Investigations of Health IT–related Deaths, Serious Injuries or Unsafe Conditions

Final Report

Contract number:
HHSP233201300019C

Prepared for:
Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Project Officer: Kathy Kenyon, JD, MA
330 C Street SW Room 1200
Washington, DC 20201

Joint Commission Project Team:
Gerard Castro, PhD, MPH
Lisa Buczkowski, MS, RN
Joanne Hafner, MS, RN
Stacey Barrett, MS
Ken Rasinski, PhD
Scott Williams, Psy.D.

The Joint Commission
One Renaissance Boulevard
Oakbrook Terrace, IL 60181

Phone: 630-792-5972
Fax: 630-792-4972

March 30, 2015

ACKNOWLEDGEMENTS

This study was made possible through a contract (contract number: HHSP233201300019C) from the federal Office of the National Coordinator for Health Information Technology (ONC).This in no small part was due to the vision and leadership of ONC Senior Policy Advisor Kathy Kenyon who served as advisor and project officer.

We are also grateful for the time and contributions of the four medical centers for hosting the project team learning visits. The organizations and individuals were promised that their information and identities would be kept confidential, but their candid feedback and willingness to share greatly enhanced the substance of the project findings and will help advance health IT safety. We would also like to thank the subject matter experts who participated in the learning visits and advised us on the development of the online educational module:

- Peter Almenoff, MD, Assistant Deputy Under Secretary for Health, Quality and Safety, Department of Veterans Affairs
- Danielle Hoover, MD, Patient Safety Physician, National Center for Patient Safety, Veterans Health Administration
- Jeanie Scott, MT, Director of Informatics Patient Safety, Office of Informatics and Analytics/Health Informatics, Veterans Health Administration
- Hardeep Singh, MD, MPH, Chief, Health Policy, Quality & Informatics Program, Center for Innovations in Quality, Effectiveness and Safety, Michael E. DeBakey VA Medical Center
- Dean Sittig, PhD, Professor, University of Texas, Memorial Hermann Center for Healthcare Quality and Safety

TABLE OF CONTENTS

PAGE

LIST OF TABLES

LIST OF FIGURES

Investigations of Health IT–related Deaths, Serious Injuries or Unsafe Conditions
Final Report
March 30, 2015

Executive Summary

In July 2013 the Department of Health and Human Services (HHS) issued its *Health IT Patient Safety Action and Surveillance Plan* ("Health IT Safety Plan"). The Health IT Safety Plan addresses the role of health information technology (IT) within HHS's commitment to patient safety and builds on recommendations from the 2011 Institute of Medicine report, *Health IT and Patient Safety: Building Safer Systems for Better Care*. It has two fundamental objectives: (1) use health IT to make care safer, and (2) continuously improve the safety of health IT.

The Health IT Safety Plan proposes actions that HHS and private sector stakeholders can take to improve health IT safety, organized under three strategies:

1. **Learn:** Increase the quantity and quality of data and knowledge about health IT safety
2. **Improve:** Target resources and corrective actions to improve health IT safety and patient safety
3. **Lead:** Promote a culture of safety related to health IT

Towards this end the ONC contracted with The Joint Commission to establish a credible and meaningful process that can be used to identify, understand, disseminate and eventually help prevent health IT-related sentinel events that may cause serious or fatal harm to patients (contract number: HHSP233201300019C).

As part of The Joint Commission's accreditation program, organizations voluntarily report sentinel events to The Joint Commission's Office of Quality and Patient Safety (OQPS). The OQPS staff works with organizations to review the results of their investigation and root cause analysis to ensure that they are thorough and credible. The data from these reports are de-identified, aggregated, and shared to increase public knowledge about sentinel events, their causes, and strategies for prevention. ONC's contract with The Joint Commission has the following objectives:

- To support root cause analyses and investigations of health IT-related sentinel events, in both hospitals and ambulatory settings, as part of The Joint Commission's ongoing Sentinel Events program;
- To make information publicly available on identifying and avoiding health IT-related sentinel events;
- To better understand health IT-related sentinel events in the context of all causes of sentinel events;
- To evaluate factors that impact effective investigations of health IT-related sentinel events and the role of external organizations in such investigations;
- To provide information that will enable ONC to strengthen its health IT patient safety programs.

This Executive Summary includes a brief overview of the findings from the analysis of 120 reported health IT-related sentinel events and learning visits to four accredited medical centers.

Analysis of Health IT-related Sentinel Events
Joint Commission staff performed categorical and keyword queries of the sentinel event incident reports reported between January 1, 2010 and June 30, 2013 (n=3,375). Content analysis of the full incident reports yielded 120 sentinel events where health IT was a contributing factor. The 120 health IT-related sentinel events fell into 15 different types of events. The three most frequent types of events were (1) medication errors, (2) wrong-site surgery (which encompasses surgery performed on the wrong side or site of the body, wrong surgical procedure performed, and surgery performed on the wrong patient), and (3) delays in treatment.

Since there are multiple contributing factors to any one sentinel event, 305 health IT-related contributing factors were identified across the 120 health IT-related sentinel events. Contributing factors associated with the *human-computer interface* were identified most frequently, representing 33% of all contributing

factors. The next most frequently identified contributing factors were related to *workflow and communication* (24%) and to *clinical-content* (23%).

The AHRQ Common Formats Hospital Version 1.2 for "Device or Medical/Surgical Supply, including Health Information Technology," was used to categorize the type of health IT device involved. More than one health IT device can be involved in a sentinel event so the number of health IT devices involved (n=147) is greater than the number of health IT related sentinel events (n=120).[1] In the Common Formats, EHRs and components of EHRs including CPOE systems, pharmacy systems, e-MARs, clinical documentation systems (e.g., progress notes), and clinical decision support (CDS) systems are grouped together. The majority (66%) of health IT-related sentinel events involved EHRs or some component of the EHR.

Learning Visits

The Joint Commission completed four learning visits at Joint Commission accredited medical centers. A "learning visit" is a non-accreditation related information gathering process that is frequently used to support the development of accreditation standards and was adapted to meet the objectives of this project. During the course of a learning visit Joint Commission staff seek to learn more about an organization's unique features, structure, operations, patient population, and provision of care, treatment and services. The Joint Commission sought to learn how health IT in the hospital: (1) is organized, operates and contributes to patient safety and quality of care; (2) is integrated into and functions within a larger organization; (3) helps to maintain a patient-centered focus in its approach to and delivery of care; and (4) can introduce risk or lead to unintended consequences. These visits are interactive and mutually beneficial to the organization and Joint Commission staff.

Participating hospitals and medical centers were recruited through referrals by project advisors and members of the Joint Commission Patient Safety Advisory Group yielding a convenience sample of relative variability: a suburban, not-for-profit hospital outside a large metropolitan area; an urban, not-for-profit hospital in a large metropolitan area; a large, academic medical center; and a Veterans Affairs medical center. All of the participating medical centers had mature, well-functioning health IT systems.

During the learning visits, discussions centered on the implementation or integration of a specific health IT hardware or system such as electronic health records, CPOE, or laboratory information system. The researchers also discussed workflows, processes, policies, and procedures with clinical leadership, IT staff, quality and safety staff, clinical users, and administrative users. The team also discussed with medical center representatives how health IT-related hazards or unsafe conditions were identified and what actions were taken to reduce the risk of harm to patients. The learning visit discussions also included examples of health IT-related patient safety events, the organizations' experience, and what was learned as a result.

Key Findings and Conclusion

The Joint Commission's analysis of health IT-related sentinel events suggests that risks and hazards associated with health IT are uncovered through comprehensive systematic analyses, such as a root cause analysis, of adverse events. Since the distinguishing characteristic of sentinel events is primarily severe patient harm or death, the identification of health IT as a contributing factor to the event will likely be uncovered during the course of the investigation and root cause analysis. In other words, health IT as a contributing factor in this analysis was a latent condition that may not be readily apparent when the event occurs. Identifying the role of health IT in adverse events often requires special expertise. Using Reason's oft-cited Swiss cheese analogy, health IT as a contributing factor to a sentinel event is a vulnerability represented by a hole in one of the layers of Swiss cheese furthest away from the patient.[2] This also means that when health IT is functioning optimally, the vulnerability is mitigated and health IT may help prevent patient harm.

Once health IT is identified as a potential contributing factor, the organization's information technology, clinical informatics, or biomedical engineering staff should be involved in the analysis to help uncover specifically how the technology could have contributed to the event, such as through poor human-

computer interface design, data integrity issues caused by poor system to system interfaces, software configuration issues, or failure of the software to meet user expectations, in the context of the existing clinical workflows.

Since health IT as a contributing factor was usually identified as a vulnerability or latent factor, rather than a more direct or immediate cause of harm, recognition and reporting health IT-related hazards necessitates staff "situational awareness."[3] Recognition involves not only identification of health IT-related hazards but also recognition of the potential patient harm that could result if the hazard is not mitigated. This can only be successful in an organization with a strong patient safety infrastructure characterized by a culture of safety where hazards and close calls ("near misses") are routinely reported, process improvement is comprehensive and systematic, and leadership acts upon the identified issues in a timely manner.[4-6] Proactive risk assessments, such as Failure Mode and Effects Analysis and the ONC Safety Assurance Factors for EHR Resilience (SAFER) Guides,[7] should be integrated into a strong patient safety infrastructure in order to identify health IT-related hazards before harm reaches the patient.

The Joint Commission's learning visits to medical centers found that interdisciplinary collaboration among IT professionals, clinical staff, biomedical engineering, and patient safety staff, supported by strong leadership commitment to health IT as a way to improve patient safety, were common factors for successful implementation and safe use of health IT. Despite their focused efforts, the medical centers faced several similar challenges associated with the design and use of health IT. Depending on how the health IT system is designed and implemented, relevant clinical information can be difficult to find in the EHR contributing to difficulties following the clinical care of patients. Health IT as a barrier to communication among clinicians and with patients also emerged as a common theme. Overall, each of the participating medical centers struggled with how health IT changes clinical workflows and with finding the best ways to safely and efficiently integrate health IT systems into those workflows.

The medical centers, like most, struggle with problems associated with technology. However, the medical centers we visited had empowered, knowledgeable staff who work collaboratively to find ways to balance clinical workflow, cross organizational silos, and alleviate technology limitations. They also used technology to monitor for hazards and safety issues. In each of the medical centers, the organizational leadership recognized that safe technology and safe use of technology are priorities.

Private and federal safety organizations that aggregate and analyze patient safety event reports such as The Joint Commission, Patient Safety Organizations (PSOs), or the VA National Center for Patient Safety play an important role in enhancing health IT safety. They can collect adverse event reports while maintaining privacy and confidentiality protections. Aggregation and analysis of patient safety event reports facilitates identification of risks and hazards that may not be readily apparent to an individual healthcare organization. Safety organizations also assist healthcare organizations in their adverse event investigations and analyses by helping them probe into health IT-related latent conditions and associated workflows. Reports on health IT-related hazards (properly de-identified) and learning tools produced by safety organizations can be shared and can serve as valuable educational resources.[8-11] An individual healthcare organizations' ability to utilize these external resources however is dependent on the strength of its patient safety infrastructure.[4-6]

Avoiding the kinds of health IT-related hazards the Joint Commission identified in its research and optimizing the role of health IT in patient safety requires more intentional collaboration among stakeholders than currently exists. The problems identified in our research were clearly related both to health IT design issues, which are often largely within the control of health IT developers, and to implementation, maintenance, use, and oversight, which are primarily the responsibility of healthcare organizations (even when they can only be addressed with developer support). This intentional collaboration should occur within the safety and quality programs of healthcare organizations, as they work with their health IT developer partners to implement and service health IT.

However, health IT safety and the broader goal of using health IT to continuously improve patient safety requires more than collaboration **within** healthcare organizations. Collaboration on health IT and patient

safety should also occur nationally, as part of a learning collaborative, where stakeholders contribute knowledge, evidence, research, and expertise, and learn from each other. Clinicians and patients, who rely upon the safety of health IT (as designed, implemented, and maintained by others), should be engaged as well.

The Joint Commission agrees with the recommendation made in the draft FDASIA Health IT Report (April 2014), to create and support an environment of learning and continual improvement related to health IT and patient safety. One means of doing so proposed in the draft FDASIA report was a Health IT Safety Center, as a public-private entity to serve as "a trusted convener of health IT stakeholders in order to focus on activities that promote health IT as an integral part of patient safety..." Whether through a federally funded Health IT Safety Center, or some other means, the Joint Commission supports the need for collaboration at a national level on health IT safety as part of a learning collaborative.

I. Analysis of Health IT-related Sentinel Events

A. Defining Patient Safety Events

Definitions of patient safety events (PSEs) differ widely. The definition of patient safety event and how it is applied will determine the information that is collected on different types of events. Different definitions hinder systematic aggregation of data from incident reports, but all agree about differentiating events that reach the patient versus those that do not.[12-14] Patient safety events are circumstances that could have resulted, or did result, in unnecessary harm to a patient.[15] Defining PSEs in this way includes close calls (also called "near misses") and hazards. Patient safety events can be categorized into four different types (Figure 1):

Adverse event—an incident that resulted in harm to a patient. This includes "sentinel events" (defined below in the Methods Section).

No harm event—an incident that reached a patient, but no discernable harm resulted.

Close call ("near miss" or "good catch")—an incident that did not reach the patient. The more widely used term in patient safety literature is "near miss," but close call is the more descriptive term.

Hazard/unsafe condition—a situation in which there was potential for harm, but no incident occurred.

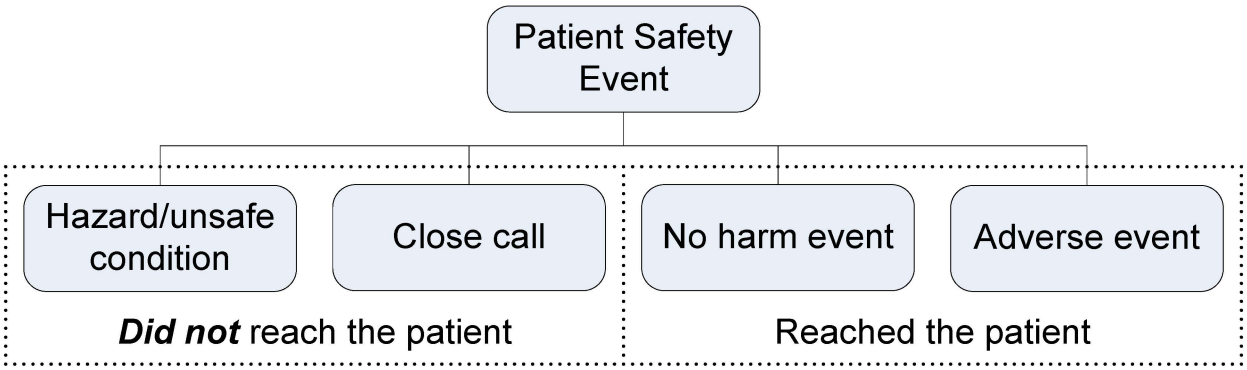

Figure 1. Types of patient safety events

The distinguishing factor between close calls and adverse events is whether or not the event reached the patient. As an example, if a nurse performing a medication double-check—which includes confirming the correct medication, dose, route, timing, and patient—realizes that it is the wrong dose prior to administering it to the patient, the event is a close call. If, however, the wrong dose is administered to the patient, the event "reached the patient" and can result in either no harm or an adverse event. Key aspects of close calls and adverse events can be identical (e.g., in contributing factors, people, and processes involved) except for the distinguishing factor of reaching the patient. A comprehensive systematic analysis, such as a root cause analysis, of the contributing factors would be used to investigate both close calls and adverse events. By virtue of close calls not reaching the patient and, therefore, not causing harm, they are considered information-rich opportunities for learning.

B. Sociotechnical Model for Health IT

Health IT-related sentinel events do not occur in isolation, but in the context of a sociotechnical system that includes technology, people, processes, organizations, and the external environment.[16] This system includes all components of health IT and medical devices as well as external forces such as government regulations, incentives, and oversight. In order to reduce the risk of the occurrence of a health IT-related PSE, the interactions between the components of the system need to be studied. Health IT—when thoughtfully designed, systematically implemented, and used appropriately—can improve the quality and safety of healthcare provided to patients. When health IT design is inadequate, implemented

haphazardly, or used inappropriately, however, it can add a layer of complexity to an already complex system, which can lead to PSEs.[16]

When applied to health IT, the sociotechnical system model offers a more detailed depiction of the dynamics involved between the technology, people, and environment. A sociotechnical model describes the way the components of social systems and technical systems interact and the impact of these interactions. Considering health IT risks to patient safety in the context of an overarching sociotechnical model helps facilitate an understanding of the relationships between different components of the system.

Sittig and Singh[17] offer a model that specifically addresses the design, development, implementation, use, and evaluation of health IT. Their model adapts components of other related sociotechnical models,[18-23] and delineates the technology component to make it more specific to health IT. Sittig and Singh's eight dimensions of a sociotechnical model for evaluating health IT are as follows:

- Hardware and software—e.g., computers, keyboards, data storage, software to run health IT applications;
- Clinical content—data, information, and knowledge stored in the system;
- Human-computer interface—hardware and software interfaces that allow users to interact with the system or health IT device;
- People—software developers, IT department personnel, clinicians, healthcare staff, patients, and others involved in health IT development, implementation, and use;
- Workflow and communication—steps followed to ensure patients receive the care they need at the time they need it;
- 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;
- External rules, regulations, and pressures—external forces, such as federal and state rules to ensure privacy and security protections and federal payment incentives to spur health IT adoption; and
- System measurement and monitoring—processes to measure and monitor health IT features and functions.

Examining health IT-related patient safety events within the context of the sociotechnical model enables individuals and organizations to understand the PSE in the context of the people who use the system and the other technologies and processes affected by health IT.

C. Methods

The Joint Commission analyzed a de-identified sample of sentinel events in its database, using a two-step process: (1) database queries, and (2) content analysis of the full sentinel event incident reports.

Sample

The sample of events was drawn from sentinel events reported to The Joint Commission by accredited organizations from January 1, 2010, to June 30, 2013, (n=3,375). The Joint Commission is an independent, not-for-profit organization that evaluates and accredits or certifies more than 20,000 healthcare organizations and programs in the United States. The Joint Commission, through its sentinel event reporting system, collects information on adverse events from accredited healthcare organizations to facilitate learning about ways to reduce the risk of harm to patients. Sentinel events reported to The Joint Commission are a unique subset of PSEs in that they are voluntarily reported from accredited organizations, focus primarily on significant or severe PSEs, and include findings from the organizations' root cause analyses. The Joint Commission Sentinel Event Policy provides the organizations with specifications for what types of incidents can be reported to The Joint Commission and what constitutes an acceptable (thorough and credible) root cause analysis.

Overview of The Joint Commission Sentinel Event Policy

At the time of the analysis,* The Joint Commission defined a sentinel event as an unexpected occurrence involving death or serious physical or psychological injury, or risk thereof.[24] The phrase "risk thereof" is important because sentinel events by definition include not only incidents where a patient has been harmed, but also "near misses," close calls, and hazardous conditions. The Joint Commission requires accredited healthcare organizations to create an organization-specific definition for sentinel events, derived from The Joint Commission's definition, and requires accredited organizations to conduct a root cause analysis of each event meeting this definition. A subset of those events, "reviewable sentinel events," are reviewable by The Joint Commission, and healthcare organizations are strongly encouraged to voluntarily report these to The Joint Commission. A reviewable sentinel event is an event that has resulted in an unanticipated death or major permanent loss of function, not related to the natural course of the patient's illness or underlying condition. Reviewable sentinel events also include the following specific event types, even if no serious harm occurred or the event is related to the natural course of the patient's illness:

- Suicide of any patient receiving care, treatment and services in a staffed around-the-clock care setting or within 72 hours of discharge;
- Unanticipated death of a full-term infant;
- Abduction of any patient receiving care, treatment, and services;
- Discharge of an infant to the wrong family;
- Rape, assault (leading to death or permanent loss of function), or homicide of any patient receiving care, treatment, and services;
- Rape, assault (leading to death or permanent loss of function), or homicide of a staff member, licensed independent practitioner, visitor, or vendor while on site at the health care organization
- Hemolytic transfusion reaction involving administration of blood or blood products having major blood group incompatibilities;
- Invasive procedure, including surgery, on the wrong patient, wrong site, or wrong procedure;
- Unintended retention of a foreign object in a patient after surgery or other invasive procedures;
- Severe neonatal hyperbilirubinemia (bilirubin > 30 milligrams/deciliter);
- Prolonged fluoroscopy with cumulative dose >1,500 rads to a single field; or any delivery of radiotherapy to the wrong body region or >25% above the planned radiotherapy dose.

Reviewable sentinel events are, therefore, a subset of PSEs that reach the patient and cause serious permanent harm or death, or types of events listed above.

Even though reporting of sentinel events is voluntary, as specified in the *Sentinel Event Policy*, if The Joint Commission is notified that a reviewable sentinel event has occurred at an accredited organization (e.g., through a complaint or the media), The Joint Commission will ensure that the organization has investigated and analyzed the incident. This activity is part of The Joint Commission's responsibility to hold organizations accountable for a "thorough and credible" response to an incident.[25]

A healthcare organization can use one of several mechanisms to report a sentinel event, including US mail, electronically through an online reporting tool, or an in-person interview. For all of these mechanisms, a Joint Commission "Patient Safety Specialist" (masters prepared nurses or human factors engineer) works with the organization, reviews the organization's root cause analysis, assures that the analysis meets the criteria for being "thorough and credible," and abstracts information from the organization's root cause analysis for entry into the sentinel event database.

A Root Cause Analysis Framework[26] is used to ensure that the organization has addressed the active failures and latent conditions[2] associated with the sentinel event. The Framework consists of 24 questions

* The definition has since been revised, effective January 2015.[25]

that ask the organization about the intended process flow, steps in the process flow that did not occur as intended, environmental factors, human factors, and organizational culture. The responses to these questions are typically uncovered during the course of the organization's root cause analysis and are included in the sentinel event report to The Joint Commission.

Identifying health IT-related sentinel events

Prior to querying the database, the sentinel event incident reports reported between January 1, 2010 and June 30, 2013, (n=3,375) were de-identified in accordance with the Health Insurance Portability and Accountability Act.[27] A combination of categorical and keyword queries was used to identify sentinel events where health IT may have been involved. This was followed by application of criteria from the AHRQ Common Format to identify health IT-related sentinel events.

Keyword queries were performed on the narrative components of the sentinel event report adapting an approach developed by Sparnon.[28] A literature review was performed to generate keywords for the keyword query. Keywords such as "EMR," "EHR," "PACS," and vendor names were used in the query. The investigator then applied criteria based on the AHRQ Common Format (Figure 2) to determine health IT involvement in the sentinel event. In cases where the involvement of health IT was possible, the sentinel event was included for the next round of analysis. A total of 195 potentially health IT related events were identified through the queries.

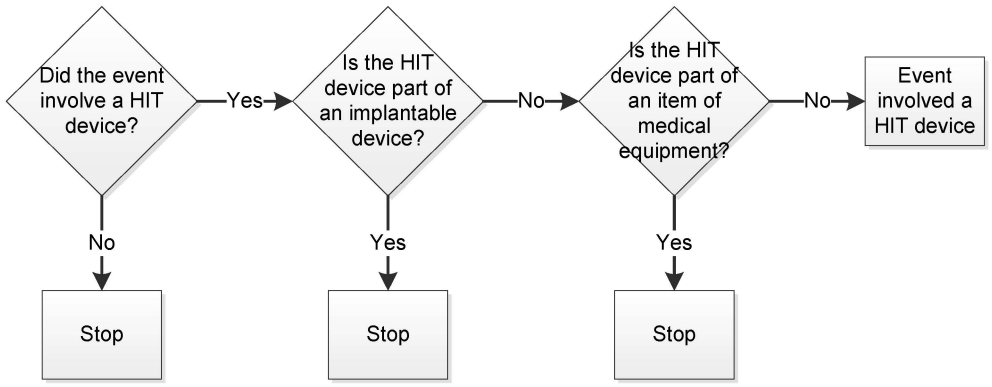

Figure 2. Algorithm for identifying health IT-related events

The next round of analysis involved two master's-level nurses and the principal investigator performing content analysis of all the full sentinel event incident reports which includes the organization's responses to the Root Cause Analysis Framework questions to determine if health IT contributed to or caused the event, and if so, how and why did health IT contribute to or cause the event.[26] A qualitative confirmatory analysis was performed on the details captured by the reviewers of how and why health IT contributed to or caused the event to the identify concepts and themes. Using existing classifications of health IT-related contributing factors, including the AHRQ Common Formats,[1] AHRQ Hazard Manager Ontology,[29] Magrabi's classification,[30] and Sittig and Singh's sociotechnical model,[17] the principal investigator created a composite classification of health IT-related contributing factors organized by sociotechnical dimensions.[31] This classification was used to code the contributing and causal factors identified during the review.

The sentinel events were also categorized using a component of the AHRQ Common Formats Hospital Version 1.2 for "Device or Medical/Surgical Supply, including Health Information Technology."[1] Specifically, the classification of health IT devices related to the event or unsafe condition in Question 21 of the abovementioned Common Formats was used to categorize what type of devices were involved in the sentinel event.

D. Results

The queries and content analysis of the sentinel event incident reports resulted in the identification of 120 sentinel events where health IT was a contributing factor. The 120 health IT-related sentinel events resulted in 15 different types of events. The three most frequent health IT-related events were (1) medication errors, (2) wrong-site surgery (which encompasses surgery performed on the wrong side or site of the body, wrong surgical procedure performed, and surgery performed on the wrong patient), and (3) delays in treatment. All health IT-related sentinel event types are listed in Table I.

TABLE I
HEALTH IT-RELATED SENTINEL EVENT TYPES

Event Type	% (n=120)
Medication error	29% (35)
Wrong-site surgery	19% (23)
Delay in treatment	12% (14)
Suicide	8% (10)
Fall	6% (7)
Radiation overdose	6% (7)
Transfusion error	4% (5)
Unintended retention of a foreign body	4% (5)
Op/Post-op complication	3% (4)
Med equipment-related	3% (3)
Other unanticipated event	2% (2)
Perinatal death/injury	2% (2)
Transfer-related event	1% (1)
Maternal death	1% (1)
Ventilator death	1% (1)

One sentinel event can impact more than one patient. The 120 health IT-related sentinel events affected 125 patients. The sentinel events resulted in the deaths of a little more than half of the patients (53%, n=66), unexpected additional care or extended stay for approximately one-third (30%, n=37), and permanent loss of function for 11% (n=14). "Other outcomes" not resulting in death, additional care, extended stay, or permanent loss of function were reported for 6% (n=7). Psychological impact was reported for one patient (1%). See Figure 3 for a comparison of patient outcomes.

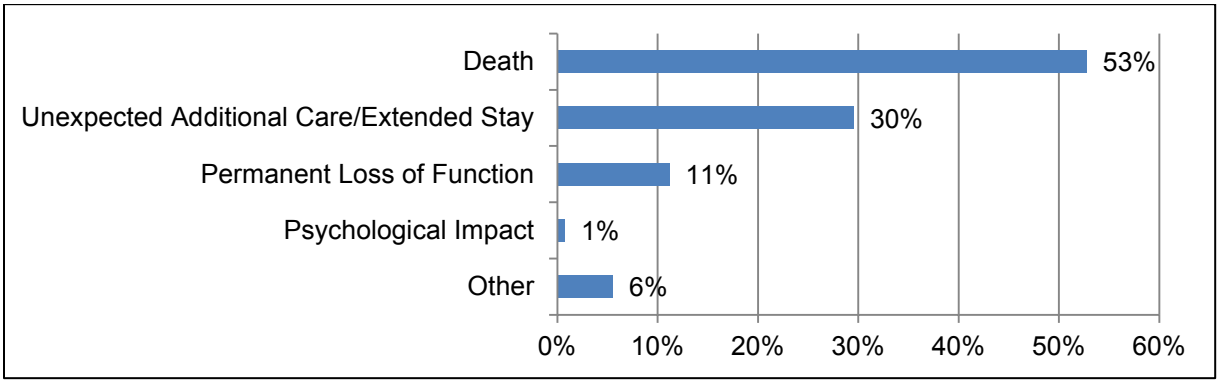

Figure 3. Patient outcomes for health IT-related sentinel events

Each sentinel event is associated with multiple contributing factors. Three hundred five health IT-related contributing factors were identified (Table II) and were categorized by sociotechnical dimension.

Contributing factors associated with the human-computer interface were identified most frequently, representing 33% of all contributing factors. The next most frequently identified contributing factors were workflow and communication related (24%) and clinical-content related (23%). The remaining dimensions and their percentages are listed in Table II.

TABLE II
CLASSIFICATION OF SOCIOTECHNICAL DIMENSIONS

Sociotechnical Dimensions	% (n=305)
Human-computer interface	33% (101)
Workflow and communication	24% (72)
Clinical content	23% (70)
Internal organizational policies, procedures, and culture	7% (20)
People	6% (19)
Hardware and software computing infrastructure	6% (18)
External rules, regulations, and pressures	1% (3)
System measurement and monitoring	1% (2)

The AHRQ Common Formats Hospital Version 1.2 for "Device or Medical/Surgical Supply, including Health Information Technology," was used to categorize the type of health IT involved. More than one health IT device can be involved in a sentinel event so the number of health IT devices involved (n=147) is greater than the number of health IT related sentinel events (n=120). In the Common Format, EHRs and components of EHRs including CPOE systems, pharmacy systems, e-MARs, clinical documentation systems (e.g., progress notes), and CDS systems are grouped together. The majority (66%) of health IT-related sentinel events involved EHRs or some component of the EHR. If specific component of EHR was identified in the report, it was grouped into an appropriate subcategory (i.e., CPOE, CDS). When a sentinel event was identified as having involved the EHR, but did not specify which component was involved, it was included in the general "EHR" subcategory. The distribution of health IT devices is listed in Table III.

Health IT categories	% (n=147)	
EHR or component of EHR		66% (97)
EHR	22% (32)	
CPOE system	20% (29)	
e-MAR	9% (13)	
Clinical documentation system (e.g. progress notes)	7% (10)	
Pharmacy system	6% (9)	
CDS System	3% (4)	
Radiology/diagnostic imaging system, including PACS		14% (20)
Human interface device (e.g., keyboard, mouse, touchscreen, speech recognition system, monitor/display, printer)		7% (10)
Administrative/billing or practice management system—Registration /appointment scheduling system		6% (9)
Automated dispensing system		5% (7)
LIS, including microbiology, and pathology systems	3% (4)	

Sociotechnical dimension: human-computer interface
When the contributing factors from the health IT-related sentinel events were categorized by sociotechnical dimension, contributing factors in the human-computer interface dimension were identified most frequently, representing 33% of all contributing factors. These contributing factors primarily involved inaccurate data entry or erroneous data selection, difficulty finding information, or some aspect of the display of information that prevented the user from accurately interpreting the information. Examples of data entry problems from the health IT-related sentinel events included typing the dosage of a medication in the wrong field or entering weight in pounds instead of kilograms, which can affect the calculation of medication dosage administered to the patient.

Erroneous data selection typically involved the CPOE system and the selection of an incorrect procedure or medication. The erroneous data selection was in some events caused by the correct "orderable" or medication "order sets" not being available as a selection in the drop-down menu. Sentinel events associated with erroneous data selection also involved events where additional details regarding the procedure or medication were entered in the notes section of the system and then neither transferred appropriately nor viewed by the clinicians performing the procedure or administering the medication. In other events, the selection was "auto-populated" with the incorrect dosage, frequency, or procedure, and the selection was not corrected.

The location of the hardware presented problems by limiting the accessibility of information when it was needed. In one event, the view screen for the radiology image was not in the operating room, limiting the ability of the clinicians performing the "time out" to confirm the laterality of the procedure. The common theme for these contributing factors was that the technology interface facilitated the communication of erroneous information or limited the availability or accuracy of required clinical information.

Sociotechnical dimension: workflow and communication
The next most frequently identified contributing factors were related to the workflow and communication (24%) dimension. Of all identified contributing factors across all sociotechnical dimensions, "communication among team members" was most frequently identified. As previously mentioned, contributing factors associated with the human-computer interface dimension oftentimes impacted communication, so the contributing factors between these two dimensions were often associated with one sentinel event. Additionally, the most frequently identified contributing factors in this dimension were often identified together, describing slightly different aspects of the communication and workflow problems.

A theme that emerged in the analysis of health IT-related sentinel events associated with communication among team members was clinicians relying on the "notes" section of the EHR to convey critical patient information to another clinician, resulting in a second clinician not seeing the note, resulting in a delay in patient treatment. Another theme that emerged related to communication among team members was the use of hybrid systems (using paper and electronic records) for documentation. Clinicians were missing relevant clinical information because it was being maintained in multiple locations on paper, or in different electronic systems, contributing to an unclear clinical picture of the patient's condition.

This lack of cohesive clinical picture was characterized by the contributing factor "suboptimal support of teamwork," which was a frequently identified contributing factor in this dimension. For sentinel events related to this contributing factor, it was not only the device, but also the processes and workflows associated with the health IT. Hybrid systems again played a role because clinical information was documented on paper or electronically, but the information was not handed off during shift change to the next clinician providing care. The contributing factor discrepancies between user expectations and the function of the technology were often associated with communication among team members and suboptimal support of teamwork because the clinicians had the expectation that once the information was documented, it would be conveyed to the next clinician on shift.

Sociotechnical dimension: clinical content

Contributing factors in the clinical content-related dimension (23%) were associated with events in which clinical decision support safeguards were missing—often unexpectedly. As previously discussed, the clinical content dimension is associated with the data, information, and knowledge stored in the health information system. Since clinical decision support is built on established practice guidelines or performance measures, the absence of that established practice guideline or performance measure is identified as a contributing factor associated with the clinical content dimension. When reviewing the organizations' documented findings, it was often noted that clinicians were surprised by the absence of clinical decision support or other safeguards such as an alarm for when medications exceeded dosing limits. For other sentinel events that dealt with patient falls or suicide, organizations reported that clinicians had expected a prompt to perform a risk assessment if certain clinical criteria were entered into the EHR system. The failure to perform the risk assessment that would identify the risk of a patient fall or suicide is what ultimately contributed to the sentinel event.

Health information technology-related sentinel event types

The analysis of the 120 health IT-related sentinel events resulted in 15 different types of events, but most frequently resulted in medication errors, wrong-site surgery (which encompasses surgery performed on the wrong side or site of the body, wrong surgical procedure performed, and surgery performed on the wrong patient), and delays in treatment. This is not surprising given the contributing factors involved. Incorrect or erroneous data entry or selection of a procedure or medication within a CPOE system would ultimately result in a medication error or wrong-site surgery, respectively, if not identified before reaching the patient. In these cases, as previously mentioned, workflows associated with the health IT, such as medication double checks by the nurse administering the medication or a "time out" before the procedure, if performed appropriately could have prevented these events.

Health IT-related sentinel events resulting in a delay in treatment were more related to contributing factors such as communication among team members and suboptimal support of teamwork. The theme that was most relevant to these events was the failure to transfer relevant clinical information from one clinician to another, resulting in an incomplete clinical picture of the patient or a failure to recognize the severity of the patient's condition. For these events, the outcome for the patient was a delay in receiving a needed procedure or medication. Health IT-related sentinel events resulting in the suicide of the patient, the fourth most frequently identified event type, were also related to communication among team members and suboptimal support of teamwork. For these events, however, clinical content-related contributing factors were also associated with the failure to perform a suicide assessment or an expectation of the presence of a computer-based alert of suicide risk or to perform a suicide assessment.

Health information technology device involved

The identified contributing factors are most often related to the EHR and the CPOE (considered a component of the EHR), a relationship clearly demonstrated in the distribution of the different types of health IT devices involved (Table III). Contributing factors related to communication and teamwork were associated with the use of the EHR system. Contributing factors related to data entry or selection and to communication were associated with CPOE systems. Other systems were involved to a lesser extent, but it is interesting to note that radiology/diagnostic imaging systems, including PACS, were most often related to wrong-site surgery events due to the orientation of images.

II. Learning Visits

The Joint Commission performed four learning visits at four Joint Commission accredited medical centers. The "learning visit" approach was adapted for the purposes of this project and is an established Joint Commission process used to support the development of accreditation standards. Learning visits were utilized instead of on-site investigations of a sentinel event due to the lack of organizations voluntarily requesting Joint Commission on-site review of sentinel events. Participating medical centers were recruited through referrals by project advisors and members of the Joint Commission Patient Safety Advisory Group yielding a convenience sample of relative variability: a suburban, not-for-profit hospital outside a large metropolitan area; an urban, not-for-profit hospital in a large metropolitan area; a large, academic medical center; and a Veterans Affairs medical center. All of the participating medical centers could be characterized as having mature, well-functioning health IT systems and supporting organizational infrastructure.

During the course of a learning visit Joint Commission staff seek to learn more about an organization's unique features, structure, operations, patient population, and provision of care, treatment and services. The Joint Commission examined how health IT in the hospital: (1) is organized, operates and contributes to patient safety and quality of care; (2) is integrated into and functions within a larger organization; (3) helps to maintain a patient-centered focus in its approach to and delivery of care; and (4) can introduce risk or lead to unintended consequences. These visits are intended to be interactive and mutually beneficial to the organization and Joint Commission staff. Representatives from the participating medical centers were asked to draft a learning visit agenda around the following issues:

- People, processes and workflows associated with the use of health IT
- Policies and procedures on the use of health IT
- External factors that may influence a program or organization's safe use of health IT
- Hardware and software computing infrastructure
- User interfaces
- Risks and unintended consequences of health IT.

The project team for learning visits was composed of the principle investigator, Gerry Castro, and the Associate Director of the Sentinel Event Analysis Unit, Lisa Buczkowski. The following project advisors and subject matter experts accompanied the team on learning visits when available:

- Peter Almenoff, MD, Assistant Deputy Under Secretary for Health, Quality and Safety, Department of Veterans Affairs
- Danielle Hoover, MD, Patient Safety Physician, National Center for Patient Safety, Veterans Health Administration
- Jeanie Scott, MT, Director of Informatics Patient Safety, Office of Informatics and Analytics/Health Informatics, Veterans Health Administration
- Dean Sittig, PhD, Professor, University of Texas, Memorial Hermann Center for Healthcare Quality and Safety

Learning visit discussions ranged from a number of different topics such as implementation or integration of a specific health IT device or system including electronic health records, CPOE, or laboratory information system. Discussions on workflows, processes, policies, and/or procedures involved relevant clinical leadership, IT staff, quality and safety staff, clinical users, and administrative users. The team also discussed with medical center staff how health IT-related hazards or unsafe conditions were identified and what if any actions were taken to reduce the risk of harm to patients. Health IT-related patient safety events were discussed only if the organization was amenable to sharing.

A. Suburban, Not-for-profit Medical Center Outside a Large Metropolitan Area

The medical center is part of a health system of hospitals and ambulatory healthcare centers. The health system serves a large metropolitan and suburban area bordering two states. The team started the visit at the health system's Information Services (IS) facility that serves as the data center, help desk, and training center for the system's hospitals and ambulatory care centers. The project team was hosted primarily by the IS team which included the Chief Information Officer, Chief Technology Officer, and the Program Manager for Medical Device Systems. Clinical engineering and biomedical services are integrated into Information Services with IT. The integration has helped facilitate implementation of health IT enabled medical devices and their connection overall into health system facilities. The IS team feels that with clinical engineering integrated into IT, they are organizationally aligned to ensure that health IT is well integrated into clinical care. Since biomedical and clinical engineering are traditionally disconnected from IT, smaller community hospitals will struggle with implementation. The IS team commented that their role in patient safety has involved primarily implementation of technology and not investigation technology related safety events.

At the time of the learning visit the health system was in the process of transitioning from primarily one large EHR vendor to another large EHR vendor system wide. A number of different solutions were in use in other facilities and they would be making the transition as well. The implementation was to be incremental starting with major clinical applications followed by administrative applications. Usability was an issue with the previous EHR and they felt that many workflows were not easily implementable. In general the IS team felt that the applications are not always designed for fault tolerance which is dependent on the software design and architecture. Ultimately the amount of customization is dependent on the resources you want to devote. The IS team felt that the new EHR better supported customization to adapt to clinical workflows. The ambulatory care center connected to the hospital currently uses a different EHR and EHR vendors vary by facility across the system. Doctors however have access to hospital records via portal.

The IS team identified a potential risk in the way in which the new software was designed to display information and the interface used to access the information. During the implementation of their "bring your own device" policy they found that specific applications were not designed for a particular form factor. Accessing clinical information through a cell phone browser for example will affect the way in which the information is displayed which may cause vital information to be missed if the software is not specifically designed for that form factor. An extension of this problem was discovered during their implementation of the new EHR. All of the existing monitors had to be replaced with larger, higher resolution monitors because the information would not be displayed correctly.

Hospital Tour

During the tour of the hospital, the workstations with the new monitors were demonstrated for the team. Users are required to login by tapping their identification cards on a card reader every time they access the system. The login process takes seconds and any applications or records that were open during the previous user session were reopened. This means that users can login to any workstation in the hospital and pick up working where they left off. The workstations are spaced throughout the units so that a clinician can walk out of the patient's room and begin charting. It was stressed that the abovementioned features were essential in facilitating timely and accurate clinical documentation. They had tried mobile workstations on carts, but no one wanted to use them because they were cumbersome. They tried workstations in patients' rooms, but clinicians thought it interfered with their work and their ability to interact with patients.

The patient rooms are equipped with physiologic monitors that are networked to a central monitoring station. If a patient's physiologic parameter(s) trigger an alarm the monitor tech has the ability to open a video feed to the patient's room and speak to them over a video conferencing system. Additionally, the nurse on duty will receive an audible and tactile alarm notification through a mobile communication device provided by the hospital. While it would be ideal if clinicians could use their own personal devices the IT team felt that the technology was not available to support those devices because of variations in technology and potential security problems.

Safe Use of Technology
The IS team commented that financial constraints are limiting but their leadership has committed to investing in the health system's IT hardware, software, and support staff. In making technology decisions the IS team has had to weigh access to information versus the functionality of the device used to access the information. Robust support for mobile technology (i.e., apps for iOS and Android operating systems) is not yet available. Vendors are developing health IT apps which are increasingly functional and useful, but the support for the apps has not yet reached maturity. To support employee mobility and increase accessibility the health system uses a software interface for remote access.

Maturity of technology is also a limitation in meeting The Joint Commission National Patient Safety Goal (NPSG) on alarm management. The NPSG requires organizations to make improvements to ensure that alarms on medical equipment can be detected by staff. The elements of performance require organizations to assess which alarms pose the highest risk to patients if left unattended and establish policies and procedures for managing those alarms. The IS team commented that only a handful of medical device companies can handle measurement of alarms associated with the requirements of the NPSG. Other than these companies, organizations are left with putting together different systems to accomplish that goal. So far the health systems has invested approximately $2 million dollars to meet the NPSG requirements. Measurement of bed exits using bed pads results in a significant number of alarms and false alarms, but the team felt that overall the technology is not there.

The IS team provided a tour of their data center and discussed their efforts to maintain continuity of service and security. The data center is physically isolated from the rest of IS that is accessible only to technicians and staff with approved access. The data center servers are fed with a conditioned Uninterruptable Power Supply (UPS) that is supported by generator and battery backup. Server status as well as system security and integrity are constantly monitored in their secure control room. As part of their contingency planning, the IS team evaluated the current systems and their use during normal operations, but also during disasters or outages. The team stressed the need to have a contingency plan, stating "You know that the technology is going to go down and you need to know how to take care of the patient without the technology." The question they asked is if fire safety procedures are required, why not down time procedures? There is a need to assure basic competencies during down times.

The IS team commented that the SAFER guides provide a good starting point and are general enough for most users. The team found them to be straightforward but focused only on EHRs. They speculated that this may be a result of the "meaningful use" criteria as well as the consequent vendor focus. Meaningful use is what is currently driving organizations to adoption but compliance with use of the EHRs is a different matter. For example, implementing barcoding with the staff was very challenging. The IS team worked with the clinical teams to develop and implement performance measures to ensure effective use of the technology. Eventually the staff integrated barcoding into their workflow along with documentation at the point of care, but the benefits to the process had to be demonstrated.

B. Urban, not-for-profit medical center in a large metropolitan area
The project team was hosted by a large team of information technology and clinical leadership. The medical center staff included the Senior Vice President for Strategic Business Development and Performance Integration/Chief Information Officer, Senior VP Clinical Coordination, Chief Medical Officer, Chief Technology Officer, Chief Medical Information Officer, Associate Director Quality Outcomes, Associate Director Performance Excellence, Team Leader for Quality Resources, Accreditation/Patient Safety/Risk Manager, Medical Director Patient Safety, Medical Director Quality, Associate General Counsel, and Assistant Administrator for Information Management and Program Execution.

The staff provided an overview of the facilities including the medical center, the adjacent behavioral health center, and the suburban satellite medical center. The medical center is also the primary teaching hospital for a state medical school. The medical center was recently nationally recognized with an award that honors healthcare organizations that demonstrate effective and innovative approaches in using health IT.

The medical center's efforts to improve their health information infrastructure began in 2008. At that time they had a hybrid paper and electronic system which gave rise to duplicate records, but fortunately no sentinel events have occurred as a result. The system however impacted productivity and workflow.

In their implementation of their EHR, the medical center opted for the "big bang" strategy where transition from old to new electronic process occurs in one day. Clinician engagement was a recurring theme during our visit and their engagement was credited for the push to implement the EHR in the first place. Since implementing their system, training, nursing and physician support has been ongoing. The IT team, which was integrated with biomedical engineering approximately 4 or 5 years ago, holds weekly feedback sessions to continually optimize workflow and operation of the system.

Safe use of technology

A principle the medical center team has adhered to is that the higher the clinical risk, the more communication is required. The medical center team incorporated change management strategies for processes and workflows that have lasted from 1 day to 3 months, involving 4 to 100+ staff. This has facilitated rapid change and enabled greater responsiveness for improvement.

The IT staff works regularly with the patient safety staff. The teams identify and share health IT-related contributing factors to patient safety events. Another way they identify risks is through global trigger tools. When relevant, IT is part of the root cause analysis team where they help identify health IT-related contributing factors to patient safety events. Findings and recommendations are always shared amongst the team.

In addition to inpatient care, the medical center provides specialty outpatient services. Access to clinical information across the system in different settings and locations was difficult because the clinics were using a number of different EHRs. The behavioral health clinic was willing to integrate with the hospital's EHR, but other clinics were more reluctant. For them the IT team had to demonstrate sufficient audit and security processes were in place, but eventually the audit processes were withdrawn as the usefulness of an integrated IT system was demonstrated.

The team identified fragmentation of patient information as a potential risk to patient safety and described the team's efforts to implement a single patient identifier in their system to mitigate the risk. A patient for example can go to different clinics with different EHR systems resulting in two records for the same patient. The medical staff did not have all the relevant clinical information when they were treating patients. Integration of the systems was driven by the clinical need of the medical staff. It is a constant challenge linking records from different settings. They designated a full time person to monitor data integrity who usually makes approximately 10 corrections per day. In addition the organization serves a large population of Somali refugees. The birthdates for Somali refugees are all January 1st, posing a challenge to data integrity. They have had to use other identifiers including patient photos to differentiate between patients. The IT system is structured so that information feeds into their EHR and then fed to "best in breed" systems. The PACS and EKG systems now use the corporate patient identifier.

Another challenge identified by the team was the difficulty in locating relevant or high priority clinical information. In the sickle cell clinic for example the medical record is voluminous and it is difficult to find relevant clinical information. To mitigate this problem the team developed "in-pages" to pull in key vitals and lab results on a centralized screen. They also utilize a "chart search" that performs a semantic search to pull relevant clinical data on the patient. Custom in-pages were developed to focus on specific chronic diseases. The custom in-pages identify relevant labs but also identify what labs are missing. In addition to the custom in-pages, they have implemented clinical decision support, and use trending that focuses on maintaining patients' health.

C. Large, Academic Medical Center

The project team was hosted by a large contingent of IT professionals and clinicians that included the CMIO, CNIO, Associate CMIO for Ambulatory settings, Associate CMIO for ED, Patient Safety Manager, Director of Accreditation and Regulatory Readiness, Director of the Cancer Center, Nurse Coordinator for the Medical Procedures Unit (ambulatory), Associate Director for Care Management, a Pediatric Gastroenterologist, Pharmacists, and clinician researchers from the Nursing Informatics and Health Services Research. In addition to the medical center team we had the opportunity to talk with the CMIO of a large local physicians group that participates in the Health Information Exchange with the academic medical center.

At the time of our visit, the medical center was preparing to transition from a primarily internally developed EHR to a large commercial EHR for inpatient systems. The health system in addition to the CMIO, has 7 associate CMIOs championing this effort. The medical center has had 10 to 12 years of experience using an assortment of commercial and internally developed EHRs before making the transition.

Cancer Center

The Director of the Cancer Center explained that in the past they used pre-printed order sets that are imaged for communication and storage into the medical center's internally developed inpatient system. They are in the midst of transitioning to an oncology specific module of the new EHR but still utilize parts of the legacy system. They use software for labs for example, that were visible in the legacy system but not visible in the new EHR. Currently there is no content manager between old lab viewer and the new EHR. In addition people like the old system's lab view better.

The internally developed inpatient system uses a separate software for billing OR procedures. The ambulatory care module of the new EHR provides more functionality, but they feel it is more difficult to get the "patient story." The current chemo order process does not use CPOE. They have standardized order sets that are scanned. The doctor fills out the order set from the web, it is printed, and then scanned into the inpatient system. Pharmacy/infusion can view the order. There are multiple places to check the order, and modifications are difficult because they are layered on top of the scanned order. The infusion RN double check is the last process step for patient protection.

As a result there are many calls back to clinic by the infusion RN, with approximately one near miss reported per month. A multi-disciplinary patient safety committee reviews the reports. The cancer center has their own CMIO who also supports these efforts.

To date 1,400 protocols have been built in to the CPOE system. The protocols force process standardization. Doctors however want to be able to dictate and have someone transcribe the orders. The legacy system was more complimentary to this workflow, so the new EHR implementation is sometimes a challenge and some doctors "have not embraced the system, yet." The oncology tie to lab data is critical for chemo orders necessitating special focus that differs from other ambulatory settings.

Decision support for oncology is especially complex. Pediatric patients will add another degree of difficulty. National oncology standards are referenced and built in but they still have difficulty standardizing.

Currently they are in the fourth of six integrated testing cycles with the new EHR. User acceptance testing occurs with RNs, physicians, and assistants. They realized the necessity of change impact assessments when they were implementing bar coding medication administration. There was 11 hours of downtime to implement the change, then 8 hours of downtime to change back. They are currently testing workflow using tabletop simulations and dress rehearsals after training. The ideal situation would be to perform a simulation and demonstrate competency putting back orders into the system using test patients.

During the two week go-live period existing treatment plans will be difficult to manage. Different levels of superusers will be available for "at the elbow support" to take questions. For the go-live 77 ambulatory champions and 88 in-patient champions have been identified. The superusers are doctors and mid-level

providers who will have no clinical duty at that time and will perform huddles at the end of the day. The physician champions assist with workflow and operational leads from IT have also been identified to assist.

One unique aspect of oncology at the medical center is that there are both clinical and research protocols. Research protocols require IRB approval before building the order sets which adds more complexity to the process of implementation. Implementation of these protocols will be challenging in light of the upcoming transition.

Students are a special consideration. Only an attending can sign an order for chemotherapy. Medical students can enter the order but not sign indicating different levels of security and privileges by user. Security and privileges are not only granted by role but also by certification and/or policy.

In oncology there are a higher proportion of part time clinicians which changes the management dynamic. A research oncologist may be using a midlevel nurse practitioner as a scribe for the oncology software. Pharmacists have a unique role in oncology, much akin to an air traffic controller. In other services, research is usually a separate team but this is not so for oncology.

Pharmacy

The pharmacists described challenges associated with the use of different systems in different settings. It is especially difficult when patients are similar because it becomes difficult to differentiate them. For them admission is the highest risk point. To reduce the risk of medication errors they pre-populate order sets for certain settings. When possible they use pictures of patients to assist in identification. Receiving medication orders from external providers via paper, fax, and/or verbal orders is a process that is still somewhat reliant on paper.

The alert system they use is pharmacy specific. The alerting for drug-drug interactions took several hours for the team to work through. The timing of the alert is essential to the clinical relevance of the alert. They have found that forcing the clinician to "Acknowledge and proceed" leads to cancellation of the order. In order to determine effectiveness of the alert, they measure the rate of alerts for a short time to ensure the alert causes the intended behavior.

Pediatric gastroenterologist

A pediatric gastroenterologist was asked by the CMIO to talk to the project team about risks associated with the transition to the new EHR. Full dictation was used for charting with old system. With the new EHR, he feels that there is too much time spent typing and that this interferes with his connection with patients. This interruption of workflow inhibits his ability to obtain a full clinical picture of the patient, taking away from time spent with the patient. Changes in workflow will increase the risk for a patient safety event. Additionally, with greater reliance on technology he finds that some clinicians don't remember patient details because it is part of the patient’s data in the EHR. He feels that critical thinking skills are diminished because of an overreliance on technology.

For pediatric gastroenterologists there are system performance issues because patient records are data dense. Slow refresh rates switching between pages impacts workflow and productivity. The current, internally developed organ transplant information system is not only used for charting but also patient education and creating letters to a patient's family practice physician. For organ transplants they are required to submit data to maintain their certification with the United Network for Organ Sharing (UNOS), a private, non-profit organization that manages the U.S. organ transplant system. The UNOS data submission process will be more difficult with the new EHR. In their practice the pediatric gastroenterologists also handle infusions which makes the patient history all the more important. The adult standard for infusion is not appropriate for pediatrics. In the new oncology module nurses cannot set up the orders for non-oncology infusion. Pediatric gastroenterology patients have multiple clinicians with asynchronous visits, but the software unfortunately does not currently support this type of visit.

Overall, many of the current customizations are difficult to accomplish with the new EHR. The new EHR does not have the same level of functionality. In the pediatric gastroenterologist's opinion is "not ready for prime time" and it will take years to bring the new system up to the same level of functionality.

Associate CMIO for ambulatory settings

The Associate CMIO for Ambulatory settings is an Obstetrician whose responsibilities also include management of the patient portal. The Associate CMIO feels that there is currently too much information in the electronic record and it is difficult to locate relevant patient information. It has also been difficult to determine where the patient data goes. If the data is dumped in one place, it will lead to usability problems and information overload. Mapping elements to procedures and surgery lists can create clutter, contributing to "note bloat". All pathology results went into her inbox for example, but the team could not program the logic to prioritize the results in the new EHR. Any output from outpatient clinics went into physicians' inboxes. Complicating matters is the fact that inpatient doctors currently don't have inboxes on the same system.

Patient access to data has been challenging to manage. They release all test results to the patient portal after 24 hours for inpatients. For outpatients there is a delay of 3 to 4 days for blood work. The physician may not see the test results before the patient has access to them via the portal. To mitigate this risk they have implemented time frames for releasing results: pathology or text based results, about 2 weeks; HIV, 30 days; and genetic tests, 90 days. If however a test result is inadvertently marked as reviewed it will be released to the patient. The ideal is that physicians will review and release test results, but the test results will auto release after the time limit. The risk is that a patient could be notified prematurely via portal before talking to their physician.

Patients have the option to send messages to their physicians, but patients are advised that this function is only for non-urgent communication. Patients are also advised that the messages will become part of their medical record. Since the activation of the patient portal, there has been an increase in the number of requests for medical record release and correction. If the new EHR has a centralizing capability for different patient portals, it can reasonably feed into the medical record. For adolescent patients (12 to 18 years old) privacy from patient's parents becomes an issue. These patients can be granted their own account at the provider's discretion.

Charting on the wrong patient record was identified as a potential safety risk. Health information management has an entire team for merging and unmerging data in patient records. They struggled with finding the right number, but they currently limit users to having 3 patient charts open at one time.

Ambulatory care unit

The Nurse Coordinator hosted the team visit to the ambulatory care unit. There are currently a number of different systems in use in the clinic, providing an example of the challenges integrating different systems and the clinical workflows necessary to accommodate the systems. In addition to the new EHR for clinical documentation, they use a separate system for labeling, tracking scopes, and images. Anesthesiology uses a completely different EHR.

The ambulatory care unit currently uses the legacy system to view and store endoscope images which currently has 130 variations including muscle biopsies. They perform time outs before every procedure and in the current system there is a cue to perform the time out. In addition there are prompts for two patient identifiers to prevent wrong patient errors.

Order entry and the scheduler for outpatient is on the new EHR system. Inpatient orders are entered and a hard copy will be printed out in prep area, then inputted into the new EHR system scheduling module. The new system has the visit types and orders in a drop down list in addition to a section for comments. An IT help desk ticket is necessary to add to visit types.

Updates from the legacy system are pushed to new EHR system on the hour. The legacy system nursing notes however do not get pushed to the new system until they are signed off. There are email and paper

alerts to sign off on notes but the process is not automated. If a physician wants to make amendments to the legacy system notes, they have to make a request first. Changes are limited factual changes, otherwise they are added as an addendum.

Abnormal results are not automatically flagged, but they do have the ability to query text. The group observed that with fax notification to an office someone in the office is designated to pick it up and triage the notification. Contrast this to an email to a group, where no one is designated responsible for viewing and acting on the notification. Another issue that was discussed was the importance of maintaining the centrality of the problem list. A task made more difficult with their current system.

Private practice provider group

The independent, not-for-profit, multi-specialty, private practice provider group composed of over 40 clinics works closely with the medical center on efforts related to Health Information Exchange (HIE) and Accountable Care Organizations. The provider group currently uses a different EHR than the medical center. The provider group CMIO commented that the HIE is currently not as integrated as they would like. About 250 providers from the group have read only access to medical center system. For lab results, they currently interface with two different health systems and a large commercial laboratory service provider. Their EHR system interfaces with the labs, and labs come back in usable data electronically. The key to safety is the two way interface to external labs. It is possible however to segment an order and miss lab data. For example a lab request was sent out, and only 19 out of 20 lab results came back. The missing lab result was critical.

The provider group CMIO characterized the risks he deals with in this way: "It's not what we know; it's what we don't know." For example after their last system update, providers completed entering a protocol and everything entered got wiped out unbeknownst to the provider. People started to see pattern when they noticed information was missing. Another example was the implementation of their patient portal. The provider group patient portal currently serves over 110,000 patients. The system couldn't handle that number at first. They now perform load testing to assure that the patients have access to their data.

Unfortunately, there is no formal network of providers that reports problems. Compounding problems is the fact that there are organizational silos that impede communication and sharing. The LIS is administered by the lab pathology informatics team at the medical center, but they do not report to informatics. Anesthesiology, radiology, and other departments have separate informatics groups.

The provider group is currently trying to integrate 70 providers from another group but they are using a different version of their current system. The HL7 CDA is available for standardization and sharing but they are not using it. Lab and x-ray results can be shared, but the emergency department (ED) record has been difficult. The ED record does not get transmitted until the attending physician signs off, but the ambulatory physician does not receive relevant clinical information in a timely manner. In response, the provider group has created an overarching policy that providers have up to 30 days to sign. In implementing this policy they were trying to strike the balance between sending complete results versus results that could be changed.

Nursing informatics and health services research

The team from Nursing Informatics and Health Services Research discussed their usage of electronic clinical data for research and measurement. In looking through the data they sought the ability to quantify a “dose of RN intervention.” They found it difficult to look for patterns or trends, however, using different search terms for pulling information out of record. The medical terminology is extremely variable making the records problematic to analyze.

In studying interoperability, they consider “thoughtflow, workflow, and process flow.” Complicating their effort is the fact device features are developing faster than our ability to understand. Nurses use multiple systems for documentation, different devices (e.g., monitors, ventilators, infusion pumps), and ultimately have to validate the accuracy of the clinical information. Order reconciliation has to be performed frequently but is especially problematic at transitions. It is difficult to determine when the last medication

was given in the electronic medication administration record (eMAR). The challenge is how to view the data, because the physician view of the data may differ from that of the nurse.

Other issues that the team discussed in general were that "Documentation does not substitute for communication," "BID" (abbreviation for an order for administration of medication or treatment twice a day) does not translate electronically past 9 PM, and that provider group specific order sets and the ability to save favorites are becoming unmanageable. An ongoing structure and governance is necessary to ensure that these problems are addressed from a multidisciplinary perspective.

Associate director for care management
A nurse and social worker are primarily responsible for coordinating the admission process, ensuring patient flow and appropriate transfers. The Associate Director observed that there are multiple processes for doing the same thing depending on the department. The ED EMR differs because care management is for the first 24 hours. Medicine and surgery have different processes for ordering. The technology can be configured to do things one way through policy, but there are risks, efficiency can be affected, and the potential tradeoffs need to be considered. The governance issues can be untenable.

There was an incident where verbal orders were received, but when the patient arrived relevant clinical information was not readily available to treat the patient. They struggle to obtain relevant clinical information from the sometimes massive amounts of patient information transferred from other facilities. If they are unable to determine if a patient already exists in the system a new medical record number is created and then the records are later merged to existing records if present.

A separate system is used for discharge documentation. The documentation is uploaded into their current system, but no one can view the documentation until it is uploaded. A print out of the medical record can be provided at discharge but a printed EMR is not easy to read. The current discharge summary is functional but other parts of the summary are not as useful in print format.

D. Veterans Affairs Medical Center
The project team was hosted by the medical center's Clinical Informatics staff which includes the Clinical Coordinator for Hospital Informatics, Clinical Application Coordinator, Automated Data Processing and Application Coordinator as well as the medical center's Patient Safety Manager. The project team was joined by representatives from the Veterans Health Administration (VHA) and the local Veterans Integrated Service Network (VISN). During the initial discussion a theme that was voiced at the academic medical center visit was repeated: "Documentation does not replace communication."

Echocardiogram techs
The team first visited the Echocardiogram (Echo) Technicians in the Echo Lab. The staff do not always have much control over the interaction between medical device vendor systems and their own IT. Vendor interfaces vary. The Computerized Patient Record System (CPRS) is their CPOE interface to the Vista (Veterans Health Information Systems and Technology Architecture) EHR. Only cardiologists can see images which are made available to them through Vista imaging PACs. The Echo technicians use the medical device vendor software for image management.

Imaging orders are transmitted from Scheduling to Clinical Procedures to the work list on the vendor software. The techs print the order and the order appears on CPRS. Comment fields appear in their inbox of alerts, which can have many alerts. If the techs discover incorrect information in the order they call Clinical Informatics. They also have hard stops built into their processes, where the techs will not proceed until they receive clarification from the ordering providers on orders.

The tech discussed some of the health IT related issues they encounter. Scheduling to Clinical Procedures glitches can cause delays. The vendor software operates on a PC with an older version of the Microsoft Windows operating system and they are waiting for an update that will operate on the newest version of Windows. The software can be "glitchy," so they run audit reports in CPRS to make sure they

don't miss any orders or images. The vendor software is isolated from the medical center system architecture and has to be updated separately.

Some of the risks they see in using the software are related to incorrect data selection and duplicate records. Clinician types are included in orders but it is still possible to make incorrect selections. Duplicates usually get caught and are usually detected under the reason provided for the order. The techs and Clinical Informatics staff are always reachable to mitigate these risks quickly once they are identified.

Another potential risk the team discussed was the need to assure adequate screen resolution for imaging. This becomes especially important as telemedicine becomes more widespread. Smaller VAs that do not have the resources, will work with larger VAs but if the resolution is inadequate the image will not be useful for clinical decision making.

Clinical informatics

The Automated Data Processing Application Coordinator and Clinical Application Coordinator described their roles as part of the informatics team. The Clinical Informatics staff facilitates the integration of clinical processes, information technology, medical equipment, and patient safety. They sit on nursing committees to ensure clinical integration with IT. The Clinical Informatics staff have training in patient safety and maintain good communications among the departments and functional units despite the silos that exist within the VA system.

The medical center IT reports to the "big VA" (i.e., Department of Veterans Affairs) and not the VHA. Since the VA was one of the first large health systems to implement EHRs system wide they have long ago experienced initial implementation issues and are now working with a mature system. Issues of the computer in between clinicians interrupting workflow are still there but they have developed ways around it since IT implementation began in the VAs around 1998 to 2000.

To ensure usage, the VA issued a directive that 95% of orders must be entered in the CPOE by the provider with exceptions for dialysis and chemotherapy. They described a specific issue they uncovered with the CPOE system where an order was sometimes completed but not found in the server. The team discovered that this can happen when users open multiple instances CPRS.

The Clinical Informatics team monitors for problems using the existing technology. Since barcode medication administration (BCMA) is integrated with CPRS, the team reviews the scanning failures report to identify issues. The informatics team created the report to pinpoint medication barcodes that are problematic. The report can be used to identify issues from the national level to the clinical level. Reports can be uploaded from other facilities but it can slow down or crash the computer due to volume of data. They realized that this can be problematic for transferring images of large file size so they tag the image with the date of change and the study date.

The electronic signing process for some vendor specific software sometimes does not require authentication before entry into CPRS. The problem then is knowing whether or not the user is a clinician. Signatures are required on CPRS but this process is facility specific. The informatics team works with clinical services, billing and administration, to develop health records management, security, and governance processes.

There are several system to system interfaces which allow data from specific medical devices to be available in the records. If the data is not currently in the record then the specific service component can be interrogated and the report can be pulled into Vista imaging. In order to accomplish this there are several different servers such as those that support different clinical devices, medical device vendor software, or Vista imaging. The problem is that no one person can access all the servers and it is therefore difficult to determine if an interface is down.

The team discussed the lab results and notification of critical values and findings. There are differences in the information a clinician sees versus laboratorians due to College of American Pathologists lab accreditation requirements. For critical test results clinicians can see which tests are pending and will call to see why the results are not appearing in the system. However for truly critical results clinicians will wait with the tech to ensure immediate receipt of the results. STAT (e.g., immediate) testing has a separate, specific policy. The EHR shows the status of the test results such as when the test results are there, not there, or in process. They differentiate also between critical findings versus critical values notifications. Examples are notifications for a new HIV positive test result compared to an abnormally high lab value, respectively. Over time the expectations for notification of providers at home have changed. Responding to notifications now counts as hours working for hospitalists and intensivists, which has facilitated responsiveness.

Planned downtimes are challenging because the team not only has to make sure Vista comes back up, but also other systems' gateway (the interface to the ordering system). Due to the siloed nature of health IT in the VA, the IT staff does not know when the gateway goes down. IT helpline calls are centralized nationally but can be triaged incorrectly. The end user sometimes has to troubleshoot locally so a 24 hour call tree has been instituted by the informatics team.

Providers at the VA have access to external organization patient information through various portals. Vistaweb connects to the EHRs of VAs across the country. VA providers have access to the affiliated academic medical center through a separate system.

Biomedical engineering

A potential risk and challenge the Biomedical Engineering team identified was data access and security. Organizational separation between Veterans Health Administration (VHA) and Department of Veterans Affairs (VA), and thus the division of units within the medical center, makes assuring security complex. Department of Homeland Security regulations restrict federal networks access so much so that providers need a background check for user IDs. Care is provided for active military at VA facilities so this information is shared with the Department of Defense. Telehealth is credentialed for each VISN, but a separate login is required for each system.

Protection of patient information has also been an issue. Medical devices and associated software have USB ports, and were being used to transfer images. This could not only lead to unintended disclosures of patient information, but also potentially spread computer viruses. To prevent this, Biomedical Engineering has had to implement port controls on these devices. Another example is with Echo machines. The patient information has to be wiped before going to the vendor for service, or they have to remove the hard drive altogether.

The team recounted an occasion when a vendor update to the EKG system was made at the end of the week which resulted in no EKG results being displayed for any user over the weekend. Biomedical engineering was not available, the vendor had already left, and it took some time to identify the issue. There was no validation, the change was made, and then no one was available the next day to troubleshoot. This lead to the requirement that the process flow be developed and risks identified before implementation of changes. The process flow is intended to be a fluid document that should be updated regularly. Additionally, the vendor Memorandum of Understanding (MOU) should specify responsibilities for testing and support.

Safe use of technology

The team discussed a well-publicized health IT safety issue that was discovered by a nurse at the medical center. The nurse discovered a glitch in CPRS that resulted in incorrect doses of medication and delayed treatments. The nurse immediately reported it to Clinical Informatics and resources were rapidly mobilized to address the problem.

A number of health IT-related safety events were discussed such as a report in the wrong patient's chart and a patient receiving the wrong wrist band for identification. They utilize a combination of common

health IT safety tools and clinical processes to prevent medication errors, such as CDS, CPOE, and patient identification double checks. They have found however that there can be some over-reliance on CDS.

Cutting and pasting of patient information is a common problem. There are instances where copying national templates like the Braden scale for pressure sore risk is appropriate. Copy and paste is an issue that will have downstream effects. It is a conflict between balancing clinical duty and administrative tasks.

Communication is good internally but it has been sometimes difficult to work with vendors. Smaller vendors are easier to work with because they have more flexibility. Larger vendors do not have as much incentive to make changes and can be costly to the medical center when changes or customization are required. The patient safety program recognizes health IT as a tool to improve safety, but it must be supported by strong communication and culture.

Access to workstations and refresh rate of screens drive workflow. Clinicians receive consult update alerts, clinical alerts, and scheduling alerts raising the potential for alert fatigue. From VA to VA medical center, however, notification process flow will differ. Assigning surrogates may result in different notification settings.

In purchasing software and equipment there needs to be consideration not only at initial purchase but also for sustainability and ongoing support. The catheterization lab for example without internet access, could not access online “guard rails” (software updates for safe operation). They therefore decided against elective procedures until the problem was fixed. In granting access to systems, privacy, security, and safety must be in balance.

III. Findings and Conclusion

A. Investigating Health IT-related Sentinel Events

The Joint Commission's analysis of health IT-related sentinel events suggests that risks and hazards associated with health IT are uncovered through a comprehensive systematic analysis such as a root cause analysis of an adverse event. As previously described, when accredited organizations report a sentinel event they use a Root Cause Analysis Framework[26] to ensure that the organization has addressed the active failures and latent conditions associated with the sentinel event. The responses to these questions are typically uncovered during the course of the organization's root cause analysis and are included in the sentinel event report to The Joint Commission. During the analysis of sentinel events, review of responses to the following Framework questions, while not all directly related to health IT, helped to identify whether or not health IT contributed to the event.

- What was the intended process flow?
- Were there any steps in the process that did not occur as intended?
- What human factors were relevant to the outcome?
- How did the equipment performance affect the outcome?
- Did staff performance during the event meet expectations?
- To what degree was all the necessary information available when needed? Accurate? Complete? Unambiguous?
- To what degree was the communication among participants adequate for this situation?
- Was available technology used as intended?
- How might technology be introduced or redesigned to reduce risk in the future?

Health IT as a contributing factor in this analysis was a latent condition that may not be readily apparent when the event occurred. Using Reason's oft-cited Swiss cheese analogy, health IT as a contributing factor to a sentinel event is a vulnerability represented by a hole in one of the layers of Swiss cheese furthest away from the patient.[2] This also means that when health IT is functioning optimally, the vulnerability is mitigated and health IT may help prevent patient harm.

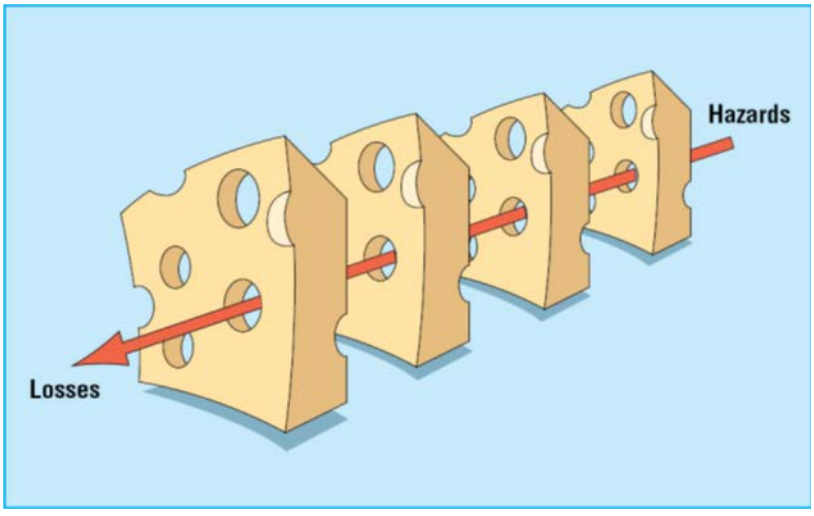

Figure 4. Reason's Swiss Cheese Model

Since the responses to framework questions were not overly technical in their descriptions, it is likely that clinical staff performed the investigation and analysis. Additionally, the responses suggest that IT, clinical informatics, or biomedical engineering staff were not involved nor was there any indication of vendor support. This could explain the lack of identification of events related to system to system interfaces, such

as CPOE to EHR or EHR to bar code scanner for example, identified in other analyses of health IT-related events.[28,30,32]

These findings suggest that when investigating and analyzing sentinel events, the analysis team can identify the role of health IT as a potential contributing factor by using the abovementioned Root Cause Analysis Framework questions. Once health IT is identified as a potential contributing factor the organization's IT, clinical informatics, or biomedical engineering staff should be involved in the analysis to help uncover specifically how the technology could have contributed to the event i.e., human-computer interface design, system to system interactions, or software configuration issues, in the context of the existing clinical workflows.

Since health IT as a contributing factor was usually identified as a vulnerability or latent factor, rather than a more direct or immediate cause of harm, recognition and reporting health IT-related hazards necessitates staff "situational awareness."[3] Recognition involves not only identification of health IT-related hazards but also recognition of the potential patient harm that could result if the hazard is not mitigated. This can only be successful in an organization with a strong patient safety infrastructure characterized by a culture of safety where hazards and close calls ("near misses") are routinely reported, process improvement is comprehensive and systematic, and leadership acts upon the identified issues in a timely manner.[4-6] Proactive risk assessments, such as Failure Mode and Effects Analysis and the ONC Safety Assurance Factors for EHR Resilience (SAFER) Guides,[7] should be integrated into a strong patient safety infrastructure in order to identify health IT-related hazards before harm reaches the patient.

B. Learning Visits

The Joint Commission's learning visits to medical centers found that interdisciplinary collaboration among IT professionals, clinical staff, biomedical engineering, and patient safety staff, supported by strong leadership commitment to health IT as a way to improve patient safety, were common factors for successful implementation and safe use of health IT. In each medical center, staff demonstrated sensitivity to the connection between health IT-related hazards and the potential for patient safety events. This is not surprising considering all of the participating medical centers could be characterized as having mature, well-functioning health IT systems and supporting organizational infrastructure.

Despite their focused efforts, the medical centers faced several similar challenges associated with the design and use of health IT. Specifically, several individuals commented that, depending on how the health IT system is designed and implemented, relevant clinical information can be difficult to find. This can contribute to "loss of clinical context" and difficulties following the clinical care of patients. Health IT as a barrier to communication among clinicians and with patients also emerged as a common theme, with one interviewee observing, "documentation is not communication." Overall, each of the participating medical centers struggled with how health IT changes clinical workflows and with finding the best ways to safely and efficiently integrate health IT systems into those workflows.

The medical centers, like most, struggle with problems associated with technology. However, the medical centers we visited had empowered, knowledgeable staff who work collaboratively to find ways to balance clinical workflow, cross organizational silos, and alleviate technology limitations. They also used technology to monitor for hazards and safety issues. In each of the medical centers, the organizational leadership recognized that safe technology and safe use of technology are priorities.

C. Role of External Organizations

Private and federal safety organizations that aggregate and analyze patient safety event reports such as The Joint Commission, Patient Safety Organizations (PSOs), or the VA National Center for Patient Safety play an important role in enhancing health IT safety. They can collect adverse event reports while maintaining privacy and confidentiality protections. Aggregation and analysis of patient safety event reports facilitates identification of risks and hazards that may not be readily apparent to an individual healthcare organization. Safety organizations also assist healthcare organizations in their adverse event investigations and analyses by helping them probe into health IT-related latent conditions and associated workflows. Reports on health IT-related hazards (properly de-identified) and learning tools produced by

safety organizations can be shared and can serve as valuable educational resources.[8-11] An individual healthcare organizations' ability to utilize these external resources however is dependent on the strength of its patient safety infrastructure.[4-6]

The current aggregation and analysis by safety organizations provide valuable information for reducing the risk of health IT-related events but are limited by the scope of the reports that each respective organization receives. As previously described, the definition for "reviewable sentinel event" is specific and does not focus on health IT-related sentinel events. Sentinel events refers to a subset of all PSEs that have either led to death or serious permanent harm to the patient or are one of the specific types of events listed in the Sentinel Event Policy. By virtue of this definition, information-rich events such as near misses, events that reached the patient but did not cause harm, or hazardous situations are excluded. In contrast many PSOs collect all types of PSEs. Furthermore safety concerns reported to the Informatics Patient Safety Office of the Veterans Health Administration also includes all types of PSEs but are focused specifically on health IT.[32]

The Joint Commission's analysis of sentinel events suggests that organizations' investigation of sentinel events does not include a detailed characterization of health IT-related contributing factors. External safety organizations can investigate the event, and there are Joint Commission and PSO options for doing so,[25,33] but the organizations who select this option consent to the external assistance and accept the costs that are incurred. Organizations that seek external investigation assistance however are the minority. Reasons for this include commitment of organizational resources, including staff time and money, state laws which may limit what can be shared with external organizations, concerns over potential liability, as well as perception that such investigations are punitive.

This punitive perception was evident in the lack of participation in The Joint Commission's offer for free on-site investigations of health IT-related sentinel events. The Joint Commission's sentinel event review process is separate from the accreditation process. None of the information obtained through the review process is used in the accreditation assessment. Despite these assurances, accredited healthcare organizations often perceive that there would be potential negative implications on their accreditation status. Therefore, the learning visit format was used in lieu of on-site investigations of health IT-related sentinel events. This would suggest that investigations of health IT-related patient safety events by an independent Federal entity may also be perceived as punitive. The punitive perception undermines safety culture and leads to less organizational willingness to share findings or worse, a reluctance to disclose a health IT-related patient safety event.

However, health IT safety and the broader goal of using health IT to continuously improve patient safety requires more than collaboration **within** healthcare organizations. Collaboration on health IT and patient safety should also occur nationally, as part of a learning collaborative, where stakeholders contribute knowledge, evidence, research, and expertise, and learn from each other. Clinicians and patients, who rely upon the safety of health IT (as designed, implemented, and maintained by others), should be engaged as well.

The Joint Commission agrees with the recommendation made in the draft FDASIA Health IT Report (April 2014), to create and support an environment of learning and continual improvement related to health IT and patient safety. One means of doing so proposed in the draft FDASIA report was a Health IT Safety Center, as a public-private entity to serve as "a trusted convener of health IT stakeholders in order to focus on activities that promote health IT as an integral part of patient safety..." Whether through a federally funded Health IT Safety Center, or some other means, the Joint Commission supports the need for collaboration at a national level on health IT safety as part of a learning collaborative.

LITERATURE CITED

1. Agency for Healthcare Research and Quality. AHRQ common formats - version 1.2: Event descriptions, sample reports, and forms. https://www.psoppc.org/web/patientsafety/version-1.2_documents#Supply. Updated 2013. Accessed December 5, 2013.

2. Reason J. Human error: Models and management. *BMJ*. 2000;320(7237):768-770.

3. Weick KE, Sutcliffe KM. Managing the unexpected : Resilient performance in an age of uncertainty. 2nd ed. San Francisco: Jossey-Bass; 2007.

4. Chassin MR, Loeb JM. The ongoing quality improvement journey: Next stop, high reliability. *Health Aff (Millwood)*. 2011;30(4):559-568. doi: 10.1377/hlthaff.2011.0076 [doi].

5. Chassin MR, Loeb JM. High-reliability health care: Getting there from here. *Milbank Q*. 2013;91(3):459-490. doi: 10.1111/1468-0009.12023 [doi].

6. The Joint Commission. Patient safety systems chapter for the hospital program. http://www.jointcommission.org/patient_safety_systems_chapter_for_the_hospital_program/. Updated 2014. Accessed 10/17, 2014.

7. Office of the National Coordinator for Health Information Technology. SAFER guides. http://www.healthit.gov/safer/. Accessed 11/21, 2014.

8. The Joint Commission. 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/. Updated 2008. Accessed 3/1, 2015.

9. ECRI Institute PSO. ECRI institute PSO deep dive: Health information technology. 2012.

10. ECRI Institute. 2015 top 10 health technology hazards. https://www.ecri.org/Pages/2015-Hazards.aspx. Updated 2014. Accessed 12/1, 2014.

11. The Joint Commission. Safe health IT saves lives. http://www.jointcommission.org/safehealthit. Updated 2015. Accessed 3/1, 2015.

12. Runciman W, Hibbert P, Thomson R, Van Der Schaaf T, Sherman H, Lewalle P. Towards an international classification for patient safety: Key concepts and terms. *Int J Qual Health Care*. 2009;21(1):18-26. doi: 10.1093/intqhc/mzn057 [doi].

13. Thomson R, Lewalle P, Sherman H, Hibbert P, Runciman W, Castro G. Towards an international classification for patient safety: A delphi survey. *Int J Qual Health Care*. 2009;21(1):9-17. doi: 10.1093/intqhc/mzn055 [doi].

14. World Alliance for Patient Safety Drafting Group, Sherman H, Castro G, et al. Towards an international classification for patient safety: The conceptual framework. *Int J Qual Health Care*. 2009;21(1):2-8. doi: 10.1093/intqhc/mzn054 [doi].

15. World Health Organization, Alliance for Patient Safety, ed. International classification for patient safety (v.1.0) for use in field testing 2009; 2008.

16. Committee on Patient Safety and Health Information Technology, Institute of Medicine. *Health IT and patient safety: Building safer systems for better care.* Washington (DC): National Academy of Sciences; 2011. NBK189661 [bookaccession].

17. Sittig DF, Singh H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *Qual Saf Health Care*. 2010;19 Suppl 3:i68-74. doi: 10.1136/qshc.2010.042085 [doi].

18. Carayon P, Schoofs Hundt A, Karsh BT, et al. Work system design for patient safety: The SEIPS model. *Qual Saf Health Care*. 2006;15 Suppl 1:i50-8. doi: 15/suppl_1/i50 [pii].

19. Harrison MI, Henriksen K, Hughes RG. Improving the health care work environment: A sociotechnical systems approach. *Jt Comm J Qual Patient Saf*. 2007;33(11 Suppl):3-6, 1.

20. Hripcsak G. Monitoring the monitor: Automated statistical tracking of a clinical event monitor. *Comput Biomed Res*. 1993;26(5):449-466. doi: S0010480983710323 [pii].

21. Henriksen K, Kaye R, Morisseau D. Industrial ergonomic factors in the radiation oncology therapy environment. In: Nielsen R, Jorgensen K, eds. *Advances in industrial ergonomics and safety.* ; 1993:325--335.

22. Rector AL. Clinical terminology: Why is it so hard? *Methods Inf Med*. 1999;38(4-5):239-252. doi: 10.1267/METH99040239 [doi].

23. Vincent C, Taylor-Adams S, Stanhope N. Framework for analysing risk and safety in clinical medicine. *BMJ*. 1998;316(7138):1154-1157.

24. The Joint Commission. *2014 hospital accreditation standards.* Oakbrook Terrace, IL.: Joint Commission Resources; 2014.

25. The Joint Commission. Sentinel event policy and procedures. http://www.jointcommission.org/Sentinel_Event_Policy_and_Procedures/. Updated 2014. Accessed 11/19, 2014.

26. The Joint Commission. Framework for conducting a root cause analysis and action plan. http://www.jointcommission.org/assets/1/6/RCA_Questions_Framework.docx. Updated 2013. Accessed 6/8, 2014.

27. Health insurance portability and accountability act of 1996. *PL No 104-191*. 1996;42 U.S.C.:§ 1320d-9.

28. Sparnon E, Marella W. The role of the electronic health record in patient safety events. *Pa Patient Saf Advis*. 2012;9(4):113-121.

29. Walker J, Hassol A, Bradshaw B, Rezaee M. Health IT hazard manager beta-test: Final report. (prepared by ABT Associates and Geisinger Health System, under contract no. HHSA290200600011i, #14). Vol AHRQ Publication No. 12-0058-EF. Rockville, MD: Agency for Healthcare Research and Quality; May 2012. http://healthit.ahrq.gov/sites/default/files/docs/citation/HealthITHazardManagerFinalReport.pdf.

30. Magrabi F, Ong MS, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. *J Am Med Inform Assoc*. 2012;19(1):45-53. doi: 10.1136/amiajnl-2011-000369 [doi].

31. Castro G. Classification of health information technology-related contributing factors to patient safety events. [PhD, Doctor of Philosophy]. University of Illinois at Chicago; 2014.

32. Meeks DW, Smith MW, Taylor L, Sittig DF, Scott JM, Singh H. An analysis of electronic health record-related patient safety concerns. *J Am Med Inform Assoc*. 2014. doi: amiajnl-2013-002578 [pii].

33. ECRI Institute. Accident investigation services. https://www.ecri.org/Accident_Investigation/Pages/default.aspx. Updated 2015. Accessed 3/1, 2015.