk Management Analyst; **Andrea J. Zavod**, Managing Editor

## ADVISORY COUNCIL

**Katrina Belt, M.P.A.**, Senior Vice President, Chief Financial Officer, Healthcare Authority for Baptist Health; **Doug Bonacum, M.B.A., CSP, CPHQ**, CPHRM, Vice President, Safety Management, Kaiser Permanente; **Darrel A. Campbell Jr., M.D.**, University of Michigan Health System; **Nancy E. Foster**, American Hospital Association; **Karen Haller, Ph.D., R.N.**, Johns Hopkins Hospital; **Stephen T. Lawless, M.D., M.B.A.**, The Nemours Foundation/Alfred I. DuPont Hospital for Children; **David C. Levin, M.D.**, Jefferson Health System; **Michael A. Olympio, M.D.**, Wake Forest University School of Medicine; **Richard G. Roberts, M.D., J.D.**, University of Wisconsin School of Medicine and Public Health; **Debra Simmons, Ph.D., R.N.**, CCNS, St. Luke's Episcopal Health System; **Robert M. Wachter, M.D.**, University of California, San Francisco

## MISSION STATEMENT

The ECRI Institute PSO is a federally listed patient safety organization that is a component of ECRI Institute. ECRI Institute, a nonprofit organization, dedicates itself to bringing the discipline of applied scientific research in healthcare to uncover the best approaches to improving patient care. As a pioneer in this science for 40 years, ECRI Institute marries experience and independence with the objectivity of evidence-based research.

*ECRI Institute PSO Deep Dive: Health Information Technology* is published by ECRI Institute, 5200 Butler Pike, Plymouth Meeting, PA 19462, USA; (610) 825-6000 (telephone); (610) 834-1275 (fax); info@ecri.org (e-mail).

For more information about ECRI Institute PSO, send an e-mail to psoheldesk@ecri.org.

ECRIInstitute  
**PSO**  
Share Learn Protect™

ECRIInstitute  
The Strength of Science. The Integrity of Independence.

## ACKNOWLEDGMENTS

ECRI Institute PSO thanks its collaborating PSOs and member organizations for sharing their health information technology (IT)-related events for this Deep Dive™ report. There are many lessons that ECRI Institute PSO members can learn from the aggregated analysis.

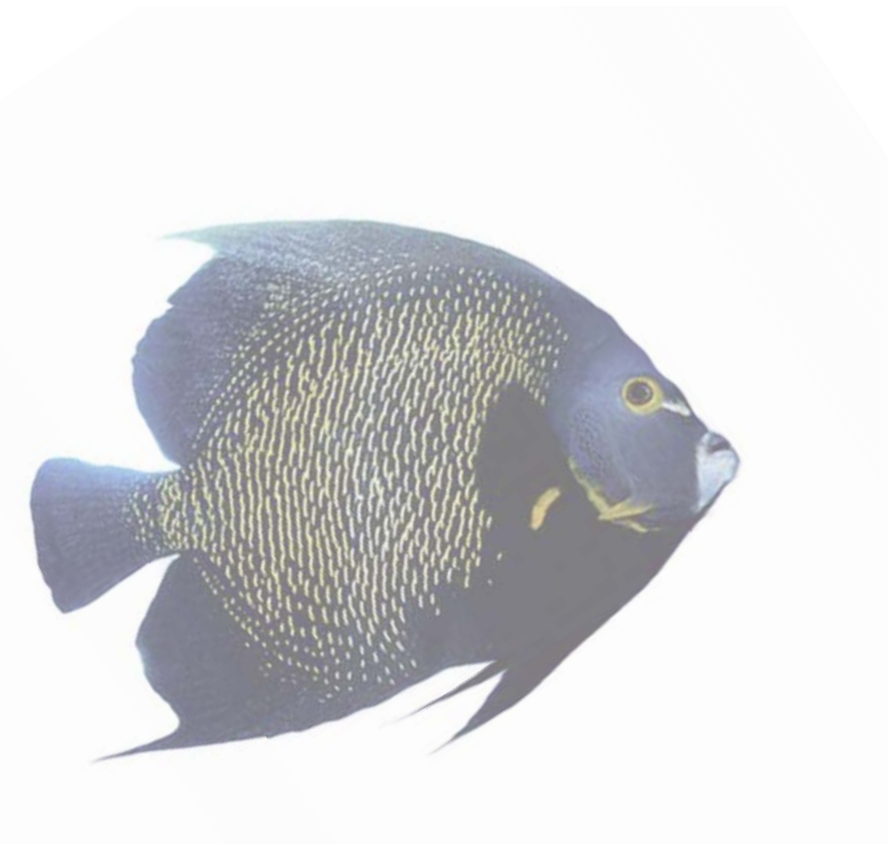
ECRI Institute PSO encourages its members to review the findings from this report and to enlist a multidisciplinary team of representatives from senior leadership, finance, clinical engineering, information technology, risk management/patient safety/quality improvement, and affected clinical departments to discuss the applicability of the findings to their health IT projects. Minimizing the unintended consequences of health IT systems and maximizing the potential of health IT to improve patient safety should be an ongoing focus of every healthcare organization. ECRI Institute PSO members can use the findings and recommendations in this Deep Dive analysis as part of their effort to achieve those goals.

In addition to the review provided by ECRI Institute PSO's Advisory Council, ECRI Institute PSO acknowledges the following individuals for their insights about this report:

- ▶ Jason Adelman, M.D., M.S., Patient Safety Officer, Montefiore Medical Center, Bronx, New York
- ▶ Leah C. Lough, Executive Vice President, Association for the Advancement of Medical Instrumentation (AAMI), Executive Director, AAMI Foundation, Arlington, Virginia
- ▶ Farah Magrabi, Ph.D., Senior Research Fellow and Leader, Patient Safety Informatics Centre for Health Informatics, Australian Institute of Health Innovation, University of New South Wales, Sydney, Australia
- ▶ Chris Riha, Senior Director, Clinical Systems Engineering, Carilion Roanoke (Virginia) Memorial Hospital
- ▶ Hardeep Singh, M.D., M.P.H., Chief, Health Policy, Quality and Informatics Program, Houston VA Health Services Research and Development Center of Excellence, Michael E. DeBakey Veterans Affairs Medical Center, and Assistant Professor, Baylor College of Medicine, Houston
- ▶ Dean F. Sittig, Ph.D., Professor, School of Biomedical Informatics at the University of Texas, Health Sciences Center at Houston

## ECRI INSTITUTE PSO DEEP DIVE: HEALTH INFORMATION TECHNOLOGY

Acknowledgments	ii
Table of Contents	iii
Executive Summary	v
Background	1
Methods	3
Results	4
Classification of Health IT Events by Safety Issue	6-16
Discussion	17-21
Risk Reduction Strategies for Health IT Projects by Strength of Impact	22
Preparation	24-29
Implementation	30-33
Continuous Improvement and Ongoing Monitoring	34-39
ECRI Institute Resources	38
Online Resources	40
References	40-41



*Healthcare providers and policymakers have embraced health information technology (IT) as an essential component of high-quality healthcare because it has the potential to provide multiple benefits: support clinical decision making, enhance provider communication, provide clinicians with access to patient data, engage patients, and reduce errors.*

*But studies also point to the so-called “unintended consequences” of health IT. Because of the large number of patients whose data is entered into an organization’s health IT system, health IT-related errors have the potential to affect many patients, and some can cause harm.*

## WHAT ECRI INSTITUTE PSO FOUND

ECRI Institute PSO reviewed 171 health IT-related events submitted by healthcare facilities during a nine-week period. Health IT problem areas identified include: inadequate data transfer from one health IT system to another; data entry in the wrong patient record; incorrect data entry in the patient record; failure of the health IT system to function as intended; and configuration of the system in a way that can lead to mistakes. Health IT must be considered in the context of the environment in which it operates during the three phases of any health IT project: planning for new or replacement systems, system implementation, and ongoing use and evaluation of the system. Shortsighted approaches to health IT can lead to adverse consequences.

## Key Recommendations

- ▶ Enlist leaders’ commitment and support for the organization’s health IT projects.
- ▶ Involve health IT users in system planning, design, and selection.
- ▶ Conduct a review of workflow and processes to determine how they must be modified.
- ▶ Evaluate the ability of existing IT systems within the organization to reliably exchange data with any health IT system under consideration.
- ▶ Conduct extensive tests before full implementation to ensure that the health IT system operates as expected.
- ▶ Provide user training and ongoing support; educate users about the capabilities and limitations of the system.
- ▶ Closely monitor the system’s ease of use and promptly address problems encountered by users.
- ▶ Introduce alterations to a health IT system in a controlled manner.
- ▶ Monitor the system’s effectiveness with metrics established by the organization.
- ▶ Require reporting of health IT-related events and near misses.
- ▶ Conduct thorough event analysis and investigation to identify corrective measures.



**AT A GLANCE**

- ▶ Health IT can only make an impact on healthcare safety and quality if it is designed, installed, and used correctly.
- ▶ Health IT-related errors can result from system malfunctions, incorrect use of the system, and faulty interfaces between different IT systems.
- ▶ As more healthcare organizations adopt health IT systems, health IT errors have the potential to affect many patients.
- ▶ PSOs provide a unique opportunity to collect, share, and learn from health IT-related events.

Healthcare providers and policymakers have embraced health information technology (IT) as an essential component of high-quality healthcare because it has the potential to provide multiple benefits, including supporting clinical decision making, enhancing provider communication, providing clinicians with access to patient data in a secure environment, engaging patients, and reducing medical errors.

**Health IT Investment**

Health IT includes hardware and software that is used to electronically create, maintain, analyze, store, or receive information to help in the diagnosis, cure, mitigation, treatment, or prevention of disease (AHRQ “Device or Medical/Surgical Supply”). For many healthcare organizations, health IT is synonymous with electronic health records (EHRs), but it also includes components of EHRs, such as bar-coded medication administration, computerized provider order entry (CPOE), medication management, emergency department (ED) documentation, laboratory information, and picture archiving and communication systems (PACS).

Significant healthcare resources are now directed at health IT. Consider the following

indicators of the nation’s sizable health IT investment:

- ▶ With funding appropriated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, the federal government is spending about \$19 billion to encourage hospitals, physician practices, and other healthcare organizations to invest in their health IT infrastructure. Most of the money will be provided as incentive payments for providers that demonstrate they have adopted and are using EHRs that meet certain criteria. (42 USC §§ 17901-17953; 42 USC §§ 300jj-300jj-51)
- ▶ Not surprisingly, IT now represents the biggest share of many healthcare organizations’ capital budgets. When asked to identify the area where their organizations will make the largest capital investment in 2012, 43% of healthcare leaders selected IT and telecommunications, an increase from 34% the previous year (Premier Inc.).

But the nation’s multibillion-dollar outlay for health IT can only make a positive impact on healthcare quality if it is planned, designed, installed, and used correctly. Just being wired to enable providers to submit medication orders electronically or view a

patient’s record from a computer screen is not a guarantee of improved patient care.

There are numerous studies to support health IT’s important role in patient safety. For example, CPOE systems can improve patient safety by eliminating transcription errors from illegible handwriting, providing clinical decision support, and alerting clinicians to potentially dangerous orders, such as a patient allergy to a selected medication (Kaushal et al.).

But studies also point to the so-called “unintended consequences” of health IT (Ash et al. “Some Unintended”). 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 screen display is confusing, resulting in a medication order for the wrong patient (Koppel et al.).

Indeed, health IT-related errors can occur under any of the following circumstances (Sittig and Singh “Defining”):

- ▶ 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.

Because of the large number of patients whose data is entered into an organization's health IT system, health IT-related errors have the potential to affect many patients (Sittig and Singh "Defining"), and evidence is emerging that some of these errors can cause harm. For example, of the 260 reports of medical device malfunctions as a result of IT or software issues submitted to the U.S. Food and Drug Administration (FDA) over a recent two-year period, 44 described injuries and 6 involved deaths (U.S. FDA). The Joint Commission has also called attention to the safety risks of health IT in a Sentinel Event Alert on safely implementing health IT (Joint Commission). In light of these concerns, researchers have coined the term "e-iatrogenesis" to refer to "patient harm caused at least in part by the application of health information technology" (Weiner et al.).

In its 2011 report *Health IT and Patient Safety: Building Safer Systems for Better Care*, the Institute of Medicine (IOM) notes that there is no central repository of data about errors that can occur as a result of health IT (IOM). While FDA's data is enlightening, it is limited to reports either voluntarily submitted to the agency or required of those health IT vendors regulated by the agency. Although FDA maintains that it has the authority to regulate health IT software, it has exercised this authority with only certain health IT systems—laboratory information systems and PACS, for example, but not EHRs (Shuren).

Individual healthcare organizations are beginning to collect health IT event data through their event reporting systems, but that information is rarely shared because of concerns that the information may be discoverable in litigation. Also, given the limited number of events identified by any one

organization, it is difficult to identify trends about health IT hazards from an organization's data. Additionally, health IT vendors may prevent organizations from sharing this information with nondisclosure clauses that prohibit users from sharing product information about health IT-related patient safety risks (IOM).

### PSOs' Role in Analyzing Health IT Events

Absent any federal mandate to collect data about health IT-related risks, IOM's report highlights the important role of federally certified patient safety organizations (PSOs) in collecting and sharing data about health IT-related events in a nonthreatening and protected manner. The Patient Safety and Quality Improvement Act of 2005 created a framework for healthcare providers to improve patient safety by sharing data with PSOs that provide analysis and feedback regarding patient safety matters in a protected legal environment. Additionally, PSOs can collect the information in a standardized format in order to aggregate the data and learn from it.

Recognizing its important role in furthering the healthcare sector's understanding of health IT-related events and unsafe conditions, ECRI Institute PSO identified health IT-related events as the topic of its second PSO Deep Dive™ analysis\* and, in April 2012, issued a call to action to its member organizations and members of its partner PSOs to collaborate in an initiative to report health IT-related events so it can share information learned from the events as well as strategies to ensure health IT can improve healthcare quality without jeopardizing patient safety.

\* ECRI Institute PSO's first PSO Deep Dive analysis on medication safety was published in 2011 and is available to ECRI Institute PSO members and members of collaborating PSOs.

This report summarizes ECRI Institute PSO's analysis of the 171 health IT-related events submitted during a nine-week period. Because the reports were voluntarily submitted, the data represents a snapshot of patient safety issues that can arise with health IT. The data does not include all health IT-related events that may have occurred at healthcare organizations during the period for the PSO Deep Dive event submissions and, therefore, cannot be used to draw conclusions about overall health IT event frequency and severity rates. But by looking at the information from the shared events, ECRI Institute PSO can provide lessons so that all its participating organizations can learn from and act on the reports.

ECRI Institute PSO's analysis is based on the information provided in the event reports. Sometimes, the event reports are sketchy in describing the circumstances of the event, which limits the ability of this analysis to delve into all the factors that contributed to the events. For example, an event report that simply indicates that a provider entered data in the wrong patient record fails to capture important details about possible human factors that contributed to the event: Was the provider distracted and trying to respond to a nurse's question when the wrong record was pulled? Was the provider unable to see the computer display because of lighting glare on the screen? To better understand the causes of health IT-related events, healthcare organizations will need to ensure that their event reports for health IT issues collect the necessary information to help the organization make improvements to their health IT systems.

ECRI Institute PSO also conducted follow-up interviews with some of the organizations that submitted events resulting in patient harm, and throughout this report, deidentified summaries of those events and organizations' strategies to prevent the events from recurring are provided.



**AT A GLANCE**

- ▶ ECRI Institute PSO organizations collaborated to learn about health IT-related events.
- ▶ Participants submitted at least 10 health IT events using the AHRQ event reporting form for health IT.

In April 2012, ECRI Institute PSO announced to its members and members of collaborating PSOs that it was launching the second in a series of PSO Deep Dive analyses to assist the healthcare community in learning about potential patient safety issues. ECRI Institute PSO asked participants to submit at least 10 health IT-related events, including issues with EHRs, laboratory information systems, ED documentation systems, networked physiologic monitor interfaces, smart infusion pumps with software to check programmed drug doses, bar-coded medication administration systems, and medication management systems.

Member facilities submitted the events using ECRI Institute PSO’s patient safety event reporting system. Because ECRI Institute PSO and the collaborating PSOs

are federally certified as PSOs, providers that report health IT events, near misses, and unsafe conditions have the assurance that the data will be kept confidential. However, ECRI Institute PSO can share deidentified findings and lessons learned from its analysis of the aggregated data.

**Common Formats for Health IT Events**

ECRI Institute PSO’s event reporting system uses an enhanced version of the Agency for Healthcare Research and Quality’s (AHRQ) common definitions and reporting formats, which allow PSOs to collect information from providers and standardize how patient safety events are represented. AHRQ’s Common Formats (version 1.2) include an event report for health IT events and unsafe conditions, enabling providers to report these events in

a systematic manner and allowing PSOs to aggregate the data. AHRQ’s health IT event report asks up to six questions about the event or unsafe condition. For example, the report asks the organization to characterize the health IT product involved in the event as one of the following: administrative/billing or practice management system; automated dispensing system; EHR or EHR component; human interface device (e.g., keyboard, mouse, touchscreen, speech recognition system, monitor/display, printer); laboratory information system, including microbiology and pathology systems; radiology/diagnostic imaging system, including PACS; or other (and described by the event reporter). Refer to “Online Resources” for information on how to download the AHRQ health IT event report.

**AT A GLANCE**

- ▶ PSO Deep Dive analysis consisted of 171 health IT events during a nine-week reporting period.
- ▶ Events were analyzed by severity and health IT systems involved.

Participating facilities submitted health IT-related events during the nine-week period starting April 16, 2012, and ending June 19, 2012. ECRI Institute PSO pulled additional health IT events that were submitted by facilities during the same nine-week period as part of their routine process of submitting event reports to ECRI Institute PSO’s reporting program. The PSO Deep Dive analysis consisted of 171 health IT-related events submitted by 36 healthcare facilities, primarily hospitals.

Reporting organizations self report their event classification by severity (i.e., incident, near miss, or unsafe condition). The majority of the reports (105, or 61%) were classified as incidents, which are defined as patient safety events that reach the patient, whether or not the patient was harmed. Another 39 of the reports, or 23%, were near misses, which are defined as patient safety events that did not reach the patient. The remaining 27 reports, or 16%, involved an unsafe condition, or a circumstance, such as a defective environment-of-care process, that increases the probability of a patient safety event. Unsafe conditions identified by reporting organizations included power failures, inadequate screen displays, and software bugs that affected the operation of the IT network. The definitions for “incident,” “near miss,” and “unsafe condition” are from AHRQ’s

Common Formats (AHRQ “Common Formats Glossary”).

Separately, reporting organizations also select a harm score for the event as illustrated in **Figure 1**. The reporting organizations are not always consistent in classifying the event and selecting a harm score. As a result, the harm scores do not always correlate with the severity scores. For example, although the reporting organizations identified 105 incidents, 39 near misses, and 27 unsafe conditions, these numbers are reported differently by harm score as

follows: 84 incidents (harm score of C and above), 15 near misses (harm score of B), and 25 unsafe conditions (harm score of A).

**Harm Score of Health IT Events**

Facilities indicated the harm score to the patient for 124 of the 171 health IT events reported to ECRI Institute PSO. The majority of the events were caught before causing harm. Of the 171 reports, 6% of the events reached the patient and contributed to or resulted in harm, which ranged from temporary harm to death. These events are summarized in boxed articles throughout

**Table 1.**  
 Health IT Systems Associated with Events, April 16 to June 19, 2012

Health IT System	No. of Events (N = 171)	% of Total Events
CPOE system	43	25
Clinical documentation system	29	17
eMAR	25	15
Laboratory information system	22	13
Pharmacy system	19	11
Human interface device (e.g., computer not functioning)	15	9
Radiology/diagnostic imaging system (including PACS)	13	8
Automated dispensing system	3	2
Clinical decision support system	2	1

Percentages do not add up to 100% due to rounding.

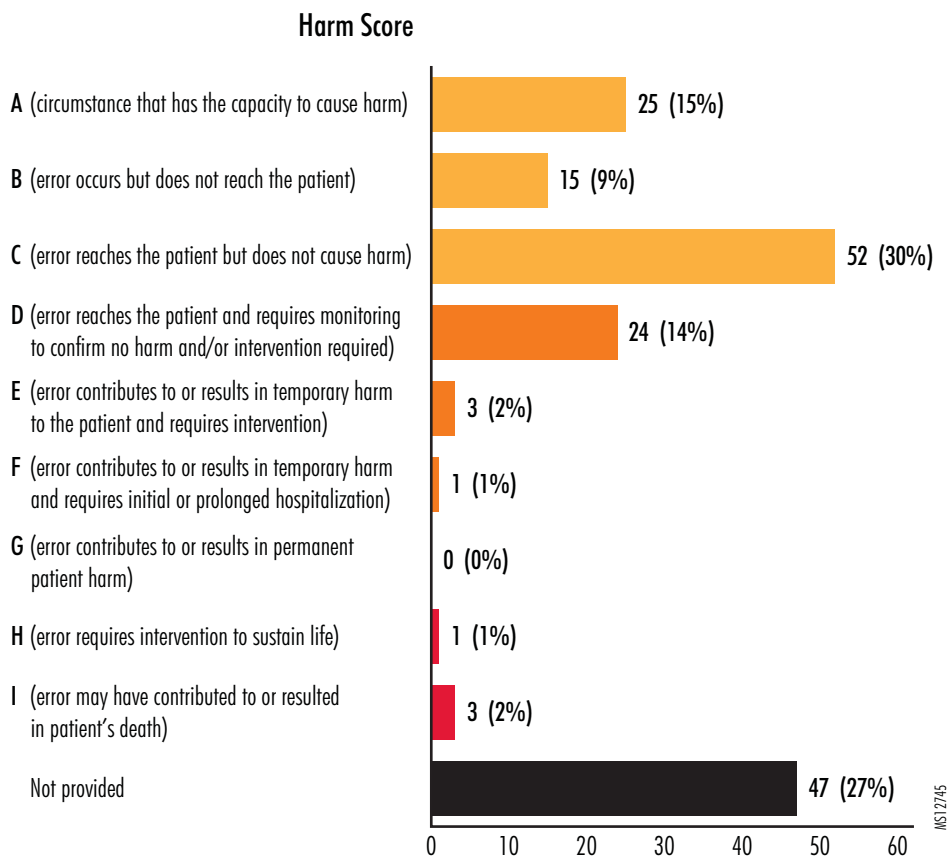
this section and include additional information collected during interviews with the organizations and not included in the event reports.

Reports resulting in patient harm are those in categories E through I using the National Coordinating Council for Medication Error Reporting and Prevention's (NCC MERP) Index for Categorizing Medication Errors. Although originally designed for medication events, the index is often used for nonmedication-related events to indicate the event's effect on the patient. See **Figure 1** for a breakdown of the reports by the NCC MERP harm score.

### Health IT Systems Associated with Events

The majority of the 171 events (53%) were associated with a health IT system for medication management, as illustrated in **Table 1**. These events involved CPOE systems (43, or 25% of all events), which were the most frequently implicated health IT systems in the analysis; electronic medication administration records (eMARs) (25, 15%); pharmacy systems (19, 11%); and automated dispensing systems (3, 2%). Following CPOE systems, clinical documentation systems, associated with 17% of the events, were the next most frequently implicated health IT systems.

**Figure 1.**  
Health IT Events by Harm Score, April 16 to June 19, 2012



Number (N = 171)

Percentages do not add up to 100% due to rounding.

MS12745

## Classification of Health IT Events by Safety Issue

### AT A GLANCE

- ▶ Health IT events were classified by 28 types of safety issues.
- ▶ A majority of events occurred at the human-computer interface.
- ▶ Top five safety issues involved system interfaces, software, and wrong-record or wrong-input errors.

With the information provided from the event descriptions, ECRI Institute PSO grouped\* the 171 health IT events based on the safety issues involved using a previously published classification system that has been used to analyze health IT events submitted to FDA's searchable Manufacturer and User Facility Device Experience (MAUDE) database (Magrabi et al. "Using FDA Reports"). FDA regulations stipulate that manufacturers and device-user facilities report to the agency any device-related events involving products regulated by the agency that result in a patient's serious injury or death, as well as device malfunctions that may result in death or serious injury if they were to recur. Additionally, manufacturers and device users can voluntarily submit adverse events involving medical devices that do not result in serious harm or death. All the event reports are kept in the MAUDE database. In addition to FDA-mandated reporting of regulated health IT products, some voluntary reporting of health IT systems that are not regulated by FDA has occurred; for example, there are some EHR-related events in the database.

The classification system, as depicted in **Figure 2**, consists of 36 categories of health IT problems; some of the categories

include subject headings for which there are subcategories to classify events. ECRI Institute PSO limited its count of health IT problem types, or safety issues, to the 27 subcategories in which health IT events can be classified.

Each category within the classification system fits into two larger groups. One group classifies events by whether the incident involved the human-computer interface or was computer- or machine-related. The other group identifies the point when the event arose: during data entry (input), transfer of the data to the health IT system (transfer), or data retrieval (output). For events that fall outside input, transfer, or output, there are two additional categories: "general technical" for hardware and software issues that arise separately, such as a computer system that is down, and "contributing factors" for variables that arise outside the context of the health IT system, such as a clinician who is multitasking while using health IT and, as a result, pulls up the wrong patient record. For its analysis, ECRI Institute PSO added a general subcategory for other types of contributing factors, such as a default-related issue (e.g., a default option was selected instead of an alternative option from a drop-down list) or a paper and EHR mismatch. As a result, there were

28 subcategories in which health IT events could be classified. ECRI Institute PSO's analysis identified events for 22 of the 28 problem types.

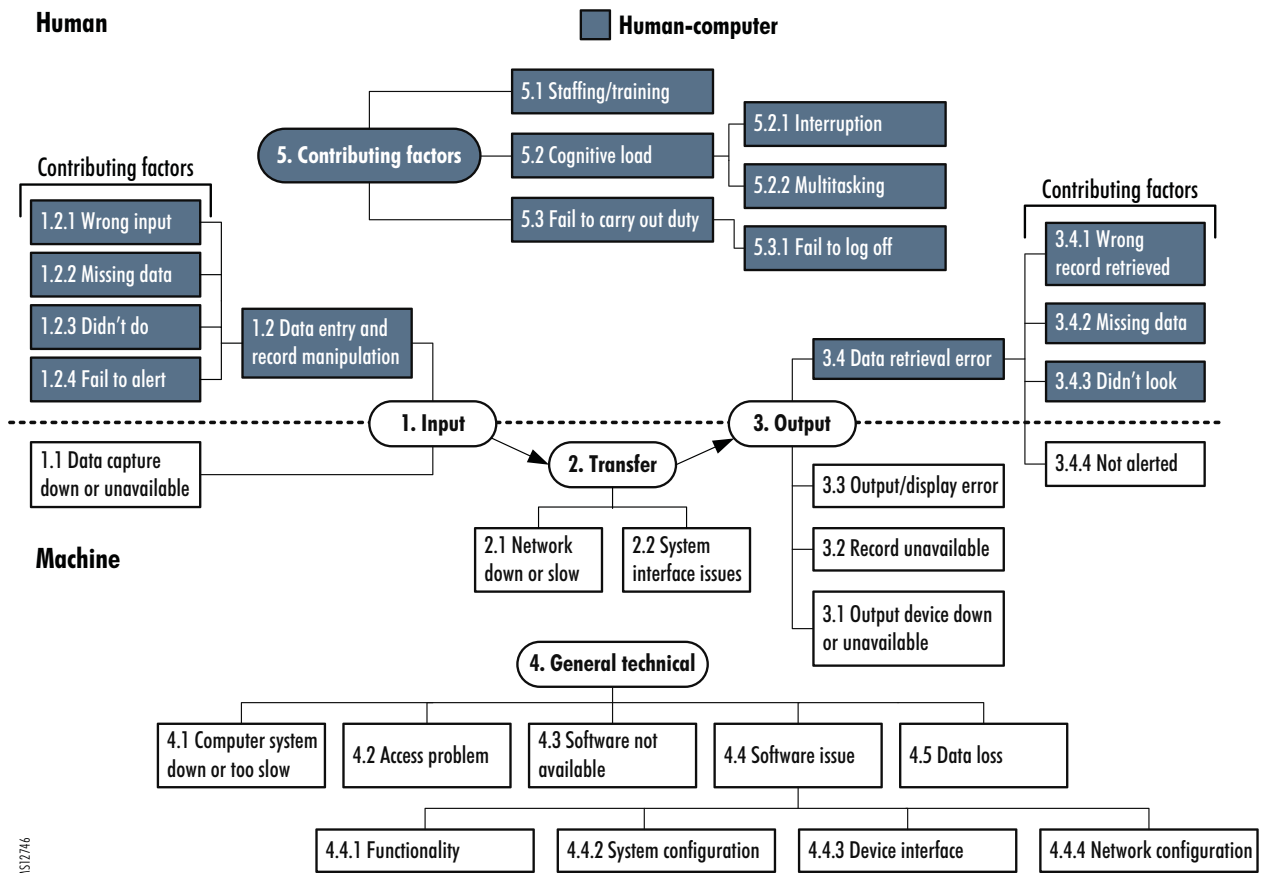
More than one safety issue was selected if the event identified multiple problems. There were 40 events that were classified in two problem types, resulting in 211 problems identified from the 171 events. As an example, one report says that important information about a surgical outpatient's medication allergies was missing from the pharmacy system (a data retrieval error) because the information did not transfer from the outpatient IT system to the EHR (a system interface issue). The pharmacist had to double-check the information with the provider:

*Pharmacy received an order to dispense an antibiotic and pain medication postoperatively for a patient in outpatient surgery. Both medications are contraindicated for patients with known allergies to the drugs. There was no allergy information for the patient entered into pharmacy system. The pharmacist consulted with outpatient surgery and verified the allergy information. The information about the patient's allergies did not cross over from the electronic health record.*

*(continued on page 8)*

\*To ensure consistency, one individual classified all 171 events.

Figure 2. Tagging Methodology



Reproduced with permission of BMJ Publishing Group Ltd. from: Magrabi F, Ong MS, Runciman W, et al. Using FDA reports to inform a classification for health information technology safety problems. *J Am Med Inform Assoc* 2012 Jan-Feb;19(1):45-53.

**Table 2.** Problems and Safety Issues Identified from Health IT Events, April 16 to June 19, 2012

Problem Type	No. of Problem Types (N = 211)	% of Total Problem Types*
<b>Data input</b>		
Wrong input	30	14
Failed to alert	10	5
Didn't do	5	2
Missing data for entry	4	2
Data capture down or unavailable	2	1
<b>Data transfer</b>		
System interface issues	33	16
Network down or slow	5	2
<b>Data output</b>		
Wrong record retrieved	23	11
Missing data for retrieval	15	7
Output/display error	10	5
Not alerted	4	2
Didn't look	1	0
Output device down or unavailable	1	0
<b>General technical</b>		
Software issue: system configuration	27	13
Software issue: functionality	20	9
Computer system down or too slow	6	3
Data loss	3	1
Access problem	2	1
Software issue: device interface	2	1
Software not available	1	0
<b>Contributing factors</b>		
Contributing factors: other (i.e., default, paper versus EHR mismatch, or wrong field for information)**	6	3
Contributing factors: staffing/training	1	0

Note: This classification of health IT events is based on a previously published classification system to analyze health IT events submitted to FDA's MAUDE database in the following article: Magrabi F, Ong MS, Runciman W, et al. Using FDA reports to inform a classification for health information technology safety problems. *J Am Med Inform Assoc* 2012 Jan-Feb;19(1):45-53.

\* Percentages do not add up to 100% due to rounding.

\*\* New category for contributing factors

(continued from page 6)

The classifications of the 211 problems identified from the 171 events are presented in **Table 2**.

### Human versus Computer?

Of the 211 safety issues identified, 118 (56%) were computer-related and 93 (44%) involved user interactions with the health IT system, or the so-called “human-computer interface” (see **Figure 3**). The results are comparable to a previous study of computer-related patient safety events using the same classification system. The study, published in 2010, found that of 117 problems from 99 incidents analyzed, 64 (55%) were computer related and 53 (45%) involved problems with the human-computer interaction (Magrabi et al. “An Analysis”).

**Computer.** Many of the computer-related events were the result of problems with system interfaces (16% of all 211 health IT problems, 28% of computer-related problems) and system configurations (13% of all problems, 23% of computer-related problems). Often, the end result was that reports of test findings were delayed or unavailable and orders were not received—all of which resulted in delays in initiating and completing clinical tasks.

In the following example, a surgeon could not electronically access a patient's radiology studies because of problems with the computer screen display:

*The surgeon tried to access a patient's radiology study from the PACS system in the OR [operating room]. The display would only show a blue screen. The patient's time under anesthesia was extended while we tried to get the computer display to work.*

Other examples of computer issues include:

- ▶ Data does not transfer from one IT system to another.

- ▶ System disruptions causing some data to be lost.
- ▶ Alerts do not display as intended for potentially dangerous medication orders.
- ▶ Incomplete patient information appears in the computer display.

**Human-computer.** Many of the events involving the human-computer interface were the result of entering the wrong data in the health IT system (14% of all 211 health IT problems, 32% of human-computer problems) or retrieving the wrong record (11% of all problems, 25% of human-computer problems). The following is an example of an event involving an incorrect data entry:

*The wrong patient weight was manually entered in electronic record. The weight was entered as 75.5 kg instead of 175 kg, which could have affected any medication dosages given.*

An example of a wrong record retrieval is as follows:

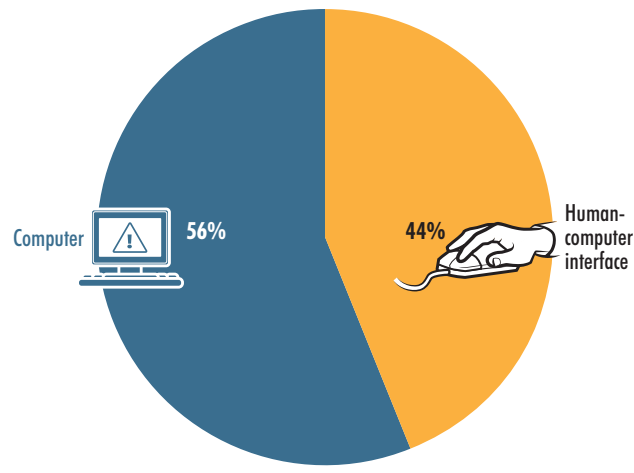
*The pharmacist entered medication orders, written and intended for one patient, for the incorrect patient. There is no system validation that the correct patient record is pulled up.*

Many of the events occurring during the human-computer interface required additional actions to correct the error, as in the following example:

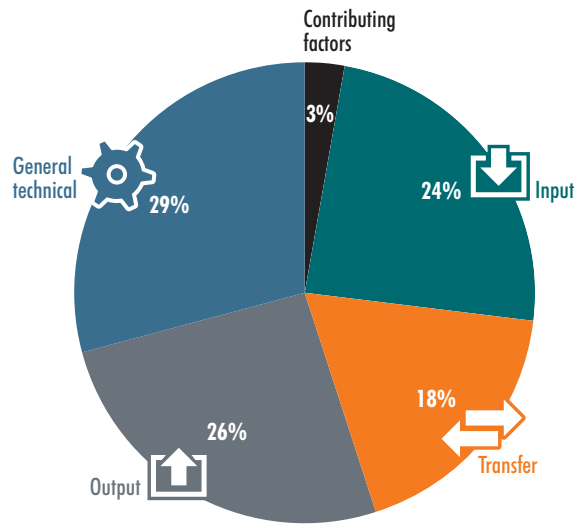
*The incorrect weight of the patient was entered on admission as 40 kg. The patient actually weighs 40 pounds. The patient's medication dose was calculated based on the patient's weight in kilograms. Pharmacy caught the error and corrected the dose based on the patient's true weight.*

The individual entering the data may have thought the patient's weight was entered in pounds, but the computer stored the information as kilograms. Without the pharmacist's intervention, the patient, a

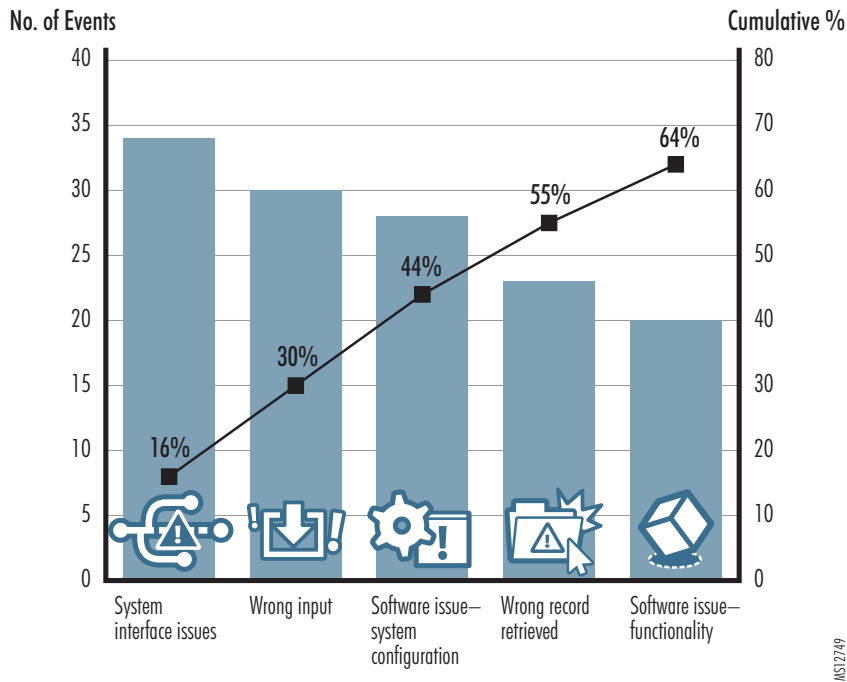
**Figure 3.** Health IT Events Classification: Computer or Human-Computer Interface, April 16 to June 19, 2012



**Figure 4.** Health IT Events Classification: Date Input, Output, Transfer, or Other; April 16 to June 19, 2012



**Figure 5.**  
Top Five Safety Issues from Health IT Events, April 16 to June 19, 2012



These five problem types represent 64% of all 211 safety issues involving health IT events in ECRI Institute PSO’s Deep Dive analysis.

child, would have received a medication dose intended for a person more than two times the patient’s actual weight.

### General Technical Problems

As illustrated in **Figure 4**, the largest percentage of the 211 safety issues (29%, or 61 problems) were associated with general technical hardware and software issues, 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.*

The largest percentage of general technical problems involved the software subareas of system configuration and functionality,

which represented 13% and 9%, respectively, of all the safety issues cited in the analysis and were among the top five health IT problem types identified in the analysis (refer to **Figure 5** to view the top five health IT problem types).

Examples of software problems affecting the system configuration or functionality 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.

- ▶ An error message displays each time a particular medication is ordered.
- ▶ The system does not alert when a pregnancy test is ordered for a male patient.
- ▶ After a laboratory order for a cardiac test is mistakenly ordered for every four hours over the next 12 days instead of the next 12 hours, the lab is unable to cancel all the extra days from the order, so the order is restarted after three days.
- ▶ An order entry system does not allow a physician to transfer the care of a patient to another physician.
- ▶ An influenza vaccine order does not drop off the active work list after it is given.

*(continued on page 12)*



## Hospital Resorts to Workaround for Pharmacy and Lab IT Systems

Although a hospital bought its medication management and laboratory information systems from the same vendor, the two systems are unable to coordinate the special timing for laboratory tests to evaluate drug levels with the administration of the first dose of aminoglycoside antibiotics for cystic fibrosis patients being treated for worsening of pulmonary symptoms. The lab specimen should be drawn two hours after the first antibiotic dose so that pharmacokinetic analysis can determine optimal dosing at the earliest point in the patient's stay.

Even though the two health IT systems were developed by the same vendor, the hospital has been unable to develop an automatic trigger to initiate the specimen draw for laboratory testing two hours after the first antibiotic dose is administered. Consequently, the ordering physician uses

a timed study designation in the electronic record when the antibiotic and lab test are ordered. The clinician inserts instructions in the comment field that the lab specimen must be drawn two hours after the first dose of antibiotic. Because these instructions can be easily overlooked in the comment field, the lab sample for therapeutic drug monitoring is often drawn with other laboratory tests conducted on the patient's admission. The sample ends up being processed before the patient receives the first antibiotic dose. Inaccurate timing of the lab test can lead to life-threatening delays in achieving effective doses of the antibiotic for cystic fibrosis patients.

A clinical pharmacist on-site works directly with the ordering physician, nurses, and lab to ensure that the laboratory sample is obtained two hours after the first

antibiotic dose is administered. Since the pharmacist is only on-site on weekdays, there is more risk of timing errors on weekends and during after-hours when an on-site clinical pharmacist is unavailable to manage the process. As a workaround, clinicians will initiate therapeutic drug monitoring around the second dose of antibiotic in an effort to separate the lab draw from the admission labs. The hospital reports that it is still exploring ways to improve the interface between its laboratory and pharmacy IT systems, but until one is developed, it will continue to rely on its clinical pharmacist to ensure appropriate timing of therapeutic drug monitoring tests for cystic fibrosis patients who are starting antibiotic therapy for acute pulmonary exacerbation.

## Confusing eMAR Display Truncates Drug Dosing Information

A hospital's eMAR system truncated 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 the patient complained of pain, the patient was given both formulations of the drug at the same time, causing the patient to suffer a respiratory arrest. Morphine is a high-alert medication, which according to the Institute for Safe Medication Practices, can cause serious patient harm when used in error (ISMP). After the patient was successfully intubated and resuscitated, the order for the patient's

as-needed pain medication was switched to hydromorphone.

Following the event, the organization worked with its health IT vendor to ensure that the eMAR display for "morphine" included the 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 vendor correct the display to show the dosing information.

**Source:** Institute for Safe Medication Practices (ISMP). ISMP's list of high-alert medications [online]. 2012 [cited 2012 Oct 24]. <http://www.ismp.org/Tools/institutionalhighAlert.asp>.

## Beware When the Clock Strikes Midnight

A doctor ordered a change in the frequency of a neonate's antibiotic from every 12 hours to every 18 hours. The intravenous infusion was needed to protect the prematurely born infant from life-threatening bacterial infections. The organization's protocol for a medication schedule change requires the patient's nurse to enter schedule changes in the eMAR as indicated by routine care processes.

After starting a new infusion for the infant near midnight, the nurse noted in the eMAR that the next infusion should be given at 3 p.m. the next day, which was a Tuesday. The nurse miscalculated the timing of the next dose, which should have been indicated for 6 p.m. the next day. Also, because the information was entered near midnight, the timing of the next dose was recorded as 3 p.m. for Wednesday, resulting in a longer interval than prescribed before the next antibiotic treatment. The nurse discovered and reported the dose omission at the start of the Wednesday afternoon shift. The infant was continuously monitored for signs of sepsis infection and, despite the dose omission, did not develop any bloodstream infection during the hospital stay.

The organization reported the event to ECRI Institute PSO to raise awareness about the vexing midnight problem with electronic orders and continues to work with the users of its order entry system to ensure they are aware of the technology's limitations and the importance of rechecking all medication orders entered into the system. While the system does alert users if they attempt to schedule a medication for a time in the past, it does not alert users if they schedule a medication for a day and time greater than 24 hours in the future.

(continued from page 10)

About 3% of the safety issues were related to computer downtime, as in the following event, which also captures the reporter's frustration with the system's temporary unavailability:

*The computer is nonfunctional. Clinicians cannot look up lab test results, order treatments promptly, or determine the next appropriate action for patients.*

Often, health IT users resorted to workarounds until the technical problems were fixed. For example, one event notes that a pharmacist set up "special-day" orders in the medication management system because it would not permit the pharmacist to order different doses of a medication on alternating days. Another event, summarized in "Hospital Resorts to Workaround for Pharmacy and Lab IT Systems," illustrates the shortfalls of workarounds to overcome system flaws.

### Data Output Problems

Data output problems occurred with 26% of the 211 safety issues. The largest share of these problems were associated with retrieving the wrong record, one of the top five problem areas identified in the analysis of health IT events. Wrong-record retrieval comprised 11% of the problems cited in the analysis, often resulting in a medication order for an incorrect patient. In the following 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.*

While medication orders were often affected when the wrong record was retrieved,

the problem could affect other types of orders, such as those for radiology studies:

*I ordered a chest x-ray for the wrong patient when I accidentally clicked on the wrong patient room number. I noticed right away that I had placed the order for the patient in room 225 instead of the patient in room 224. I promptly discontinued the order but not in time for the x-ray technician to see that the order was withdrawn. The technician performed the test on the wrong patient. I should have called the x-ray department to notify that I cancelled the test. I notified the doctor and the patient of the error.*

Some of the event reporters noted that their health IT systems did not have a process for checking that orders are placed for the correct patient, as in the following event:

*Physician entered the medication order for the incorrect patient. The error was caught before the medication was administered. There is no validation in the order entry system asking if the orders are being placed for the correct patient.*

Other data output events were associated with retrieved records that were missing data (7% of all event classifications), such as information about patient allergies or an insulin drip protocol, and output display errors (5%).

When such events occurred, important information about the patient could be missed, as in the following display error:

*Upon admission to the unit, the patient required suicide precautions, including 1:1 monitoring. This information is not showing in the display of the patient's record, although the information was provided during the handoff.*

In another event, the medication dose did not display in the eMAR:

*The physician ordered an antibiotic. The eMAR showed the drug name and volume but not the dose. The physician ordered 200 milligrams (mg), but the patient received 400 mg because the drug is only stocked in that dose.*

One event, resulting in serious harm to the patient, occurred because of a confusing display for opioid orders, resulting in the patient receiving too much of the drug. The event, and the organization's strategy to improve the display, is described in "Confusing eMAR Display Truncates Drug Dosing Information."

### Data Input Problems

Events associated with data entry represented 24% of the safety issues identified in the analysis. The most common problem with data input was entering incorrect data about the patient, such as weight, drug allergies, or identification number. In fact, the "wrong input" classification represented the second most frequently identified problem type, comprising 14% of all safety issues identified in the PSO Deep Dive analysis. Typical of such events 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.*

Sometimes, pertinent information, such as the patient's height and weight, was omitted, as in the following:

*The patient's height and weight were not entered into the electronic record when the patient was admitted. The patient required nutritional therapy, so the pharmacist used the patient's weight of 85 kg from the patient's previous admission of two years ago to prepare the solution. The dietician asked about the weight used to calculate the amount of nutritional therapy since there was no documented weight in the electronic record. The patient's current weight is 65 kg. If this had not been caught, the solution would have contained too much protein for a patient weighing 65 kg.*

## Critical Lab Results Overlooked without Full Interface for Different Health IT Systems

The interface between a hospital's laboratory information system and its transplant surgery database only allowed for certain laboratory test results to reach the transplant database. For additional test result information, the transplant team had to access the laboratory system and the organization's EHR system. When a transplant patient underwent laboratory testing, the critical test results indicating possible transplant rejection were reported to the laboratory information system but not to the transplant surgery database; the interface between the two systems did not permit results reporting of the particular laboratory test.

Because there was an incomplete interface between the two systems, 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 system for those 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" in the transplant database. In this case, 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 organization adopted the following measures to prevent a similar event from recurring:

- ▷ Rebuilt the interface between the laboratory information system and transplant surgery database to ensure more complete lab results reporting to the transplant staff
- ▷ Designed a more proactive process to run laboratory reports of results requiring follow-up
- ▷ Educated transplant staff on using additional features of the organization's EHR system to assist in the follow-up process
- ▷ Developed written guidance for organ transplant patients on life after transplant surgery and when to seek medical care

## Outpatient Prescribing System's Interface to Organization's EHR Inadequate to Ensure Pharmacy Oversight

A cancer patient receiving chemotherapy on an outpatient basis was also taking a medication that affects metabolism of the chemotherapy drugs. During an inpatient admission, a consulting physician changed the medication to a different agent. The change should have prompted a dose reduction in the patient's chemotherapy regimen; however, neither the patient's daily progress notes nor the discharge note indicated the medication change, so the chemotherapy dosage was not decreased as appropriate with the medication switch.

Typically, information from the outpatient e-prescribing system is downloaded to the organization's EHR system to

provide decision support, such as medication review for possible drug-drug interactions and other incompatibilities, in the care of patients. The e-prescribing system did not support injectable and intravenous medications or any chemotherapy medications. Therefore, it was not possible to alert clinicians of potential or actual drug-drug or dosage interactions between the chemotherapy drugs and noncancer medications.

The oncology team was unaware that the cancer patient's noncancer medication had changed and of the subsequent need to lower the dose of the patient's chemotherapy regimen to prevent toxic buildup of the cancer treatment drugs.

The patient suffered disabling nerve damage from the continued infusion of the chemotherapy drugs at the toxic levels. Although the organization was in the process of adopting a new enterprise-wide EHR system with reliable interfaces to all its healthcare settings, it enacted interim procedures to prevent similar events until the new EHR system was in place. For example, it developed order sets for specific combinations of cancer drugs and other medications to prevent known drug-drug interactions, and it recommended pharmacy oversight of all chemotherapy regimens in the outpatient setting to ensure review of all chemotherapy orders and any other medications that cancer patients are taking.

A clinician can enter an incorrect order by selecting the wrong item from a drop-down menu, as in the following report:

*The drug was ordered as an intramuscular injection when it was supposed to be administered intravenously. The physician did not choose the appropriate delivery route from the drop-down menu.*

Additionally, clinicians might enter information in the wrong field of the patient record, as described in the following event:

*The physician ordered heparin in the communication section of the patient record, not the order entry section. The order could have been missed. Also, the order was placed for the wrong patient.*

Data input errors can also occur if the person entering the information is distracted:

*The nurse noted that a patient had a new order for acetaminophen. After speaking with the pharmacist, the nurse determined that the order was*

*placed for the wrong patient. The pharmacist had two patient records open, was interrupted, and subsequently entered the order for the wrong patient.*

Data entry errors can also occur due to a phenomenon known as the "midnight problem" (Ash et al. "Some Unintended"). For example, if an order is placed near midnight, any order that is checked in the computer as starting "tomorrow morning" may not take effect for another 24 hours, as in the following report:

*The physician ordered an antibiotic to start immediately and to be given again every six hours. Because the order was entered after 11:30 p.m., the next repeat dose was recorded as 2/24/12 at 6:00 a.m. instead of 2/23/12 at 6:00 a.m.*

The event summarized in "Beware When the Clock Strikes Midnight" illustrates that the so-called "midnight problem" can result in delayed administration of vital medications.

Often, data input problems were caught by vigilant staff members who questioned the accuracy of information in the electronic record or sought additional guidance about an order, as in the following event:

*The physician used the order entry system to order multiple pain medications for the same indication. The nurse asked the pharmacist to review the order. The order was clarified with the physician, and the multiple medications were not administered to the patient. The system did not trigger an alert for multiple pain medications ordered for the same indication.*

The above event was classified as a "failed to alert" data input problem, occurring with 5% of all safety issues identified in the analysis.

### Data Transfer Problems

Problems in the transfer of information, occurring with 18% of the safety issues

## Hybrid Approach to Paper and Electronic Records Creates Gaps in Communicating DNR Status

An organization in the process of converting to fully digital records was still documenting patient information with a mix of paper and electronic documentation when it discovered that the hybrid approach hindered important patient DNR information from reaching all those who needed it.

A patient with metastatic cancer had signed DNR orders upon admission to the hospital. The information was electronically documented in the hospital's electronic nursing documentation system and included in the patient's paper chart. Because the electronic nursing documentation system was not connected to other IT systems within the facility, other departments could not access the information electronically.

When the patient was transported to the radiology department for diagnostic imaging studies, the paper chart, with information about the DNR status, did not accompany the patient, and the transporter was unaware of the patient's DNR request. The IT system in the radiology department was not connected to the electronic nursing documentation system, so the department staff did not have access to the patient's DNR information.

During imaging, the patient suffered an anaphylactic reaction to the contrast dye used for the imaging study, so a code team was called. Nearby ED staff reached the patient and began resuscitation when a nurse from the unit where the patient was being treated arrived at the radiology

department and informed the code team of the patient's DNR. The code was stopped, allowing the patient to die.

Although patients' DNR information will be available to all departments once the organization converts to an enterprise-wide EHR system, the facility adopted interim measures to ensure patients' code statuses are communicated when they are taken to other departments for care. For example, the code status is indicated on the "ticket-to-ride" documentation provided to transporters taking the patient from one care area to another, and the handoff communication between the care unit and transporter, as well as the transporter and the receiving department, covers information about a patient's code status.

identified with health IT events for the analysis, can happen if there are snags with system interfaces or if the computer network goes down. System interface problems were the most commonly identified health IT problem, representing 16% of all problem types analyzed. These events often resulted in missed orders for medications and various other types of tests, as in the following two examples:

*The physician ordered that 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. We are seeing sporadic occurrences of medication orders not being received by the pharmacy system. The IT department says a planned upgrade will address the problem.*

*The nurse entered an order for a patient to have an electrocardiogram. The order was not received by*

*the cardiopulmonary department. The IT department reported that there was a problem during the data transfer of the order.*

Significantly, system interface problems were implicated in two of the eight events that reached the patient and contributed to or resulted in harm. One event described in "Critical Lab Results Overlooked without Interface for Different Health IT Systems" illustrates the serious ramifications that a partial interface between two health IT systems had in providers missing important test results. The other event, recounted in "Outpatient Prescribing System's Interface to Organization's EHR Inadequate to Ensure Pharmacy Oversight" involved an incomplete interface between an organization's outpatient e-prescribing program and its EHR system. Without sufficient information to review drug regimens of patients in the outpatient setting, the pharmacy

department did not recognize that one cancer patient was receiving toxic levels of chemotherapy drugs.

Problems with transferring information as a result of network downtime were cited in 3% of the events of the analysis. One of those events almost endangered the resuscitation of a patient when a code was called. The nurse call system went down when the code-blue button on the system was pressed. Fortunately, a physician and respiratory therapist were nearby and able to resuscitate the patient. The organization classified the incident as a high-severity event that could have caused patient harm. The organization's IT department was unable to replicate the problem with additional testing.

### Contributing Factors

The events grouped into the category "contributing factors," representing about 3% of

the problem types identified in the health IT event analysis, describe some of the various human factors that can contribute to patient safety events. A human factors approach analyzes an individual's performance within the context of the surrounding environment. For example, a person who is multitasking may be too distracted to notice that he or she is entering information in the wrong patient record.

Of the seven events involving contributing factors, four were linked to systems that had not fully converted to the electronic environment and were still using some paper systems for compiling patient data. The events suggest that staff were inadequately

trained in how to use the hybrid approach, as in the following:

*When the medication administration screen was up for the particular patient, two medications appeared, so I scanned the medication labels and gave the medications at 17:00. I later realized the medications were ordered for bedtime, as listed in the medication administration sheet.*

As summarized in “Hybrid Approach to Paper and Electronic Records Creates Gaps in Communicating DNR Status,” a facility's combined use of both paper and electronic records almost jeopardized a do-not-resuscitate (DNR) request when a seriously ill patient with DNR orders had an adverse reaction to contrast dye.

## Staff Training Essential

Concerns about insufficient staff preparation in using organizations' health IT systems are reflected in the following report:

*The staff member says there is not enough support with training and providing assistance in using the health IT system.*

Indeed, poorly implemented health IT systems can challenge the patience of its users and lead to many of the unintended consequences and patient safety incidents described in the health IT events submitted to ECRI Institute PSO. The next section of this report describes strategies available to healthcare organizations to ensure that health IT systems are used as intended—to improve patient care—and do not create new opportunities for error.

AT A GLANCE

- ▶ Consider health IT solutions in the context of the socio-technical model—the environment in which health IT operates.
- ▶ Divide strategies for health IT solutions into three phases: preparation, implementation, and continuous improvement and monitoring.
- ▶ Incorporate a hierarchy of error-reduction techniques in the health IT adoption strategy.
- ▶ Remember: shortsighted approaches to health IT during any of the three adoption phases can doom its success.

*One fundamental but seldom voiced barrier to our reaching health IT's potential is our systematic refusal to acknowledge health IT's problems, and, most importantly, to learn from them. (Koppel)*

The health IT events reported to ECRI Institute PSO reinforce findings in the clinical literature about the unintended consequences of the technology. Although healthcare facilities are adopting health IT to improve care delivery, they nevertheless encounter errors associated with the technology's use. Indeed, in its annual list of top 10 health technology hazards for 2013, ECRI Institute identified health IT issues as 3 of the 10 topics. Refer to "ECRI Institute Resources" for information on accessing the report online.

As the events in this analysis illustrate, errors can occur at any point with health IT data management—when data is entered (e.g., the wrong drug, dose, or mode of delivery is selected from a lengthy drop-down list), when data fails to transfer from one health IT system to another (e.g., critical laboratory test results cannot be sent electronically from the laboratory information system to another clinical information system), and when data is retrieved for patient care activities (e.g., digital diagnostic imaging studies do not display on an operating room monitor).

While the published literature suggests that the incidence of health IT-induced events is low—representing under 1% of all errors (Ash et al. "Roadmap")—this rate, when applied to the universe of patients whose care is managed in some way by a health IT system, has the potential to affect a large number of people. The possible number of individuals who could be affected will likely increase given the push by healthcare organizations to adopt health IT in the next few years while the federal and state governments, with funding from HITECH, are providing incentive payments to those organizations that can demonstrate they use EHRs to achieve certain goals established by the federal government.

As researchers have pointed out, the push to adopt health IT systems within a short time frame may have its own unintended consequences as a result of poorly implemented systems by organizations that fail to address the complex issues involving health IT (Coiera et al.).

Health IT problem areas identified by ECRI Institute PSO's Deep Dive analysis include the following:

- ▶ Inadequate data transfer from one health IT system to another (e.g., a drug regimen provided to a patient in the outpatient setting is not reviewed by

a pharmacist, because the outpatient prescribing system does not send all appropriate data to the pharmacy medication management system)

- ▶ Data entry in the wrong patient record (e.g., medication order entered for the wrong patient)
- ▶ Incorrect data entry in the patient record (e.g., patient's weight recorded is in kilograms when the number reflects pounds)
- ▶ Failure of the health IT system to function as intended (e.g., a vaccine order does not drop off the active list of medications to be given to a patient after it is administered)
- ▶ Configuration of the health IT system in a way that can lead to mistakes (e.g., a bar-code scanner does not record the correct medication dose into the eMAR when the medication label is scanned)

Some of the event reports hint that health IT users are quick to blame technology for the incident—"there is no validation in the system asking if the orders are placed on the correct patient," says one report—even though 44% of the events in the analysis were a result of problems with the interface between people and computers, often as a result of poor system usability (e.g., distractions from too many

decision-support alerts, confusion from a lengthy drop-down list) or other human factors.

While health IT is designed to help providers and others at healthcare organizations do their jobs better, this goal can only be accomplished if health IT is used correctly. Health IT is not a replacement for human judgment and, in fact, human vigilance is needed to ensure appropriate use of health IT to improve patient care (Ash et al. “Some Unintended”). Providers must be aware of the unintended consequences of health IT, as identified in this analysis and elsewhere in the clinical literature, to intervene to prevent the problems that health IT can both

promulgate and hide. Indeed, some of the events in this analysis were caught by attentive providers—for example, a nurse who asked a pharmacist to review a questionable medication order that should have been flagged by the order entry system—before patients could be harmed.

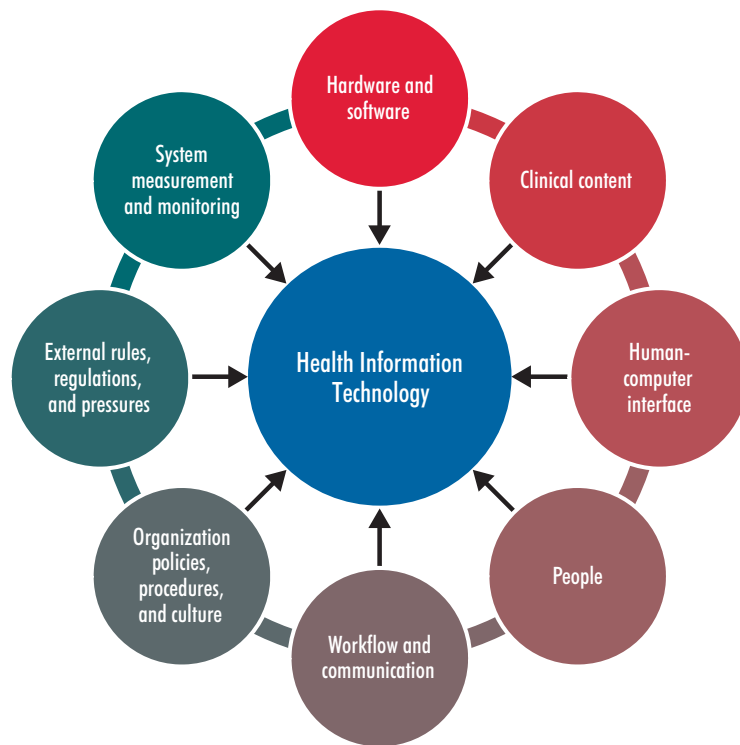
Researchers have coined the concept of the socio-technical model for evaluating health IT in healthcare systems. The model (as illustrated in **Figure 6**) emphasizes that health IT does not operate in a vacuum and must be considered within the context of eight dimensions that affect the development, implementation, and ongoing application of health IT in a complex

healthcare system (Sittig and Singh “A New Socio-technical Model”).

The eight dimensions of a socio-technical model for evaluating health IT are as follows (Sittig and Singh “A New Socio-technical Model”):

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)

**Figure 6.** Socio-technical Model for Health IT



**Source:** Sittig DF, Singh H. A new socio-technical model for studying health information technology in complex adaptive healthcare systems. *Qual Saf Health Care* 2010 Oct;19(Suppl 3):i68-74.



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

In short, health IT must be considered in the context of the environment in which it operates. The eight dimensions of the socio-technical model must be addressed during all phases of health IT adoption—during planning for new or replacement health IT systems, health IT implementation, and

ongoing use and evaluation of the system. If, for example, a medication management system does not match the workflow that clinicians, nurses, and pharmacists are accustomed to follow to order, dispense, and administer medications, the system could interfere with care delivery. If the organization does not evaluate its existing infrastructure’s ability to support a health IT system, it could be caught off guard by a computer crash triggered by an outdated network, as happened at one Boston hospital (Kilbridge).

An organization’s health IT system is doomed to failure if the multidimensional aspects of health IT are not addressed

## A Tale of Two CPOE Systems

The feasibility of safely implementing commercially available CPOE systems in hospitals was hotly debated after a 2005 study concluded that a commercially available CPOE system that was adopted at a children’s hospital was associated with an increase in patient mortality. Prescribers and other providers struggled to adjust to the new technology, which was implemented over a six-day period. For example, orders that once took a few seconds to submit on a written form required an average of 10 clicks with the CPOE system, or almost one to two minutes of the prescriber’s time. (Han et al.)

A subsequent study showed that the same system was not associated with an increase in mortality at another children’s hospital after months of careful planning and implementation, including active involvement of multiple departments (Del Beccaro et al.). Others said that trying to adopt a CPOE system in six

days “goes beyond challenging and borders on the temerarious” (Sittig et al.).

### References

- Del Beccaro MA, Jeffries HE, Eisenberg MA, et al. Computerized provider order entry implementation: no association with increased mortality rates in an intensive care unit. *Pediatrics* 2006 Jul;118(1):290-5.
- Han YY, Carcillo JA, Venkataraman ST, et al. Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. *Pediatrics* 2005 Dec;116(6):1506-12.
- Sittig DF, Ash JS, Zhang J, et al. Lessons from “Unexpected Increased Mortality after Implementation of a Commercially Sold Computerized Physician Order Entry System.” *Pediatrics* 2006 Aug;118(2):797-801.

during all phases of its adoption. The story of two organizations' very different approaches to adopting a CPOE system from the same vendor, as described in "A Tale of Two CPOE Systems," underscores the need for a well-planned and well-executed approach to health IT.

The strategies provided in this Deep Dive analysis consider health IT within a socio-technical context. They are not solely limited to important safety features such as technology design and user training but incorporate important factors ranging from organizational goals and objectives for adopting health IT to alignment of health IT with clinical workflow. The strategies are divided into three phases of health IT adoption, as follows:

1. Preparation (covering aspects such as health IT needs assessment and vendor evaluation)
2. Implementation (addressing factors such as system testing before it goes live and user training)
3. Continuous improvement and ongoing monitoring (encompassing ongoing strategies to monitor the health IT's function as well as measures to ensure health IT users do not resort to workarounds as easy fixes for suboptimal health IT design)

Of course, attention to patient safety is embedded in every strategy and all three phases of health IT adoption.

As noted in IOM's report, health IT systems—if designed, implemented, and used appropriately—can transform care delivery. Shortsighted approaches to any one of the three phases to health IT adoption can lead to adverse consequences—for example, dosing errors, failure to detect

fatal illnesses, or delays in treatment—as described in the events submitted to ECRI Institute PSO. Following the recommendations outlined in this report will reduce the likelihood of unintended outcomes from health IT.

To assist healthcare organizations with health IT adoption, ECRI Institute PSO has grouped the strategies discussed in this report by their impact—whether high, medium, or low—in preventing adverse outcomes (see "Hierarchy of Error-Reduction Techniques" for an explanation of this approach). The strategies are summarized by strength of impact and stage of health IT project adoption in the table, "Risk Reduction Strategies for Health IT Projects by Strength of Impact." These strategies apply for any type of health IT system, whether a stand-alone laboratory

## Hierarchy of Error-Reduction Techniques

Experts in system safety have developed a hierarchy of error-reduction techniques based on the impact that they can have in preventing errors. The high-impact strategies, which "design out" the hazard, are considered the most powerful and most desirable strategies because they can eliminate hazards. For example, high-impact strategies incorporate fail-safe mechanisms and forcing functions that provide a barrier or safeguard to prevent a hazard from adversely affecting the process. An example of a forcing function is an order entry system that will not open a patient record until the user reenters patient identifying information, which reduces the likelihood that orders are placed in the wrong patient record.

Moderate-impact strategies do not eliminate a hazard but use techniques such

as standardization, process simplification, warnings, and alarms to reduce the likelihood that errors will occur. While effective, these error-reduction techniques are rated as moderate because they are highly dependent on the behavior of people using the system. For example, CPOE systems allow a facility to create standardized order sets that can be activated for certain clinical routines, replacing the need to input a sequence of individual orders. If properly implemented with input from clinicians, pharmacists, and others, order sets can help increase clinicians' compliance with standardized care protocols, as well as reduce the likelihood of data entry errors.

Low-impact strategies use special policies and procedures and education to reduce errors. For example, health IT users should

not be allowed to use a newly installed or updated system unless they have completed training and demonstrated competence in using the system. By itself, the training policy will not prevent all mishaps, but, in combination with other measures, such as standardized order sets and measures to prevent wrong-patient orders, training will contribute to overall safety and heightened user awareness of health IT's limitations.

In sum, consider the various high-, moderate-, and low-impact approaches listed in **Figure 7** when developing strategies for health IT adoption. A plan should include all three approaches. Of course, organizations should choose those safety strategies that will have a higher impact in preventing unintended consequences from health IT as often as possible.

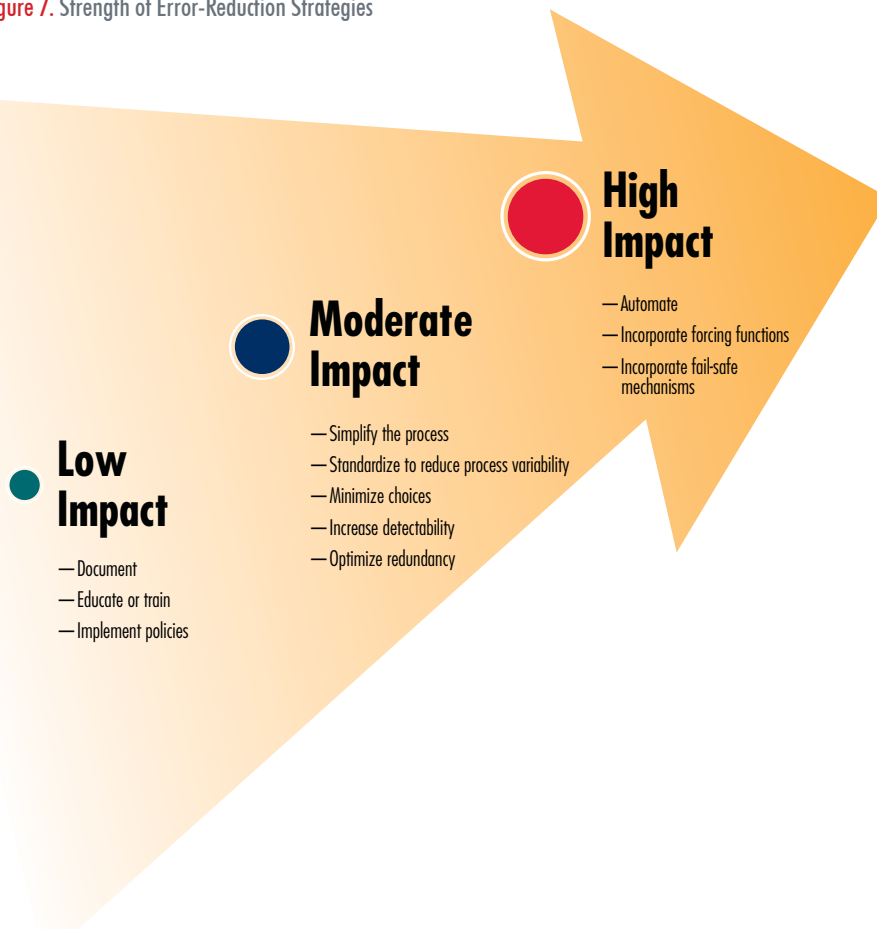
information system or an enterprise-wide EHR system.

Additionally, ECRI Institute PSO has developed a Self-Assessment Questionnaire (SAQ), called “Self-Assessment Questionnaire for Health IT Projects,” to identify some of the specific patient safety and risk management issues that organizations must address with every health IT system project. The SAQ prompts organizations to explore many of the issues identified from this analysis; it can be used to identify the strengths

and weaknesses in the organization’s risk management approach to health IT and focus on those areas requiring attention.

The SAQ is available as a supplement to this report. A downloadable version of the SAQ is available on your PSO member site.

Figure 7. Strength of Error-Reduction Strategies



MS11546



# Risk Reduction Strategies for Health IT Projects by Strength of Impact\*

## PREPARATION PHASE

Low Impact	Moderate Impact	High Impact
<p>Show leadership’s support for the project.</p> <p>Allow sufficient time for planning and implementation; some health IT projects are multiyear initiatives.</p> <p>Be willing to commit the necessary time and resources to the initiative.</p> <p>Engage a multidisciplinary committee, comprising individuals from every area affected by the project, in planning and decision making.</p> <p>Identify physician and nurse leaders with informatics experience to serve as health IT champions.</p> <p>Visit other hospitals and healthcare organizations that have adopted health IT systems, particularly the same systems under consideration by the organization, to learn about their experiences and lessons learned.</p> <p>Prepare for the exchange of electronic information with other providers in the community by assessing the interoperability needs of health IT systems across the continuum of care within the community.</p>	<p>Define the organization’s goals and objectives for the health IT project.</p> <p>Evaluate the facility’s infrastructure and IT network to assess the organization’s ability to support increased demand from the health IT system and target areas needing improvement.</p> <p>Assess employees’ and other staff members’ current computer practices and readiness for a new health IT system, and use the findings to guide health IT planning and decision making.</p> <p>Evaluate current clinical and administrative work practices (including those for clinical orders, documentation, and policies and procedures) affected by the project and, with user input, rework the practices for the electronic environment.</p> <p>Rethink work practices to make efficiency improvements, to eliminate process breakdowns, and to take advantage of automation and other benefits of an electronic environment.</p> <p>Develop, with input from users, a list of questions to evaluate a health IT system’s usability and features that promote safe use (e.g., intuitive data display, easy navigation, consistency in screen display).</p> <p>Evaluate a health IT system’s ability to exchange data with other existing and planned IT systems and medical devices within the organization.</p> <p>Require that the health IT system vendor support inter-operability through adherence to standard formats that enable data sharing among health IT products.</p> <p>Negotiate commitments from vendors in contracts to work with the organization’s IT department to build system interfaces or, at a minimum, provide, at no charge, the documentation for the organization to build and maintain its own interfaces or to contract with a third-party supplier to do so.</p> <p>Seek risk management and legal counsel review of health IT vendor contracts (e.g., review of contract language for warranty disclaimers, damage limitations, hold-harmless and indemnification provisions, and purchaser obligations).</p>	

## IMPLEMENTATION PHASE

Low Impact	Moderate Impact	High Impact
<p>Provide all health IT system users with training tailored to their needs and specialty.</p> <p>Ensure that training addresses both the benefits and limitations of the health IT system.</p> <p>Educate users on the backup measures to follow when the health IT system is down.</p>	<p>Seek health IT system users’ feedback on the system’s ease of use and problems they encounter throughout the implementation phase.</p> <p>Follow a process to promptly address health IT system problems and concerns that can cause patient harm.</p>	<p>Conduct extensive tests to ensure the health IT system will operate as expected (e.g., the right data flows into the right record) before it is used to provide patient care.</p> <p>Incorporate health IT system user interfaces that are designed to prevent errors (e.g., does not display menu items that are inappropriate for a given context, does not allow alphabetic characters in numeric entry fields).</p>

**IMPLEMENTATION PHASE (continued)**

Low Impact	Moderate Impact	High Impact
<p>Educate users on the process for reporting problems, near misses, and hazardous situations they experience with the health IT system.</p> <p>Prohibit staff members and employees from using the health IT system for patient care until they have demonstrated competence in using the system.</p> <p>Set a realistic, but short-range, goal to phase out paper systems used in routine patient care that are replaced by the health IT system.</p> <p>Provide health IT users with one-on-one support, 24 hours a day, seven days a week during the first few months of the system's implementation.</p> <p>Enlist computer-proficient clinician and staff "super users" who are available to help others with their health IT system questions.</p>	<p>Ensure that those medical devices that are networked to a patient's electronic records are disassociated when the devices are switched from one patient to another.</p> <p>Incorporate health IT system user interfaces that are designed to detect errors (e.g., patient drug allergies, drug-drug interactions), and permit users to address the errors with easy-to-understand instructions.</p> <p>Incorporate health IT system user interfaces that permit easy reversal of actions if an entry mistake is made (e.g., there are intuitive ways for the user to get back on track without losing data).</p> <p>Restrict clinical decision support alerts to those that are essential for safe patient care to minimize distractions for health IT system users.</p> <p>Highlight copy and pasted text from previous record entries so that health IT system users are aware of how the information was obtained and have a heightened suspicion of its accuracy.</p> <p>Create multiple backup systems to ensure the continued operation of the health IT system during power failures and other unplanned power interruptions.</p>	<p>Incorporate forcing functions (e.g., reentering a patient's initials, gender, and age before a record opens) to reduce the likelihood of selecting the wrong patient record.</p>

**CONTINUOUS IMPROVEMENT AND ONGOING MONITORING**

Low Impact	Moderate Impact	High Impact
<p>Allocate staff time and funds to support ongoing maintenance and updates to the health IT system.</p> <p>Maintain an inventory of interfaced devices and systems within the institution, including software versions and configurations of the various interfaced components.</p> <p>Establish metrics (e.g., percentage of system uptime, percentage of alerts overridden by clinicians) to monitor and assess the health IT system's performance and effectiveness.</p> <p>Foster a culture in which caregivers recognize the importance of reporting events and near misses involving health IT systems as part of the organization's overall commitment to safety.</p> <p>Provide ongoing health IT system training for staff, and always provide training when changes are made to the system.</p> <p>Ensure that all new hires and temporary staff are instructed in the operation of health IT systems in their assigned areas before they are permitted to provide patient care.</p> <p>Enlist leaders to conduct walkarounds to ask staff members about their experience using the health IT system and ask for input on needed improvements.</p>	<p>Perform alterations to a health IT system or network (e.g., hardware and software upgrades, security changes, new applications, new work processes, planned maintenance) in a controlled manner to prevent disruptions to the system and patient care.</p> <p>Provide structured formats for reporting health IT-related events to collect the necessary information to evaluate the event and its causes.</p> <p>Apply proactive risk assessment to improve high-risk processes identified through event reporting.</p> <p>Use root-cause analysis to understand the underlying causes of health IT-related events and to identify strategies to prevent the recurrence of similar events or to mitigate harm when events do occur.</p> <p>Identify workarounds adopted by staff to circumvent health IT system design flaws; then, address the design flaws to eliminate the need for workarounds.</p>	

\* Organizations must consider a combination of the high-, medium-, and low-impact safety strategies to prevent any unintended consequences from health IT projects. No one strategy by itself is effective in minimizing health IT-related errors.

### AT A GLANCE

- ▶ Enlist leaders' commitment and support for the organization's health IT project.
- ▶ Expect to devote considerable time and resources to the project.
- ▶ Involve health IT users in the planning, design, and selection of the system.
- ▶ Conduct a review of workflow and processes to determine how they must be modified for the electronic environment.
- ▶ Evaluate the ability of existing software-based systems within the organization to reliably exchange data with any health IT system under consideration.

*Implementing health information technology (IT) in a systematic manner is a major strategic objective involving careful coordination, open communication, and collaboration across the provider community (DeVore and Figlioli).*

An organization must plan extensively for its switch to a new health IT system, whether it is a CPOE system, PACS, or facility-wide EHR system. All participants in the effort must be aware that the organization will incur significant investments of time, effort, and money. One large care network logged approximately 3,000 hours just of staff training over 18 months before setting a “go live” date for a new CPOE system (Dixon and Zafar). Listed below are recommendations and resources to guide the organization through health IT planning. See “EHR Planning and Implementation: ‘Labor of Love’” for a summary of one 142-bed hospital's journey in adopting EHRs.

**Start with leadership commitment.** The time, effort, financing, and support for this massive undertaking is such that a project cannot proceed without the complete, prolonged, and dedicated support of the facility's entire board of directors and leadership. Leaders cannot simply rubber-stamp the project with their approval but must show enthusiasm for the initiative and a

belief that it will have a positive impact on work practices and patient care. Leaders' enthusiasm creates a supportive and positive approach to the project that carries over to the project team leaders, as well as the clinicians and employees who are most affected by the initiative (Day et al.).

**Devote time and resources.** Health IT systems are not a “plug and play” technology. Because the selection, acquisition, and implementation of a health IT system represents a highly complex process, healthcare facilities can expect to devote months to years to the project, depending on the system and its enterprise-wide impact.

**Involve users.** A multidisciplinary committee, comprising individuals from every area that will be affected by the health IT system, should be involved in the planning and decision-making process. Those who will be using the system—for example, nurses, physicians, pharmacists, lab technicians, and others—must provide input in the planning, design, and selection of the system, examine its impact on workflow, and identify necessary changes to workflow processes. In fact, the initiative should be viewed as a clinical project requiring the IT department's input and expertise. It should not be viewed solely as an IT effort.

In addition to clinical users, the committee should include representatives from senior leadership, finance, clinical engineering, IT, risk management/patient safety/quality improvement, and affected clinical departments (e.g., pharmacy, laboratory, radiology, surgery, intensive care). The committee should also include physician and nurse leaders, preferably those with informatics training and experience, who will serve as health IT champions and help to gain the support of medical and nursing staff as the project moves into its implementation phase.

**Identify health IT system objectives.** Defining the organization's goals and objectives for its health IT system will provide the framework for its purchase and implementation decisions. While some of the organization's goals may include nonclinical objectives—for example, obtaining bonus payments from the federal government for EHR adoption—the transition to a health IT system must be understood by clinical staff as a clinical initiative to improve clinical care and to promote patient safety and quality improvement.

**Evaluate infrastructure.** A health IT system can place new demands on a facility's IT infrastructure as well as the building itself. Can the IT network support increased

## EHR Planning and Implementation: “Labor of Love”

“I really feel that this electronic transition is a remarkable labor of love,” says the chief medical information officer (CMIO) of a 142-bed Massachusetts hospital that made the move from paper to electronic records. “Although it takes coordination and effort, the transition has been a time of rebirth for our hospital, combining the best of our old practices with the best of the new,” says the CMIO.

The hospital had invested in a clinical system for order entry of medications, as well as lab and radiology studies, but within 10 years, hospital leaders determined that the system did not meet its strategic goals for EHRs. Although challenging, its journey to an EHR system was not insurmountable.

The hospital attributes its success to the commitment of its leadership and staff.

Senior executives were committed to making management and budget decisions. Various hospital committees reviewed and redesigned their information workflow. Clinical staff learned to use the new technology and terminology while redesigning some core clinical processes. The IT department designed and delivered solutions on time, and clinical IT staff ensured safe implementation of the changes.

Key lessons learned in the hospital’s transition to EHRs are as follows:

- ▷ Begin planning early.
- ▷ Conduct an early review of workflow, order sets, documentation, and policies and procedures to determine how they must be modified for the electronic environment.

- ▷ Anticipate organizational change and committee reorganization.
- ▷ Devote resources to educating nurses and physicians about the EHR system.
- ▷ Network with other hospitals to learn from them.

The hospital’s EHR transition story is described on the HHS’s website promoting health IT. The site was developed by the Office of the National Coordinator for Health IT. Refer to “Online Resources” for information on accessing stories of other organizations’ health IT journeys.

**Source:** Office of the National Coordinator for Health Information Technology. EHR adoption marks a time of rebirth for Massachusetts hospital [online]. 2010 Jun 6 [cited 2012 Oct 1]. <http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=1958&PageID=20168>.

demand from a health IT system? Can the network support the system 24 hours a day, seven days a week? Does the facility have backup systems, such as backup generators and backup data storage, which will enable a facility’s computer networks to continue to operate during a power outage and other disasters? Other infrastructure considerations include department layout and space

requirements, as well as more basic issues, such as the location of electrical outlets. Even these basic matters can have a huge impact on the project’s success: ensuring that electrical outlets are easily reachable, for example, eliminates the need for a nurse to bend to plug an electrical cord for a portable workstation into an outlet. In deciding where health IT workstations are

placed, remember to choose an environment away from distractions that could interfere with data entry by health IT users (Joint Commission). Advance planning may have avoided one facility’s last-minute health IT installation change. The facility planned to use wall-mounted desktop computers but, during installation, discovered they were too heavy, so the installation continued with

computers mounted on wheeled carriers (Ramirez et al.).

**Assess health IT readiness.** Organizations may want to gain insights into staff’s current practices with computers and their readiness for a new health IT system. What are the opinions of the organization’s clinicians and staff about the use of computers in health-care? To what extent do clinicians and staff currently use computers in the organization and for which functions? What possible hurdles do clinicians and staff perceive to adopting new systems? The Department of Health and Human Services’ (HHS) Office of the National Coordinator for Health IT has posted several health IT readiness assessment surveys on its website that organizations can tailor to meet their needs and use the findings to guide health IT planning and decision making. Another toolkit for measuring health IT stakeholders’ expectations is available from AHRQ (see “Online Resources” for accessing the readiness assessment surveys and health IT evaluation toolkit online).

**Examine work processes.** Evaluate current clinical and administrative work practices that will be affected by a health IT system to identify any risks, such as process breakdown points, and inefficiencies (Joint Commission). Proactive risk assessment tools, such as failure mode and effects analysis (FMEA), can help to identify these process breakdown points so the organization can explore solutions in a wired environment. Say, for example, that the lab’s standard practice is to alert the ordering physician by phone of any abnormal critical test results but that the process can fail when the lab is unaware that the physician has signed out and transferred the patient’s care to another physician. If a new EHR system is under consideration, it can be used to help prevent critical communication breakdowns by requiring an electronic

receipt acknowledgment of the test results and an electronic alert to the lab if there is no acknowledgment of the results within a specified time frame. Work practices and processes affected by health IT can range from patient admission procedures to lab results reporting to medication reconciliation at discharge. In reviewing its current work practices, the organization should also identify whether these practices have been modified over time from one department to another as staff developed shortcuts, workarounds, and variations to the practices.

**Rethink workflow in a health IT environment.**

Adopting a health IT system provides a catalyst that encourages clinicians to rethink their workflow, to make efficiency improvements, and to take advantage of automation provided by EHR and other health IT systems (CHF). It will be necessary to explain to clinical staff members that the health IT system will not mimic their current workflow exactly and that they may need to change some processes to take advantage of the features of the new system. For example, CPOE systems allow for the creation of order sets that can be activated for certain clinical routines, replacing the need to input a sequence of individual orders. If properly implemented with clinician input to reflect department-specific needs, order sets can help increase clinicians’ compliance with standardized care protocols. However, the organization must also ensure that it does not unintentionally create unsafe practices with the new workflow by, for example, bypassing important pharmacy double checks or by indiscriminately applying alerts and reminders that end up annoying clinicians and cause unnecessary distractions that can lead to errors. With regard to order sets, the Joint Commission recommends that pharmacists review orders that fall outside usual parameters (Joint Commission). Refer to “Online Resources” for information

on accessing online tools from AHRQ for assessing and mapping workflow in a health IT environment.

**Conduct field trips.** Visit other hospitals and healthcare organizations that are health IT adopters to learn about the capabilities of their systems, to ask how they prepared for their health IT system, and to probe about lessons learned along the way (Joint Commission). In particular, organizations should consider visits to facilities using the same systems they are considering for purchase.

**Evaluate vendors for the right hardware and software solutions.**

Having the right health IT hardware and software is a key aspect in the socio-technical model of health IT and underscores the importance of involving the end user in both the design and selection of the product. According to the IOM report, essential attributes for health IT systems are as follows (IOM):

- ▶ Easy retrieval of accurate, timely, and reliable data
- ▶ System features that appeal to the user
- ▶ Simple and intuitive data displays
- ▶ Easy navigation
- ▶ Evidence at the point of care to aid clinical decision making
- ▶ Enhancements to workflow, automation of mundane tasks, and streamlining of work without adding to physical or cognitive workload of the user
- ▶ Easy transfer of information to and from other organizations and providers
- ▶ No unanticipated downtime

Additionally, health IT system purchasers must consider vendors’ responsiveness to concerns raised by customers about their products. Do the vendors address customers’ concerns to make improvements to their products?



## Human-Computer Interface: Design Features to Promote Safe Use

- ▷ User interface is intuitive and simplifies tasks with, for example, drop-down menus, dialogue boxes, forms, and icons.
- ▷ User interface is consistent in its presentation and appearance.
  - Information on the screen is organized and clear.
  - Critical information is available *and* observable.
  - Text is easily readable at a normal viewing distance and is in a consistent size and font (e.g., Times New Roman, or Arial).
  - Contrast between text font and background colors is adequate.
  - Ratio of text and graphics to total viewing area is adequate (i.e., display is not cluttered).
  - Uppercase text format is used for single words, such as “ON” and “OFF,” and avoided for multiword text.
- Cues, such as text color, are used consistently to indicate important information and warnings based on typical conventions and user expectations.
- ▷ User interface caters to all types of users, with explanatory text available for novices and navigation shortcuts for experts.
- ▷ User interface follows a “three-click rule” of getting to any level of data manipulation within three clicks of a mouse, stylus, or similar device.
- ▷ User interface offers informative feedback, such as instructing the user about the nature of an error if one has been made or indicating to the user that the system is ready to use and accept data or provide data.
- ▷ User interface is designed to prevent errors (e.g., does not display menu items that are inappropriate for a given context, does not allow alphabetic characters in numeric entry fields).
- ▷ User interface is designed to detect errors and permit users to address errors with easy-to-understand instructions.
- ▷ User interface provides ample reminders when it requires that the user remain vigilant (e.g., infrequent or major actions call for a response from the user).
- ▷ User interface permits easy reversal of actions; if a mistake occurs in data access, retrieval, storage, or deletion, there are intuitive ways for the user to get back on track and reverse actions without losing data.
- ▷ User interface reduces short-term memory load (e.g., user is not required to remember information from one screen when working in another screen).

In evaluating vendors’ products, organizations must be mindful of the events from this analysis and others as they consider the health IT system’s features. For example, some events revealed that users are often good at detecting when they have made data entry mistakes (e.g., ordering a radiology test for the wrong patient), but that the system does not completely support error correction (e.g., a diagnostic imaging order is cancelled but the radiology department cannot detect that the error is withdrawn). Therefore organizations should evaluate how a system is designed to address errors, such as data entry mistakes. How easily can the user reverse actions if a mistake is made? Can the user get back on track without losing data?

Other questions suggested from the Deep Dive findings include: Are there some designs that can increase the risk of opening the wrong patient record, as often seen in these events, or are there features that help to minimize these risks? Are there inflexible order sequences that could cause the physician to forget an intended order while navigating through mandatory screens? How easy is it for the clinician to retrieve important laboratory and radiographic data? Refer to “Human-Computer Interface: Design Features to Promote Safe Use ” for a list of desirable features for the user interface with the computer based on human factors design.

### Poor Design Threatens Safety

Poor usability of health IT systems, according to the IOM report, is “one of the greatest threats to patient safety.” In contrast, systems that effectively address usability can promote patient safety.

While a list of all the questions to ask when considering different vendors is beyond the scope of this report, organizations may want to refer to guidelines from the National Institute for Standards and Technology on EHR usability and evaluation. The institute’s report, *Technical Evaluation, Testing, and Validation of the Usability of Electronic Health Records*, lists questions that can be used to evaluate EHR systems under consideration (see “Online Resources”). Although intended for vendors

developing health IT systems, the questions can also guide purchasers during their evaluation of various products. Of course, organizations should also ask vendors about any testing that was conducted for product development: How did they involve the intended users of their products in the system design? What type of testing was performed before the product's release to eliminate any software problems and bugs?

**Evaluate system interoperability.** In making their health IT system selection and implementation plans, organizations must also consider the extent of data exchange they expect to promote within their facilities for the sharing of information across different health IT systems, as well as the retrieval of data from medical devices. As many of the events reported to ECRI Institute PSO illustrate, inadequate interfaces between health IT systems presented considerable risk for patient safety because important data, such as critical test results, could not be shared electronically or through properly built interfaces, causing near misses and actual errors.

The number of health IT applications and integrations will likely increase dramatically, given that criteria for demonstrating meaningful use of EHRs include sharing of data with other systems such as CPOE systems, eMAR systems, PACS, laboratory information systems, and electronic

prescribing. An organization that intends to build customized interfaces must consider the interoperability of the systems it purchases. Interoperability refers to the ability of two or more diverse systems or components to exchange information and to use that information (ANSI/AAMI/IEC).

### Challenges to Achieving Interoperability

Despite the goal of using health IT to facilitate electronic access to clinical information and to enhance patient care, there are challenges to achieving interoperability. As one health IT researcher laments, “the promise of interoperability is thwarted by a digital tower of Babel that keeps information siloed and mutually incomprehensible” (Koppel). Even variations in how systems present information—for example, the same icon can represent different actions in each health IT system—and in how they require sign-ons and sign-offs will frustrate end users if they must use these diverse systems to manage patients' care.

ECRI Institute identified system incompatibilities between medical technology and health IT as one of its top 10 high-risk health technology hazards for 2011 (ECRI Institute “Top 10 . . . 2011”) and again for 2013 (ECRI Institute “Top 10 . . . 2013”). Refer to “ECRI Institute Resources” for a bibliography of resources available from

ECRI Institute to guide organizations in supporting interoperability.

Vendors must demonstrate that their products can support interoperability through adherence to standard formats that enable data sharing among health IT products. Several initiatives are in place—such as the Digital Imaging and Communications in Medicine (DICOM) standard and the Integrating the Healthcare Enterprise (IHE) efforts—to make interoperability within healthcare more smooth and seamless. IHE is a voluntary initiative by healthcare professionals and suppliers that seeks to promote the exchange of healthcare information and ensure compatibility by developing standardized message structures and formats, one of which is the DICOM standard for communicating radiographic data.

In negotiating contracts with vendors, organizations should seek commitments from vendors to work with the organization's IT department to build system interfaces or, at a minimum, provide, at no charge, the documentation that will help a facility build and maintain its own interfaces or contract with a third-party supplier to do so. Additionally, the vendor should indicate its intent to design products that adhere to relevant standards.

Incompatibilities between medical technology and health IT systems can also lead to patient-data association errors, or

the association of one patient's data with another patient's record, which ECRI Institute identified as one of the top 10 health technology hazards for 2013 (ECRI Institute "Top 10 . . . 2013"). In addition to the wrong-input and wrong-record events identified in the Deep Dive, safety notices in ECRI Institute's *Health Devices Alerts* demonstrate the kinds of problems that have been observed:

- ▶ A radiation oncology treatment planning system may use images from the wrong patient, posing a risk of treatment to the incorrect area.
- ▶ Software that aggregates data from different systems may incorrectly match patient data, potentially resulting in the incorrect patient data being displayed.
- ▶ A software flaw in data servers would allow images from one patient to be put into another patient's study.
- ▶ Annotation data from one patient may be displayed with the results for a different patient on a radiation therapy workstation.

Before and during implementation of health IT systems, organizations must ensure successful data transfer between a medical device and an IT system by verifying that (1) the data from the device is associated with the correct patient's record in the IT system and (2) the device and

patient record are correctly disassociated when the device is switched from one patient to another.

### Prepare for Electronic Data Sharing

Healthcare organizations must also prepare for the exchange of electronic information with other providers in the community, such as physician offices and long-term care facilities. But according to a survey of senior healthcare leaders conducted by ECRI Institute and the health IT consulting firm s2a Consulting, only 54% of the respondents indicated that their organization has formally assessed their health information exchange and interoperability needs across their communities (ECRI Institute "Crossing"). Refer to "ECRI Institute Resources" for information on downloading a white paper, "Crossing the Connectivity Chasm: Pinpointing Gaps in Readiness to Exchange Health Information," summarizing the survey results.

**Review vendor contracts.** In addition to seeking assurance in their contracts with health IT vendors that the companies will support interoperability, organizations must review the contracts for potential risks of liability. One concern is whether contractual agreements with health IT vendors will limit vendor liability and create new legal duties for clinicians and healthcare organizations regarding patient care. Health IT vendors

typically use contract language to limit their liability exposure for patient harm that may be related to the use of their systems. Vendor contracts may include warranty disclaimers, damage limitations, hold-harmless and indemnification provisions, purchaser obligations requiring data confirmation (e.g., verification of the accuracy of critical test results), duties to identify and report program errors, and statements that the software is not intended to substitute for the skill, knowledge, and experience of a licensed physician. Allocation of liability is an important consideration during negotiations with vendors; consequently, organizations should ensure that contracts with IT vendors are reviewed by legal counsel knowledgeable about health IT systems.

Other equally important contract considerations include hardware, software, and future upgrade costs; provider ownership of all data generated by the health IT system; installation and maintenance; initial one-on-one user support and ongoing support; training for front-end users and technical support staff; and provisions to inform health IT system users of measures to ensure continued operation of the system if the vendor is acquired, goes out of business, or files for bankruptcy. Remember: everything is negotiable before the contract is signed. (ACS)

## AT A GLANCE

- ▶ Conduct extensive tests to ensure that the health IT system is properly and fully implemented and operates as expected.
- ▶ Provide user training in the health IT system, and ensure users demonstrate their competence in using the system.
- ▶ Educate health IT system users about the capabilities and limitations of the system.
- ▶ Provide health IT system users with ongoing support, particularly in the early stages of implementation.
- ▶ Closely monitor the system's ease of use and problems encountered by users, and promptly address issues that arise.

*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 most likely to appear (IOM).*

The implementation of the health IT system throughout a department or facility must be as carefully planned as the rest of the process. During this stage, safety issues can arise as the organization tests the system, helps users get accustomed to new processes, and identifies and addresses unanticipated quirks in the system. Keys to success are extensive testing, user training, access to ongoing support, and close monitoring for unintended consequences, with a commitment to addressing them promptly.

**Test, test, and retest.** A multiphase testing process is necessary to ensure that the health IT system is properly and fully implemented and to verify that the system behaves as expected. For example, does the right data flow into the right record for the various clinical workflows? The goal is to uncover any problems with the system during the testing phase so these issues are addressed before staff and clinicians use the system to provide patient care. Extensive testing should examine parameters such as order sets, clinical decision support, clinical workflow, ease of use for users, and potential correctable oversights. As a first step, practicing with artificial cases can allow for

fairly accurate testing of workflow processes; however, test scenarios should be designed in such a way as to avoid merging test data with real patient information. As a next step, some organizations may choose to pilot the system in one area of the facility to refine the system before full implementation. Including frontline staff in testing is critical, so organizations will need to add staff members who can cover for those frontline staff members assigned to participate in testing.

### Phase Out Paper

While testing the system, consideration must also be given to the user's environment. Are the workstations installed in areas away from distractions? Is there sufficient room for the workstation?

During pilot testing, organizations that are moving away from paper-based systems may want to use the health IT system simultaneously with the paper-based one. Although dual documentation can slow the process slightly, research has shown that this strategy strengthens user trust in the electronic system (Moniz). Once the facility is ready for full implementation, it should plan to gradually replace the paper-based system rather than to eliminate it at once. It should be aware, however, that the hybrid environment, in which care is documented in both paper charts and an electronic

record, can introduce errors, as some of the reports submitted to ECRI Institute PSO indicated. If an organization chooses a hybrid approach for the health IT system implementation, it should set a realistic, but short-range, goal for phasing out paper systems once it has confidence that the health IT system is performing as expected.

**Apply lessons learned by others.** Although these issues will also be addressed during the project's planning, testing should address the significant patient safety issues identified from the events submitted for this analysis and in other published reports. What happens when orders and other data are entered and sent? Is the information delivered electronically as intended or does it end up in a black hole? Are there other mechanisms for resending test results or for sending them to another designee if there is no computer-generated response from the intended user? Do the drop-down menus meet users' needs? Does too much information in the drop-down lists make it difficult for users to find what they want? Is the arrangement of medication names listed in drop-down lists intuitive to users? Are users satisfied that alert notifications are applied judiciously? Is the system designed to minimize the risk of selecting the wrong patient record?

*(continued on page 32)*

## Strategies to Reduce Entry Errors in Wrong Patient Records

One of the most common problems involving health IT systems identified in ECRI Institute PSO's Deep Dive analysis is selecting the wrong patient record to enter orders and data. The reasons for these errors are numerous and include the following: the font size for displaying patient names is too small; there is no mechanism to alert providers when there are patients with the same name; there are no forcing functions for providers to verify a patient's identity; and multiple interruptions distract a provider who happens to be toggling between two patient records.

Two innovative healthcare organizations have recently shared their strategies to minimize the risk of these errors using electronic verification and patient photos.

In a study published in the *Journal of the American Medical Informatics Association*, researchers at a New York City hospital found that wrong-patient electronic orders occurred with 58 per 100,000 electronic orders in a CPOE system, a rate consistent with other studies. To identify wrong-patient orders, the researchers developed a retract-and-reorder tool that electronically identified orders retracted within 10 minutes and reordered by the same provider within 10 minutes of the retraction.

Testing an intervention to reduce wrong-patient orders, the researchers added an alert to require the prescribing provider to verify, with a single click, the patient's name, gender, and age to ensure the order

was for the correct patient. The intervention resulted in a 16% reduction in wrong-patient order entries. Trying a second intervention, the hospital required the provider to reenter the patient's initials, gender, and age a second time before the order could be sent. The reentry function reduced wrong-patient orders by 41%. The patient identification reentry function was likely more effective than the identification-verify alert because it required providers to pay more attention to the patient data, prompting the providers to catch more errors. The strategy did not completely eliminate events, because some providers may still reenter a patient's initials, gender, and age without verifying the patient's identity. Human factors and usability experts will be needed to further develop solutions to prevent wrong-patient electronic orders. (Adelman et al.)

In a study published in *Pediatrics*, researchers at a children's hospital reviewed errors occurring with CPOE systems and were surprised to see how many involved placing orders in the wrong patient's chart. Seeking to reduce the frequency of these errors, the study team made two changes to the CPOE system: the first was to incorporate a verification screen in the ordering process for the provider to confirm that the patient's name is correct; the second was to add a picture of the patient on the verification screen. The changes resulted in a 75% decrease in wrong-patient order errors. Although the researchers encourage others

to incorporate patient photos in electronic records, they recommend that organizations address any potential Health Insurance Portability and Accountability Act privacy concerns and the need to update the picture with changes in the patient's appearance. (Hyman et al.)

Other strategies to address many of the human-factors considerations with health IT systems that can lead to entry errors for the wrong patient include the following:

- ▷ Use alternate line colors for lists of patient names to help with visual separation of the names between rows.
- ▷ Choose methods to list patient names other than by alphabetical order, which can result in similar patient names next to each other, making it easier to choose the wrong patient name.
- ▷ Ensure that the patient name appears on all order entry screens.

### References

- Adelman JS, Kalkut GE, Schechter CB, et al. Understanding and preventing wrong-patient electronic orders: a randomized controlled trial. *J Am Med Inform Assoc* 2012 Jun 29 [pub ahead of print].
- Hyman D, Laire M, Redmond D, et al. The use of patient pictures and verification screens to reduce computerized provider order entry errors. *Pediatrics* 2012 Jul;130(1):e211-9.

## “Sloppy and Paste” Function Repeats Errors in Electronic Records

Clinicians’ habit of copying and pasting notes from an electronic medical record can turn into a case of whisper-down-the-lane, with the meaning changing drastically from the original version, as presented in an online case study summarized in the July 2012 issue of AHRQ’s WebM&M.

For nearly a decade, a patient’s electronic medical record indicated a history of “PE,” which the patient’s clinicians interpreted as pulmonary embolism, despite the patient’s protests that he never had a pulmonary embolism. An ED physician treating the patient went through the patient’s electronic records and discovered the letters “PE” to reflect a “physical examination” in an entry from a decade earlier. The PE designation apparently had been copied and pasted in

the electronic record “time and time again,” the case note says. The patient’s clinicians mistakenly assumed the letters indicated that the patient had a history of developing blood clots. The ED physician updated the record to state, “This patient never had a pulmonary embolism.”

Copy-and-paste errors occur in about 10% of electronic patient records, according to the report. To remedy what the case study refers to as “sloppy and paste” errors, the author recommends the following measures:

- ▷ Highlight copy-and-pasted text with color or italics so that other providers are aware of how the information was obtained and have a heightened suspicion of its accuracy.

- ▷ Audit documentation practices, including copy-and-paste use, and educate providers of instances of copy-and-paste misuse.

- ▷ Educate providers to question the need to import “large chunks of data into their notes.” In the digital world, “database trumps narrative.”

The American Health Information Management Association has developed recommendations to audit the copy-and-paste function in electronic records, as well as a sample audit policy. The materials are available online (see “Online Resources”).

**Source:** Hirschtick R. Sloppy and paste [online]. WebM&M 2012 Jul [cited 2012 Aug 31]. <http://webmm.ahrq.gov/case.aspx?caseID=274>.

*(continued from page 30)*

(See “Strategies to Reduce Entry Errors in Wrong Patient Records” for suggestions for reducing the risk of pulling the wrong patient record.)

While the reports submitted to ECRI Institute PSO did not indicate problems with copy-and-paste functions, other reports have found that providers may try to save time by cutting and pasting a patient’s past medical history into the current record. In some cases, inaccurate patient information is inadvertently recorded and copied along with everything else, creating opportunities for errors and patient harm. See “‘Sloppy and Paste’ Function Repeats Errors in Electronic Records” for an example of one such event and suggested strategies to prevent them.

**Provide comprehensive user training.** Users should not be allowed to use the health IT system unless they have completed training and demonstrated competence in using

the system. User training also provides an opportunity to inform users about the technology’s limitations, as well as its capabilities, and to emphasize that automation is not a substitute for user vigilance. Just as in the paper world, the risk remains of entering data in the wrong record or entering incorrect data. Users must continue to double-check their data and reconfirm that they have pulled the correct record. Users should also be made aware of the new types of errors (for example, the so-called “midnight problem” of near-midnight entries) that can be introduced in an electronic world and that differ from those in the paper world (McBride et al.). Additionally, trainers should address one of the common frustrations with health IT adoption: it will take time to learn to use the system, but the end goal is improved patient care. Staff must remain vigilant about their care duties while learning to use the system. ECRI Institute is aware of events occurring with the introduction of a new health IT system when staff members

encounter problems with the new system and are distracted from patient care duties, such as patient monitoring and medication administration.

### One-on-One Support after Implementation

When training staff members, one possible successful method is to train groups of staff by specialty. This avoids training that is too general and allows healthcare providers to ask questions and to create and learn about processes that are unique to their specialty (Birk). Training should comprise several steps: general information sessions, group training, one-on-one usage time, and individualized follow-up (Birk; Ramirez et al.). Once training is completed, ensure that the time between orientation and system implementation is short so that the information remains fresh (Joint Commission).

After the system is live, the facility will need to provide one-on-one support,

24 hours a day, seven days a week, during the first few months to increase users' effectiveness with the system and comfort level. Many organizations' IT departments have help desk staff who respond to computer questions and problems; a similar type of help desk (or "emergency issues desk," as suggested by the Joint Commission) might be established to provide immediate assistance to health IT system users—particularly in the early stages of implementation.

Some organizations also identify computer-proficient clinicians and staff in each unit and enlist their help as "super users" who can be available to help others, particularly during the first critical days of implementation. Additionally, the facility should require new training whenever the system undergoes a significant change and should periodically monitor health IT system users to ensure they follow safe practices. All new employees and temporary hires must receive training on any health IT applications they are expected to use before they provide patient care.

Documentation of training provided to staff should be maintained in each employee's personnel file.

**Interview users and conduct walkarounds to gain insights.** Throughout the health IT system implementation phase, the system's clinical champions should talk to users and seek their feedback on the system's ease of use and problems they encountered, as well as gauge the impact of the health IT system on users' workloads (Sittig and Singh "Defining"). One way to prompt users to identify specific concerns is for the interviewer to ask each user, "If you could change one aspect of the health IT system, what would it be?" Any concerns that are raised should be promptly addressed and rapidly resolved, since the problems identified may have the potential to lead to patient harm.

The New York City Department of Health and Mental Hygiene has developed a four-page survey, available online, to obtain

EHR users' feedback after the system's implementation (see "Online Resources" for information on accessing this survey, as well as another survey available from AHRQ). Many of the survey questions could also be used to guide one-on-one interviews with users. Sample questions from the survey include the following:

- ▶ Is the organization of the menus or information lists logical?
- ▶ Can you find the information you need?
- ▶ Is the information presented in a useful format?
- ▶ Is there any extra information on the screen that you don't need?
- ▶ How easy is it to move from one task to another?
- ▶ Does the system ever behave in a way that you don't understand?
- ▶ Can you count on the system being up and available when you need it?
- ▶ Are you satisfied with the system?

**Ask users to report problems.** During the health IT system implementation phase, organizations must continuously monitor for problems, ask users to promptly report issues they encounter, and ensure project experts are available to rapidly resolve them. 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. To systematically track and address these bugs, organizations should provide users a means to report issues that arise and should educate users about how to use the reporting system.

The organization's patient safety adverse event reporting system provides a readily available tracking process and simultaneously ensures that patient safety, risk, and quality staff are kept informed of incidents, as well as near misses, that affect patients. If the organization's event reporting system is used to track implementation bugs

and events, the risk management department should have a process to promptly forward reports raising technical issues to the IT department for resolution. For more information on event reporting, refer to the section Continuous Improvement and Ongoing Monitoring.

To track all health IT-related issues and the organization's response, organizations should maintain a log describing the problem, how it will be resolved, and who is responsible for the response plan. HHS's Office of the National Coordinator for Health IT has developed a sample issue log to track the following:

- ▶ Description of the problem (When did the problem occur? Where? What was the user doing?)
- ▶ Stage in health IT implementation when problem occurred (Did the problem occur during testing, during an upgrade, or during another stage? Who identified the problem?)
- ▶ Suspected cause of the problem and its impact on the patient and patient care
- ▶ Corrective actions and status of those actions

The sample issue log is available online (see "Online Resources") and can be modified to meet the needs of the organization.

**Plan for backup systems.** As some of the events reported to ECRI Institute PSO indicate, computers and computer networks can go down unexpectedly. Organizations must have multiple backup systems in place for these events, including backup power sources during power failures and procedures for using paper-based backup measures if, for example, the only way to submit a medication order is the old way: using paper. Health IT user training should include instructions on these backup procedures.

## Continuous Improvement and Ongoing Monitoring

### AT A GLANCE

- ▶ Allocate staff time and funds to support ongoing maintenance and updates to the health IT system.
- ▶ Introduce alterations to a network or a health IT system in a controlled manner to prevent unintended consequences.
- ▶ Monitor the system's effectiveness with metrics established by the organization and use the data to address needed improvements.
- ▶ Require health IT system users to report health IT-related events and near misses via the facility's event reporting program.
- ▶ Conduct thorough event analysis and investigation to identify corrective measures to prevent similar events or to mitigate harm when errors do occur.
- ▶ Consider workarounds a symptom of suboptimal health IT system design; examine why staff adopt workarounds, and address their concerns.

*Organizations must continually evaluate the usability and performance of their systems after implementation, reliably measure benefits, and assess potential iatrogenic effects (Sittig and Singh "Eight Rights").*

Once their health IT systems are in place, organizations must take steps to ensure their continued reliable performance by monitoring the system's function, collecting user reports of system glitches and difficulties, and adopting measures to remediate problems. To do so, organizations must continue to allocate staff time and funds to their health IT systems for ongoing maintenance and updates. Additionally, ensuring that the network is secure from software viruses, malware, and other cyber-attacks is an ongoing process. Listed below are recommendations to guide the organization in maximizing the benefits of health IT systems to improve care delivery.

#### **Pay attention to change management.**

Change management is a structured approach for ensuring that alterations to a network or system are performed in a controlled manner. Because computerized medical devices and health IT systems are so interconnected, healthcare facilities must be aware of possible downstream effects when changes to one component of the system affect the operation of another. In 2012, ECRI Institute identified inattention to change management for health

IT systems—and in particular, medical technology and IT—as one of its top 10 high-risk health technology hazards (ECRI Institute "Top 10 . . . 2012"). For its 2013 list, ECRI Institute reiterated that this problem contributes to interoperability failures with medical devices and health IT systems (ECRI Institute "Top 10 . . . 2013"). Refer to "ECRI Institute Resources" for information on accessing the reports online and additional guidance on change management.

### Manage Change to Prevent Unintended Effects

ECRI Institute is aware of an increasing number of problems relating to change management, including issues involving wireless networks, cybersecurity, planned maintenance, or software upgrades. Many of the events reported to ECRI Institute PSO for this analysis were associated with data transfer problems, such as physician medication orders that are not received by the pharmacy department, and may be the result of insufficiently testing upgrades and system connections. Without sufficient planning and testing, what is thought to strengthen the health IT system's operation in one area may end up weakening it in others.

Even new policies and procedures can negatively affect health IT systems and workflow and must be evaluated for any

possible ramifications before they are fully adopted.

Effective approaches to change management include the following:

- ▶ Maintain an inventory of interfaced devices and systems within the institution, including the software versions and configurations of the various interfaced components.
- ▶ Take steps to ensure that changes are assessed, approved, tested, and implemented in a controlled manner. Change management applies to a variety of actions, including hardware upgrades, software upgrades, security changes, new applications, new work processes, and planned maintenance.
- ▶ Evaluate the facility's policies and procedures regarding change management. Care should be taken to determine how technology decisions involving health IT systems, medical devices, and IT networks can affect current operations, patient care, and clinician work processes.
- ▶ Develop contract wording that is specific to change management. For example, contracts with vendors (e.g., information system vendors, device suppliers) should require the necessary documents (e.g., revised specifications, software upgrade documentation, test scenarios) to be



provided to the appropriately designated staff member(s) to facilitate change management. Stipulating that vendors provide advance notice of impending changes can give healthcare facilities time to budget and adequately plan for changes.

- ▶ Ensure that any system updates do not jeopardize processes to maintain the privacy of patients' protected health information and the security of records with that information.
- ▶ Ensure good working relationships among departments that have a direct responsibility for health IT systems and change management; involve the appropriate stakeholders (e.g., IT, clinical engineering, nursing staff) when changes are planned.
- ▶ When making changes to interfaced systems, closely monitor the system after the change is made to ensure its safe and effective performance.
- ▶ Provide frontline staff members a point of contact for reporting problems relating to change management and health IT systems. Education, training, and good escalation procedures can help to ensure that problems are addressed with the appropriate urgency.

**Monitor and assess health IT system effectiveness.** The organization should identify

an interdisciplinary group of health IT system stakeholders to identify metrics to monitor the system's effectiveness, to review the data, to verify that the system is working as planned, to brainstorm about the findings and possible improvements to the health IT system, and to report the findings and planned improvements through the organization's quality and patient safety processes.

The following suggested metrics were developed to track CPOE system function, but they can also be used as monitoring metrics for other health IT systems, such as EHRs (Sittig et al.):

- ▶ Percentage of system uptime (calculated as the number of minutes the system was functional in a given month divided by the total number of minutes that the system was supposed to be functional for that month)
- ▶ Mean response time (calculated for any routine tasks, such as accessing a patient's medication list)
- ▶ Percentage of all orders entered electronically by physicians and other clinical decision makers
- ▶ Percentage of order sets and templates used over a 12-month period (to determine if they are used as expected)

- ▶ Percentage of alerts triggered (can be calculated over a one-week, one-month, or one-quarter time frame)
- ▶ Percentage of alerts overridden by clinicians
- ▶ Percentage of progress notes copied from an earlier record
- ▶ System interface efficiency (calculated as the number of successful transmissions between an EHR system and other ancillary systems—such as PACS and pharmacy and laboratory IT systems—divided by the total number of transmissions attempted)
- ▶ Percentage of all orders submitted as free-text entries

Periodically, organizations should assess their health IT system practices—in areas ranging from order entry to test results reporting to back up measures for patient data—to identify system strengths and weaknesses and areas for improvement. Assessment tools will soon be available through work funded by HHS's Office of the National Coordinator for Health Information Technology. The research team is developing a series of about 15 checklists and best-practice tools to evaluate health IT practices in inpatient and ambulatory settings. Among the topics covered are order entry, system customization and upgrades,

## Workarounds: Examine Why Staff Choose Them, Then Tackle Solutions

Workarounds are a symptom of suboptimal design of health IT systems (IOM). When frontline workers develop workarounds, organizational leaders can be misled into thinking that flawed systems are working well. Eventually, the workarounds can lead to adverse events, as in one case summarized in the March 2011 edition of AHRQ's *WebM&M* of a patient whose follow-up visit was missed because of a poorly implemented workaround.

The patient presented to the ED with a fractured humerus and was told to follow up with an orthopedist. The patient failed to keep a follow-up appointment because of transportation issues; a secretary at the hospital cancelled the appointment from the system, as per protocol, so it could be

rescheduled. Because the facility designed the appointment and referral system to require that follow-up appointments occur within 30 days of referral, staff regularly canceled appointments missed by patients before rescheduling to minimize the presence of black marks on the 30-day reports. In this situation, the system failed to notify the patient's primary care provider, and the follow-up appointment was never rescheduled.

Although the patient did not experience harm from the error, the commentary's author stresses that health IT systems should be designed to support the performance needs of the system and its users and that organizations should work with vendors before purchase to ensure that

products can meet these needs. A seemingly well-intentioned goal of seeing patients within 30 days of a referral led to a workaround: cancelling appointments for missed visits. Had the organization examined the rationale for the measure, it may have realized that patient-driven cancellations, which happen frequently, would make the measure artificial. Additionally, in a "learning organization," staff would not have feared reprimand for a low 30-day follow-up rate and would have worked with the organization to identify areas for improvement.

**Source:** Karsh BT. Dropping the ball despite an integrated EMR [online]. *WebM&M* 2011 Mar [cited 2012 Sep 4]. <http://webmm.ahrq.gov/case.aspx?caseID=237>.

patient identification processes, clinical decision support, and laboratory results review (Weinstock). Results from the project, called SAFER: Safety Assurance Factors for EHR Resilience, will be available in 2013.

Additionally, organizations should occasionally interview staff about their experience using health IT systems. Leadership patient safety rounds offer an ideal opportunity to conduct such interviews. The user feedback surveys referenced in the section on implementation can also be used for this purpose.

### Promote event and near-miss reporting.

Once the health IT system is fully implemented, staff must remain alert for any unintended consequences that arise. Healthcare staff should report health IT system-related events and near misses to the facility's event reporting program. Additionally, staff should report unsafe conditions that may lead to adverse events.

A mechanism must be in place to identify and respond to critical problems within a specific time frame so that the system does not continue to adversely affect patient care. Further analysis of the causes of these and other events can be addressed through root-cause analysis. The information learned from the analysis can be used to identify strategies to prevent similar events.

Essential approaches for an effective event reporting program include the following:

- ▶ Make it easy for staff to submit reports by ensuring easy access to the event reporting system.
- ▶ Foster a culture in which caregivers recognize the importance of reporting events and near misses involving health IT systems as part of the organization's overall commitment to safety. The organization's safety culture must support an atmosphere in which healthcare

workers can report actual or potential errors, events, and hazards without fear of reprisal (unless the events reflect willful disregard, wrongful intent, or noncompliance with procedures).

- ▶ Specify the information that should be submitted for health IT-related events and consider providing event reporting forms that are specifically designed for health IT events.
- ▶ Use common language, such as that provided by AHRQ's Common Formats, to enable more efficient sharing of data about events involving health IT systems.
- ▶ Participate in initiatives, such as this PSO Deep Dive analysis, to support learning about events associated with health IT.
- ▶ Use the information learned from event reports to improve health IT systems. The power to improve safety of health IT systems rests in the ability to act on

## Establish Alert Priorities to Minimize Alert Fatigue

Alerts, notifications, and hard stops in health IT systems must be carefully designed to alert the system user to a significant potential error, but they must not be so common that the user ignores them. In such cases, the risk of error is greatly increased.

When planning and implementing a CPOE system, for example, the facility should carefully determine the various alerts that will be programmed into the system. Alerts can be programmed to appear for any reason, but the creation of too many alerts will likely contribute to alert fatigue and allow medication errors, order duplications, or other patient safety risks to be missed. Before implementing the CPOE system, the input of pharmacy staff, clinicians, specialists, and others should be solicited to determine the appropriate levels for programmed alerts.

Different levels of severity for alerts can be set up in the system. For instance, in some systems, a low-level alert can be

overridden with a simple mouse click, but a high-level alert can be overridden only after the clinician enters a reason. This reason, as well as the identity of the author and the time and date, is recorded in the system along with the order itself. Such tiered alerts can range from a simple notification to a hard stop, depending on what entry prompted the alert. One facility redesigned its CPOE alerts structure so that only the most serious drug-drug interaction risks would require a response from the managing physician. Less serious alerts were noninterruptive, informational notifications. (Paterno et al.)

A common concern among patient safety experts is that any alert short of a hard stop requiring authorization will simply be overridden without being acknowledged, which may cause the patient harm. Alerts for such factors as drug-drug interactions or missing information fields (e.g., patient weight) should not be ignored but should

be carefully calibrated to ensure the highest likelihood of response by the healthcare provider. (Paterno et al.)

Also, a review of skipped or rejected alerts may provide important insights about their necessity. Many alerts are overridden because they conflict with commonplace clinical practices; more effort is needed to reduce alerts that contradict these accepted practices. (Russ et al.)

### References

- Paterno MD, Maviglia SM, Gorman PN, et al. Tiering drug-drug interaction alerts by severity increases compliance rates. *J Am Med Inform Assoc* 2009 Jan-Feb;16(1):40-6.
- Russ AL, Zillich AJ, McManus MS, et al. Prescribers' interactions with medication alerts at the point of prescribing: a multi-method, *in situ* investigation of the human-computer interaction. *Int J Med Inform* 2012 Apr;81(4):232-43.

and learn from events, says IOM's report on health IT.

The AHRQ Common Format for reporting health IT events and unsafe conditions, which was used by ECRI Institute PSO to collect events for this analysis, can also be used by healthcare facilities to structure event reports for health IT-related issues so that the organization collects the necessary information about the event. In its review of the 171 event reports for this analysis, ECRI Institute PSO often found that information was incomplete, so staff members should be educated about essential information to include in the health IT event reports. Forms that prompt reporters to provide specific information will enable the organization to collect more complete event information.

Because some reports may raise only technical issues, the risk management department should also have a process to promptly forward those reports to designated individuals in the IT department for IT staff to address. For more information available from ECRI Institute about event reporting and a safety culture, see "ECRI Institute Resources."

Additionally, ECRI Institute PSO participated in an AHRQ-funded project to develop a web-based software tool to capture information about health IT hazards before they can cause patient harm. Once available, the web-based tool, called the Hazard Manager, will provide a common language for systematically reporting health IT system events across the continuum of care. Organizations might also consider using

the Hazard Manager to determine the type of data to seek in their event reports about health IT systems. The Hazard Manager provides formats for important event report parameters such as the event description, health IT systems involved, discovery of the event, causes of the event (e.g., usability, data quality, decision support), and impact of the event on care processes. Refer to "Online Resources" for information on accessing an online report describing a beta version of the Hazard Manager.

**Conduct thorough event analysis to identify corrective actions.** Events identified by incident and near-miss reporting should be analyzed in a structured, step-by-step inves-

*(continued on page 39)*

## ECRI Institute Resources\*

- ▷ 10 questions about IEC 80001-1: what you need to know about the upcoming standard and networked medical devices [guidance article]. *Health Devices* 2010 May;39(5):146-9.
- ▷ Avoid risk with health information technology [webinar]. 2011 Mar 16. For more information on this webinar, visit [https://www.ecri.org/ConferencesAudioConferences/Pages/Health\\_Information\\_Technology.aspx](https://www.ecri.org/ConferencesAudioConferences/Pages/Health_Information_Technology.aspx).
- ▷ Avoiding the pitfalls of medical device connectivity [webinar]. 2011 Oct 12. For more information on this webinar, visit <https://www.ecri.org/Conferences/AudioConferences/Pages/Medical-Device-Connectivity.aspx>.
- ▷ CE/IT collaboration: putting the pieces together [guidance article]. *Health Devices* 2009 May;38(5):138-47.
- ▷ Coping with convergence: a road map for successfully combining medical and information technologies [guidance article]. *Health Devices* 2008 Oct;37(10):293-304.
- ▷ Crossing the connectivity chasm: pinpointing gaps in readiness to exchange health information [white paper]. 2012. <https://www.ecri.org/hie>.
- ▷ Culture of safety. *Health Risk Control* 2009 Jan;Suppl A:Risk and quality management strategies 21. Available online to ECRI Institute PSO members at <https://members2.ecri.org/Components/HRC/Pages/RiskQual21.aspx>.
- ▷ Electronic health records. *Health Risk Control* 2007 Jul;2:Medical records 1.1. Available online to ECRI Institute PSO members at [https://members2.ecri.org/Components/HRC/Pages/MedRec1\\_1.aspx](https://members2.ecri.org/Components/HRC/Pages/MedRec1_1.aspx).
- ▷ Event reporting. *Health Risk Control* 2009 Jul;2:Incident reporting and management 1. Available online to ECRI Institute PSO members at <https://members2.ecri.org/Components/HRC/Pages/IncRep1.aspx>.
- ▷ Implementing computerized provider order entry. *Health Risk Control* 2011 Jul;Suppl A:Pharmacy and medications 6. Available online to ECRI Institute PSO members at <https://members2.ecri.org/Components/HRC/Pages/Pharm6.aspx>.
- ▷ Look who's talking: a guide to interoperability groups and resources [guidance article]. *Health Devices* 2011 Jun;40(6):190-7.
- ▷ Making connections: integrating medical devices with electronic medical records [guidance article]. *Health Devices* 2012 Apr;41(4):102-21.
- ▷ Patient safety at the intersection of medical and information technology. *PSO Navigator* 2011 Aug;3(3):1-8. Available online to ECRI Institute PSO members at <https://members2.ecri.org/Components/HealthCareGPS/Documents/PSONavigator/PSONav0811.pdf>.
- ▷ Physiologic monitoring: a guide to networking your monitoring systems [guidance article]. *Health Devices* 2011 Oct;40(10):322-45.
- ▷ Technology's role in preventing medication errors. *PSO Navigator* 2010 Nov;2(4):1-9. Available online to ECRI Institute PSO members at <https://members2.ecri.org/Components/HealthCareGPS/Documents/PSONavigator/PSONav1110.pdf>.
- ▷ Top 10 health technology hazards for 2013: key patient safety risks, and how to keep them in check [guidance article]. *Health Devices* 2012 Nov;41(11):1-23. <https://www.ecri.org/2013hazards>.
- ▷ Top 10 technology hazards for 2011: a guide for prioritizing your patient safety initiatives [guidance article]. *Health Devices* 2010 Nov;39(11):386-98. [https://www.ecri.org/Forms/Pages/2011\\_Top\\_10\\_Technology\\_Hazards.aspx](https://www.ecri.org/Forms/Pages/2011_Top_10_Technology_Hazards.aspx).
- ▷ Top 10 technology hazards for 2012: the risks that should be at the top of your prevention list [guidance article]. *Health Devices* 2011 Nov;40(11):1-16. [https://www.ecri.org/2012\\_Top\\_10\\_Hazards](https://www.ecri.org/2012_Top_10_Hazards).
- ▷ Vital signs monitoring systems: a look at seven monitors and their connectivity solutions [evaluation]. *Health Devices* 2011 Sep;40(9):274-311.

\* For information on obtaining ECRI Institute reports, contact ECRI Institute PSO at [psohelpdesk@ecri.org](mailto:psohelpdesk@ecri.org).

*(continued from page 37)*

tigation involving those familiar with the event. Proactive analysis, such as FMEA, or reactive analysis, such as root-cause analysis, should be used to understand where failures occurred for incidents that reached the patient, as well as why the event happened and its underlying causes. The analysis should be conducted by a multidisciplinary team of health IT system stakeholders who can help to identify safeguards and barriers that can be implemented to prevent recurrence of a similar event or to mitigate any harm if the error does occur.

Interviews of staff who witnessed an event are one of the primary means to gather information for an event investigation. Ask each individual involved to tell their story with questions such as:

- ▶ What were you seeing?
- ▶ What were you focusing on?
- ▶ What were you expecting to happen?
- ▶ If you had to describe the situation to a colleague at the point the incident occurred, what would you have told them?

Several tools are available from HHS's Office of the National Coordinator for Health Information Technology to assist with root-cause analyses for health IT systems. They include a set of questions to use

during root-cause analyses of EHR system events to help identify the underlying causes of the events and a template for listing and tracking corrective actions identified from root-cause analyses. Refer to "Online Resources" for more information on downloading the tools.

Following the event investigation, staff should be provided with feedback about the analysis—and the error-prevention strategies put in place—so that they understand that their event reporting leads to safer patient care and continue to participate in the process. Additionally, organizations must monitor the effectiveness of their error-prevention strategies to ensure they have the intended effect.

**Stamp out complacency.** Errors can occur as health IT users become more complacent with the technology, causing them to skip or reject alerts with important insights and resort to workarounds that drift further from the expected practice (IOM). Once health IT systems are fully deployed, organizations must monitor these hazards that can develop at the human-computer interface and take steps to address them. Refer to "Workarounds: Examine Why Staff Develop Them, Then Tackle Solutions" and "Establish Alert Priorities to Minimize Alert Fatigue" for recommendations to address workarounds and alert fatigue.

## CONCLUSION

Health IT's promise for improved patient safety and healthcare delivery is great, but so too are its risks of jeopardizing patient safety and care if organizations fail to address, throughout the life cycle of any health IT project, the issues raised by this Deep Dive report. As healthcare facilities respond to government incentives to adopt health IT, they must also keep their attention focused on how systems affect safety to ensure that the benefits of health IT can be realized.

IOM notes in its report on health IT and patient safety that health IT safety is a shared responsibility of users, policymakers, and vendors. Healthcare organizations and their health IT users, as well as researchers, policymakers, and vendors, must continue to monitor the unintended consequences of health IT and share their findings. The lessons learned from projects such as ECRI Institute PSO's Deep Dive of health IT-related events will foster the development, adoption, and use of the safest systems for the best care.

## Online Resources

- ▷ Agency for Healthcare Research and Quality
  - Employee/staff perceptions electronic health record system survey. [http://healthit.ahrq.gov/portal/server.pt/document/954334/employee-staffperceptionshealthrecordsystemssurvey\\_pdf](http://healthit.ahrq.gov/portal/server.pt/document/954334/employee-staffperceptionshealthrecordsystemssurvey_pdf).
  - Health information technology evaluation toolkit. [http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS\\_0\\_1248\\_875888\\_0\\_0\\_18/09\\_0083\\_EF.pdf](http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_875888_0_0_18/09_0083_EF.pdf).
  - Health IT Hazard Manager beta-test: final report. <http://healthit.ahrq.gov/HealthITHazardManagerFinalReport>.
  - Patient safety event report—hospital: device or medical/surgical supply, including health information technology (HIT). [https://www.psoppc.org/c/document\\_library/get\\_file?uuid=75912503-7bd1-4e99-a678-5dbb70008e95&groupId=10218](https://www.psoppc.org/c/document_library/get_file?uuid=75912503-7bd1-4e99-a678-5dbb70008e95&groupId=10218).
  - Workflow assessment for health IT toolkit. [http://healthit.ahrq.gov/portal/server.pt/community/health\\_it\\_tools\\_and\\_resources/919/workflow\\_assessment\\_for\\_health\\_it\\_toolkit/27865](http://healthit.ahrq.gov/portal/server.pt/community/health_it_tools_and_resources/919/workflow_assessment_for_health_it_toolkit/27865).
- ▷ American Health Information Management Association
  - Auditing copy and paste. [http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1\\_042416.hesp?dDocName=bok1\\_042416](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_042416.hesp?dDocName=bok1_042416).
- ▷ National Institute of Standards and Technology
  - Technical evaluation, testing, and validation of the usability of electronic health records. [http://www.nist.gov/healthcare/usability/upload/EUP\\_WERB\\_Version\\_2\\_23\\_12-Final-2.pdf](http://www.nist.gov/healthcare/usability/upload/EUP_WERB_Version_2_23_12-Final-2.pdf).
- ▷ New York Department of Health and Mental Hygiene
  - Post-EHR implementation survey of providers. <http://www.healthit.gov/unintended-consequences/sites/default/files/pdf/ModuleIIpdf7.pdf>.
- ▷ Office of the National Coordinator for Health Information Technology
  - Causal statements and corrective actions [template]. <http://www.healthit.gov/unintended-consequences/sites/default/files/causal-statement.xls>.
- Health IT journeys: stories from the road. [http://healthit.hhs.gov/portal/server.pt?CommunityID=1958&spaceID=5&parentname=&control=SetCommunity&parentid=&in\\_hi\\_userid=11673&PageID=0&space=CommunityPage](http://healthit.hhs.gov/portal/server.pt?CommunityID=1958&spaceID=5&parentname=&control=SetCommunity&parentid=&in_hi_userid=11673&PageID=0&space=CommunityPage).
- Health IT survey compendium [including readiness assessment surveys]. [http://healthit.ahrq.gov/portal/server.pt/community/health\\_it\\_tools\\_and\\_resources/919/health\\_it\\_survey\\_compendium/27874](http://healthit.ahrq.gov/portal/server.pt/community/health_it_tools_and_resources/919/health_it_survey_compendium/27874).
- [Issue log template]. <http://www.healthit.gov/unintended-consequences/sites/default/files/issue-log.xls>.
- [Starter set root-cause analysis questions for EHR-related problems]. <http://www.healthit.gov/unintended-consequences/sites/default/files/starter-set.xls>.

## References

- 42 USC §§ 17901-17953 (2011).
- 42 USC §§ 300jj-300jj-51 (2011).
- Agency for Healthcare Research and Quality (AHRQ):
- Device or medical/surgical supply, including health information technology (HIT) [online]. In: Hospital Common Formats—version 1.2: event descriptions, sample reports, and forms. 2012 [cited 2012 Aug 26]. [https://www.psoppc.org/web/patientsafety/version-1.2\\_documents](https://www.psoppc.org/web/patientsafety/version-1.2_documents).
- Common Formats glossary [online]. In: Hospital Common Formats—version 1.2: event descriptions, sample reports, and forms. 2012 Apr [cited 2012 Oct 22]. [https://www.psoppc.org/web/patientsafety/version-1.2\\_documents](https://www.psoppc.org/web/patientsafety/version-1.2_documents).
- American College of Surgeons (ACS). Negotiating the electronic health record vendor contract [online]. 2011 Feb 23 [cited 2012 Sep 1]. [http://www.facs.org/fellows\\_info/bulletin/negotiatingehr.html](http://www.facs.org/fellows_info/bulletin/negotiatingehr.html).
- American National Standards Institute/Association for the Advancement of Medical Instrumentation/International Electrotechnical Commission (ANSI/AAMI/IEC). *Application of risk management for IT networks incorporating medical devices—part 1: roles, responsibilities and activities*. ANSI/AAMI/IEC 80001-1. Arlington (VA): AAMI; 2010 Oct.
- Ash JS, Berg M, Coiera E. Some unintended consequences of information technology in health care: the nature of patient care information

- system-related errors. *J Am Med Inform Assoc* 2004 Mar-Apr;11(2):104-12.
- Ash JS, Kilo CM, Shapiro M, et al. Roadmap for provision of safer healthcare information systems: preventing e-iatrogenesis. Appendix C. In: Institute of Medicine. *Health IT and patient safety: building safer systems for better care*. Washington (DC): National Academies Press; 2012:1-45.
- Birk S. CPOE: a clear purpose plus top-notch technical support equals high physician adoption. *Healthc Exec* 2010 May-Jun;25(3):24-30.
- California Healthcare Foundation (CHF). Workflow analysis: EHR deployment techniques [online]. 2011 Jan [cited 2012 Aug 30]. <http://www.chcf.org/~media/MEDIA%20LIBRARY%20Files/PDF/W/PDF%20WorkflowAnalysisEHRDeploymentTechniques.pdf>.
- Coiera E, Aarts J, Kulikowski C. The dangerous decade. *J Am Med Inform Assoc* 2012 Jan-Feb;19(1):2-5.
- Day RO, Roffe DJ, Richardson KL, et al. Implementing electronic medication management at an Australian teaching hospital. *Med J Aust* 2011 Nov 7;195(9):498-502.
- DeVore SD, Figlioli K. Lessons Premier hospitals learned about implementing electronic health records. *Health Aff (Millwood)* 2010 Apr;29(4):664-7.
- Dixon BE, Zafar A. *Inpatient computerized provider order entry: findings from the AHRQ Health IT Portfolio*. AHRQ publication no. 09-0031-EF. Rockville (MD): Agency for Healthcare Research and Quality; 2009 Jan.
- ECRI Institute:
- Crossing the connectivity chasm: pinpointing gaps in readiness to exchange health information [white paper online]. 2012 [cited 2012 Oct 23]. <https://www.ecri.org/hie>.
- Top 10 health technology hazards for 2013: key patient safety risks, and how to keep them in check [guidance article]. *Health Devices* 2012 Nov;41(11):342-65.
- Top 10 technology hazards for 2011: a guide for prioritizing your patient safety initiatives [guidance article]. *Health Devices* 2010 Nov;39(11):404-16.
- Top 10 technology hazards for 2012: the risks that should be at the top of your prevention list [guidance article]. *Health Devices* 2011 Nov;40(11):358-73.
- Institute of Medicine (IOM). *Health IT and patient safety: building safer systems for better care*. Washington (DC): National Academies Press; 2011 Nov 8.
- Joint Commission. Safely implementing health information and converging technologies. *Sentinel Event Alert* 2008 Dec 11;(42):1-4. Also available at [http://www.jointcommission.org/sentinel\\_event\\_alert\\_issue\\_42\\_safely\\_implementing\\_health\\_information\\_and\\_converging\\_technologies](http://www.jointcommission.org/sentinel_event_alert_issue_42_safely_implementing_health_information_and_converging_technologies).
- Kaushal R, Shojania KG, Bates DW. Effects of computerized physician order entry and clinical decision support systems on medication safety: a systematic review. *Arch Intern Med* 2003 Jun 23;163(12):1409-16.
- Kilbridge P. Computer crash—lessons from a system failure. *N Engl J Med* 2003 Mar 6;348(10):881-2.
- Koppel R. Patient safety and health information technology: learning from our mistakes [perspective online]. *WebM&M* 2012 Jul [cited 2012 Aug 29]. <http://webmm.ahrq.gov/perspective.aspx?perspectiveID=124>.
- Koppel R, Metlay JP, Cohen A, et al. Role of computerized physician order entry systems in facilitating medication errors. *JAMA* 2005 Mar 9;293(10):1197-203.
- Magrabi F, Ong MS, Runciman W, et al:
- An analysis of computer-related patient safety incidents to inform the development of a classification. *J Am Med Inform Assoc* 2010 Nov-Dec;17(6):663-70.
- Using FDA reports to inform a classification for health information technology safety problems. *J Am Med Inform Assoc* 2012 Jan-Feb;19(1):45-53.
- McBride S, Delaney JM, Tietze M. Health information technology and nursing. *Am J Nurs* 2012 Aug;112(8):36-42.
- Moniz B. Examining the unintended consequences of computerized provider order entry system implementation [online]. *Online J Nurs Inform* 2009 Feb [cited 2012 Aug 31]. [http://ojni.org/13\\_1?moniz.pdf](http://ojni.org/13_1?moniz.pdf).
- Premier Inc. A conversation with Mark Zandi [online]. *Economic Outlook* 2012 Spring [cited 2012 Aug 13]. [https://www.premierinc.com/costs/economic-outlook/attachments/2012/FY12\\_spring\\_EO\\_PUBLIC\\_final\\_web.pdf](https://www.premierinc.com/costs/economic-outlook/attachments/2012/FY12_spring_EO_PUBLIC_final_web.pdf).
- Ramirez A, Carlson D, Estes C. Computerized physician order entry: lessons learned from the trenches. *Neonatal Netw* 2010 Jul-Aug;29(4):235-41.
- Shuren J. Statement to Institute of Medicine committee on patient safety and health information technology [online]. 2010 Dec 14 [cited 2012 Sep 27]. <http://www.iom.edu/~media/Files/Activity%20Files/Quality/PatientSafetyHIT/Meeting%201/Jeff%20Shuren%20-%20Oral%20Statement%20to%20the%20IOM.pdf>.
- Sittig DF, Campbell E, Guappone K, et al. Recommendations for monitoring and evaluation of in-patient computer-based provider order entry systems: results of a Delphi survey. *AMIA Annu Symp Proc* 2007 Oct 11:671-5. Also available at <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2655851>.
- Sittig DF, Singh H:
- Defining health information technology-related errors. *Arch Intern Med* 2011 Jul 25;171(14):1281-4.
- Eight rights of safe electronic health record use. *JAMA* 2009 Sep 9;302(10):1111-3.
- A new socio-technical model for studying health information technology in complex adaptive healthcare systems. *Qual Saf Health Care* 2010 Oct;19(Suppl 3):i68-74.
- U.S. Food and Drug Administration (FDA). Testimony of Jeffrey Shuren, Director of FDA's Center of Devices and Radiological Health [online]. 2010 Feb 25 [cited 2012 Aug 14]. [http://healthit.hhs.gov/portal/server.pt/document/910717/3shuren\\_testimony022510.pdf](http://healthit.hhs.gov/portal/server.pt/document/910717/3shuren_testimony022510.pdf).
- Weiner JP, Kfuri T, Chan K, et al. "e-Iatrogenesis": the most critical unintended consequence of CPOE and other HIT. *J Am Med Inform Assoc* 2007 May-Jun;14(3):387-8.
- Weinstock M. Ensuring that your EMR doesn't turn into HAL [online]. *Hosp Health Netw Dly* 2012 Jul 5 [cited 2012 Sep 3]. <http://www.hhnmag.com/hhnmag/HHNDaily/HHNDailyDisplay.dhtml?id=3240005051>.

The background of the entire page is a deep blue underwater scene. Several fish of various species are swimming in different directions. In the lower right corner, there is a large, branching piece of coral. The lighting is soft, creating a serene and naturalistic atmosphere.

# ECRI Institute

The Discipline of Science. The Integrity of Independence.

▷ UNITED STATES

5200 Butler Pike,  
Plymouth Meeting, PA  
19462-1298, USA  
Telephone +1 (610) 825-6000  
Fax +1 (610) 834-1275

▷ EUROPE

Weltech Centre, Ridgeway,  
Welwyn Garden City,  
Herts AL7 2AA, UK  
Telephone +44 (1707) 871 511  
Fax +44 (1707) 393 138

▷ ASIA PACIFIC

11-3-10, Jalan 3/109F,  
Danau Business Centre,  
Taman Danau Desa,  
58100 Kuala Lumpur, Malaysia  
Telephone +60 3 7988 1919  
Fax +60 3 7988 1170

▷ MIDDLE EAST

708/16 Fairmont Hotel,  
Sheikh Zayed Road,  
PO Box 24459  
Dubai, United Arab Emirates  
Telephone +971 4 3042460  
Fax +971 4 3042461