# Classification of Health Information Technology-Related Contributing Factors to Patient Safety Events

BY

GERARD MICHAEL CASTRO
BS, Loyola University at Chicago, 1996
MPH, University of Illinois at Chicago, 2004

THESIS

Submitted as partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Public Health Sciences
in the Graduate College of the
University of Illinois at Chicago, 2014

Chicago, Illinois

Defense Committee:

Ross Mullner, Chair and Advisor
Richard Croteau, Joint Commission International
Edward Mensah
Paul Schyve, The Joint Commission
Annette Valenta

This thesis is dedicated to my boys, Joseph and Gabriel.

## ACKNOWLEDGEMENTS

This study was made possible through a sole source contract (Solicitation number: 13-233-SOL-00270) 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. Without her this research would not have been possible.

I would like to thank my thesis committee—Drs. Ross Mullner, Richard Croteau, Edward Mensah, Paul Schyve, and Annette Valenta—for their guidance. Each a subject matter expert in their own right, they brought invaluable, unique knowledge to their contributions. I am grateful for their mentorship.

I am also indebted to my current and former colleagues at The Joint Commission. Lisa Buczkowski and Joanne Hafner provided me their clinical insight during the qualitative data analysis of the Sentinel Events. My dear friend Dr. Heather Sherman reviewed drafts, provided vital input, and continues to give me her unwavering support. Finally, the late Dr. Jerod Loeb, who gave me my start in patient safety research; I will always remember his feisty personality, deep knowledge of quality and patient safety, and his commitment to both his family at home and The Joint Commission.

## TABLE OF CONTENTS

## TABLE OF CONTENTS (continued)

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| AHRQ | Agency for Healthcare Research and Quality |
| ARRA | American Recovery and Reinvestment Act |
| CDS | Clinical Decision Support System |
| CPOE | Computerized Provider Order Entry |
| EHR | Electronic Health Record |
| e-MAR | Electronic Medication Administration Record |
| EMR | Electronic Medical Record |
| FDA | Food and Drug Administration |
| HITECH | Health Information Technology for Economic and Clinical Health |
| ICPS | International Classification for Patient Safety |
| IOM | Institute of Medicine |
| IT | Information Technology |
| LIS | Laboratory Information System |
| MAUDE | FDA Manufacturer and User Facility Device Experience |
| MDR | Medical Device Report |
| ONC | Office of the National Coordinator for Health Information Technology |
| PA-SRS | Pennsylvania Patient Safety Reporting System |
| PACS | Picture Archiving and Communications System |
| PSE | Patient Safety Event |
| PSO | Patient Safety Organization |
| RCA | Root Cause Analysis |
| WHO | World Health Organization |

## SUMMARY

The purpose of this study is to develop a classification for health information technology (health IT) contributing factors that can be used to identify, understand, and eventually reduce the risk of health IT-related patient safety events (PSEs). Much has already been written on the specific components of health IT and each component's potential relationship to patient safety, but the focus of this study is to describe how health IT can increase the risk for patient harm in the context of a dynamic sociotechnical system. A model describing the dimensions of the health IT sociotechnical system will be used as the framework for describing health IT-related factors that contribute to adverse events in healthcare. The classification using the sociotechnical model will then be tested using PSE data to identify associated contributing factors and unsafe conditions that can increase the risk for patient harm.

An analysis of 120 health IT-related sentinel events resulted in the identification of more than 300 contributing factors that are classified into 50 different types of contributing factors from a possible 77 contributing factors in the classification. Health IT-related contributing factors were identified in eight sociotechnical dimensions with no identified contributing factors falling outside the dimensions. This suggests that the sociotechnical model is sufficient for capturing relevant health IT-related contributing factors.

# I. INTRODUCTION

## A. Background

Health information technology (health IT) is playing an increasingly vital role in providing safer and better care to patients. Specifically, the technology is used to electronically capture, transfer, display, or store patient health information for use by clinicians, payers, insurers, regulators, patients, and the healthcare organizations to improve the quality and safety of care provided. Technology also facilitates the analysis of patient data individually and in aggregate for quality measurement, learning, and improvement. Health IT devices and systems can automate paper-based processes, electronically transfer test results to clinicians at the point of care, imbed safety functions such as dose checking or notification to clinicians of potential allergic reactions, facilitate communication with patients, and allow patients' access to parts of their medical records via the Internet. Accurate, accessible, and timely clinical information helps improve healthcare quality. Implementation of new technology also requires healthcare organizations to redesign and streamline old paper-based processes.

To access health IT's potential benefits, the US government enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act through the American Recovery and Reinvestment Act (ARRA) of 2009 (Classen et al., 2010; Office of the National Coordinator for Health Information Technology, 2009a; Payne et al., 2013). The Medicare and Medicaid Electronic Health Records (EHR) Incentives Program provides incentive payments to individual providers (physicians), hospitals, and critical access hospitals for "meaningful use" of certified EHR technology to improve

patient care (Centers for Medicare and Medicaid Services, 2014). The Centers for Medicare and Medicaid Services are charged with managing these incentive payments. The criteria for “meaningful use” are being implemented incrementally with increasing requirements from 2011 to 2015. Since its inception, the incentive program has been a driving force in the adoption of health IT. The aggressive timelines for adoption, however, may not allow for adequate customization of EHR systems to align with host organization clinical workflows (Singh, Classen, & Sittig, 2011). Safe design, implementation, and use of health IT is necessary to achieve the technology’s full benefits. Absent these criteria the health IT system can operate in unintended and unanticipated ways, contributing to adverse events that result in patient harm or death (Committee on Patient Safety and Health Information Technology & Institute of Medicine, 2011).

From a patient’s perspective, health IT can be any medical electronic device in a healthcare setting. This includes a hospital heart rate monitor, intravenous smart pump, or the EHR that the physician uses to document patient information. This represents the broadest and perhaps the most widely understood conceptualization of “health IT.” However, as defined in the Institute of Medicine (IOM) 2011 report *Health IT and Patient Safety: Building Safer Systems for Better Care*, health IT includes “a broad range of products, including EHR's, patient engagement tools (e.g., personal health records and secure patient portals) and health information exchanges; excluded is software for medical devices” (Committee on Patient Safety and Health Information Technology & Institute of Medicine, 2011). The exclusion of “software for medical devices” differentiates the broad, patient-centric concept of health IT from definitions created for

regulatory purposes. This exclusion is due to the definition of “device” as specified by federal statute and, consequently, the interpretation of the statute shaping US federal government oversight. Different government agencies have oversight over various components of health IT and have defined the components according to their regulatory responsibilities. The disparate nature of this oversight and differing definitions by which each agency defines the components, however, has contributed to a siloed approach to managing the safety of these devices. Oversight for health IT and medical devices is divided amongst different agencies within the Department of Health and Human Services. These responsibilities are shared by the Food and Drug Administration (FDA), the Office of the National Coordinator for Health Information Technology (ONC), and the Agency for Healthcare Research and Quality (AHRQ).

The FDA has an established infrastructure for medical device manufacturer reporting through the Manufacturer and User Facility Device Experience (MAUDE) reporting system. The FDA “receives several hundred thousand medical device reports (MDRs) of suspected device-associated deaths, serious injuries, and malfunctions. The MDRs [are used] to monitor device performance, detect potential device-related safety issues, and contribute to benefit-risk assessments of these products. The MAUDE database houses MDRs submitted to the FDA by mandatory reporters (manufacturers, importers, and device user facilities) and voluntary reporters (e.g., healthcare professionals, patients, and consumers)” (Food and Drug Administration, 2014b).

Section 201(h) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. § 321[h]), specifies that a “device” is “. . . an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any

component, part, or accessory", that is ". . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man . . ." or ". . . intended to affect the structure or any function of the body of man or other animals. . . " The terms "device" and "medical device" are used interchangeably, but any product that meets the above definition is subject to regulation by the FDA. This includes any software application or mobile medical applications that meet the abovementioned criteria.

The ONC has responsibility for overseeing the Medicare and Medicaid EHR Incentive Programs and establishing the criteria for "meaningful use" of EHR technology to improve patient care. The program provides incentive payments to clinicians, hospitals, and critical access hospitals to purchase or replace an EHR system. The criteria for "meaningful use" are a set of objectives that are currently being implemented in stages (Centers for Medicare and Medicaid Services, 2014).

The ONC defines an EHR as a digital version of a patient's paper chart: "EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users" (Office of the National Coordinator for Health Information Technology, 2009b, para. 1). The ONC specifies that EHRs must be able to (Office of the National Coordinator for Health Information Technology, 2009b, para. 1):

- Contain a patient's medical history, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results;
- Allow access to evidence-based tools that providers can use to make decisions about a patient's care; and
- Automate and streamline provider workflow.

The Patient Safety and Quality Improvement Act of 2005 authorized the creation of Patient Safety Organizations (PSOs) and the Common Formats for reporting of

PSEs. The Common Formats are intended to provide a standardized format for healthcare providers to collect and report PSEs within their organization or to external organizations such as PSOs or state agencies. Similar to the IOM definition of health IT, the AHRQ Common Formats definition limits the scope of health IT by excluding software in medical devices and equipment; it is the FDA that has oversight responsibility for medical devices.

The AHRQ “Common Formats for Device or Medical/Surgical Supply, including Health Information Technology” provides a more detailed definition of health IT giving examples of specific technologies (Agency for Healthcare Research and Quality, 2013). The Common Formats define health IT as follows: A health IT device includes hardware or software that is used to electronically create, maintain, analyze, store, or receive information to aid in the diagnosis, cure, mitigation, treatment, or prevention of disease and that is not an integral part of (1) an implantable device, or (2) an item of medical equipment. Health IT consists of a wide array of technologies including:

- Administrative/billing or practice management systems;
- Automated dispensing systems;
- Electronic health records or component of EHRs, including computerized provider order entry (CPOE) systems, pharmacy systems, electronic medication administration records (e-MAR), clinical documentation systems (e.g., progress notes), clinical decision support (CDS) system;
- Human interface devices (e.g., keyboards, mouse, touchscreens, speech recognition systems, monitors/displays, printers);
- Laboratory information systems (LIS), including microbiology and pathology systems; and
- Radiology/diagnostic imaging systems, including picture archiving and communications system (PACS)

The definitions of health IT and its components continue to evolve as the boundaries between health IT and medical devices become blurred. Smart pumps, physiologic monitors, and bar-code scanners are only a few examples of the devices

that are increasingly integrated with the health information systems. Within most healthcare organizations, health IT and medical devices are siloed in different departments, usually IT and biomedical engineering departments, respectively. From the perspective of the everyday clinical or administrative user, the difference is lost. Understanding how health IT, its components, and medical devices are defined, managed, and integrated, however, is necessary for a well-functioning system. Integration of these devices can increase the efficiency and accuracy of patient information available to clinicians, improving the quality of healthcare provided to the patient.

## B. **Statement of the Problem**

Health IT-related PSEs do not occur in isolation, but in the context of a sociotechnical system that includes technology, people, processes, organizations, and the external environment (Committee on Patient Safety and Health Information Technology & Institute of Medicine, 2011). This system includes all components of health IT and medical devices as well as external forces such as government regulations, incentives, and oversight. Evaluating health IT in the context of a sociotechnical model facilitates understanding of the interplay between the components and the effect of changes in the system. 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; however, when health IT design is inadequate, implemented haphazardly, or

used inappropriately, it can add a layer of complexity to an already complex system, which can lead to PSEs (Committee on Patient Safety and Health Information Technology & Institute of Medicine, 2011).

## C. Purpose of the Study

The purpose of this study is to develop a classification for health IT contributing factors that can be used to identify, understand, and eventually reduce the risk of health IT-related PSEs. Much has already been written on the specific components of health IT and each component's potential relationship to patient safety, but the focus of this study is to describe how health IT can increase the risk for patient harm in the context of a dynamic sociotechnical system. A model describing the dimensions of the health IT sociotechnical system will be used as the framework for describing health IT-related factors that contribute to adverse events in healthcare. The classification using the sociotechnical model will then be tested using PSE data to identify associated contributing factors and unsafe conditions that can increase the risk for patient harm.

## D. Significance of the Problem

While seamless integration of health IT and medical devices is the ultimate goal for healthcare organizations, the current state is hindered by limited compatibility between various technologies. Different devices interfacing with different systems across different settings add to the complexity inherent in modern healthcare. How these technologies and devices are designed and implemented will affect the clinical workflow and vice versa. Health IT has the potential to lead to increased cognitive

workload, alert fatigue, frustration, and ineffective communication, causing users to revert back to paper-based workflows (hybrid), workarounds, and wasted time (Ash et al., 2007). These alterations can lead to unintended consequences such as medication errors, wrong procedures, or delays in treatment that can ultimately lead to patient harm or death.

## E. **Significance of the Study**

A more comprehensive understanding of how health IT can lead to patient harm, impact workflow, and improve safety is needed (Committee on Patient Safety and Health Information Technology & Institute of Medicine, 2011). The potential benefits of health IT are often described, but understanding how health IT can cause harm to patients is less well understood and described. These incidents are typically evaluated on a case-by-case basis, focusing on specific components of health IT such as such as e-MARs or CPOEs (Committee on Patient Safety and Health Information Technology & Institute of Medicine, 2011).

# II. Conceptual Framework and Related Literature

## A. Conceptual Framework

### 1. Defining patient safety

The three prominent definitions of “patient safety” come from the IOM, the AHRQ, and the World Health Organization (WHO). In its 2004 report *Patient Safety: Achieving a New Standard for Care*, the IOM defines patient safety as “the prevention of harm to patients” (Aspden, Corrigan, Wolcott, & Erickson, 2004). This definition is simple, but too broad. In this definition neither the preventable outcome “harm” nor process for preventing it are defined. On its Patient Safety Network Web site, AHRQ defines patient safety as the “freedom from accidental or preventable injuries produced by medical care” (Agency for Healthcare Research and Quality, [n.d.], para. 1). This definition expands the concept of harm by including accidental and preventable injuries, offers a more precise preventable outcome, and is explicit about the process “medical care.”

The WHO in its International Classification for Patient Safety (ICPS) defines patient safety as “the reduction of risk of unnecessary harm associated with healthcare to an acceptable minimum. An acceptable minimum refers to the collective notions of given current knowledge, resources available, and the context in which care was delivered weighed against the risk of non-treatment or other treatment” (World Health Organization, Alliance for Patient Safety, 2008, p. 15). The ICPS definition of patient safety is similar to the AHRQ definition for patient safety in that both the preventable

outcome “unnecessary harm” and the process “healthcare” are specified; however, the ICPS definition is unique because it includes the critical concept risk.

Risk is a measure of the probability and severity of adverse effects (Haimes, 2009). Safety in the context of patient care is the reduction of risk of unnecessary harm to an acceptable minimum (World Health Organization, Alliance for Patient Safety, 2008). In differentiating risk and safety, the key terms to note are “reduction of risk . . . to an acceptable minimum.” Measuring risk is an empirical, quantitative activity in the measurement of the probability and severity of harm, whereas measuring safety requires determining the acceptability of risks, which is a normative, qualitative, and sometimes political activity (Haimes, 2009).

Definitions of PSEs differ widely. The definition of 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 don’t (Runciman et al., 2009; Thomson et al., 2009; World Alliance for Patient Safety Drafting Group et al., 2009). Patient safety events are circumstances that could have resulted, or did result, in unnecessary harm to a patient (World Health Organization, Alliance for Patient Safety, 2008). 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.

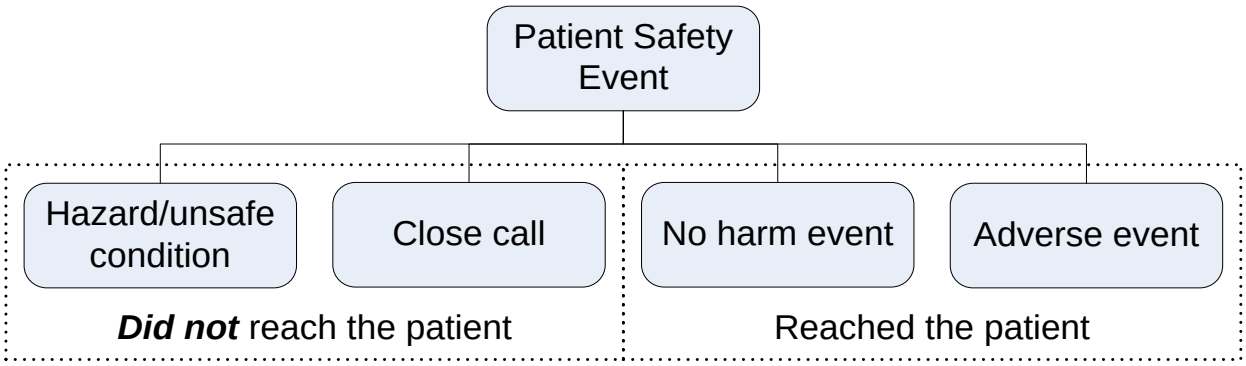



Figure 1. Types of patient safety event.

The distinguishing factor between close calls and adverse events is whether or not the event reached the patient. As an example, if a nurse while 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. Both 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 (RCA), 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.

Lack of a common language for describing and communicating PSEs led the WHO to commission the development of the ICPS (World Alliance for Patient Safety Drafting Group et al., 2009; World Health Organization, Alliance for Patient Safety, 2008). The ICPS provides a conceptual framework with 10 high-level classes organized relationally for understanding elements and processes involved in PSEs. The high-level classes include: Contributing Factors/Hazards, Incident Type, Incident Characteristics, Patient Characteristics, Detection, Mitigating Factors, Patient Outcomes, Organizational Outcomes, Ameliorating Actions, and Actions Taken to Reduce Risk (see Figure 8, Appendix A). Each high-level class has several associated concepts organized hierarchically in subclasses. Health IT in the ICPS can be considered a subclass of "Contributing Factor/Hazard" to a PSE and/or an "Incident Type." "Depending on the context, circumstances, and outcomes, an incident can be a contributing factor to another incident and/or some contributing factors can be . . . [incidents] in their own right" (World Alliance for Patient Safety Drafting Group et al., 2009, p. 5).

The classes Detection, Mitigating Factors, Ameliorating Actions, and Actions Taken to Reduce Risk describe elements and processes associated with system resilience or the healthcare organization's ability to prevent events from either reaching the patient or from causing harm to the patient. One component of system resilience (i.e., protective of patient safety) is an effective surveillance system used for detecting and learning from the incidents. Effective surveillance, however, requires not only a reporting system but also engaged healthcare staff involved in detecting and reporting

PSEs. Engaging hospital staff requires sharing findings to facilitate the development of actions to reduce risk and a culture where social and professional norms facilitate these behaviors (Anderson, Ramanujam, Hensel, Anderson, & Sirio, 2006; Chassin & Loeb, 2011; Chassin & Loeb, 2013; Gandhi, Graydon-Baker, Huber, Whittemore, & Gustafson, 2005).

2. **Investigating and analyzing patient safety events**

Formal investigation and analysis of PSEs in healthcare is usually performed through the RCA process. The concept for RCA originated from engineering, and was introduced to healthcare by The Joint Commission and the Department of Veterans Affairs, Veterans Health Administration National Center for Patient Safety in the 1990s. The purpose of the RCA is to answer three basic questions: "What happened, why did it happen, and what can be done to prevent it from happening again?" The intent of an RCA is to determine the causal and contributing factors to a PSE in order to develop interventions to prevent future occurrences of events that result in patient harm. According to the Veterans Health Administration Patient Safety Handbook, RCAs have the following characteristics (US Department of Veterans Affairs & Veterans Health Administration, 2011):

1. The review is interdisciplinary in nature with involvement of those knowledgeable about the processes involved in the event.
2. The analysis focuses primarily on systems and processes rather than individual performance.
3. The analysis digs deeper by asking "what" and "why" until all aspects of the process are reviewed and the contributing factors are considered.
4. The analysis identifies changes that could be made in systems and processes through either redesign or development of new processes, and systems that would improve performance and reduce the risk of the adverse event or close call recurrence.

Patient safety event analyses, in general, are composed of phases: investigation, analysis, and corrective actions. The investigation phase is to gather facts and information. During the analysis phase, the information from the investigation phase is used to identify contributing and causal factors associated with the incident. Once the analysis phase is complete, corrective actions are identified, implemented, and measured to determine if the corrective actions were effective.

The basic steps of the investigation phase are not unlike the process used in a police investigation (B&W Pantex—U.S. Department of Energy, 2008). Once an incident is detected, individuals responsible for the investigation secure evidence and preserve the scene of the incident. In healthcare, evidence can include health records, medical supplies, or medications. Relevant policies and procedures and review of the relevant literature may also be included in the investigation. The environmental factors and conditions that could have contributed to the event are documented and can be supplemented by photos and videos. Interviews with the individuals directly and indirectly involved in the incident or process are necessary to begin developing a timeline of the event. These interviews can include the patient and his/her family.

During the analysis phase many different quality improvement and management tools can be applied, such as process flow charts, fault tree analyses, or fishbone (also called Ishikawa or cause and effect) diagrams. In general, the tools use data that are gathered from the investigation phase, organize the data, and assist the incident analysis team in identifying contributing and causal factors that will help in the selection of corrective actions. Contributing factors are those circumstances or conditions that set

the stage or facilitate the occurrence of an adverse event. Causal factors if corrected or eliminated will likely prevent an adverse event.

3. **Reason's Swiss cheese model**

Reason's Swiss cheese model is a prevalent model of system accidents not only in medicine, but also in the nuclear industry and aviation (Reason, 1990; Reason, 2000a; Reason, 1997; Reason, 2000b). Contributing factors to an event in Reason's model are characterized as either active failures or latent conditions. Active failures are unsafe acts committed by the people directly in contact with the system or equipment failures. Active failures occur at the "sharp" end of the system, which in the case of a PSE is proximal to the patient. These can be failure to confirm the name, dose, and route of a medication prior to administering it to a patient (i.e., medication double-check) or failure to perform a "time out" to confirm the patient's identity, procedure, and laterality of the procedure prior to surgery. The medication double-check or "time out" prior to surgery is the final defense or protective slice of Swiss cheese before the event reaches the patient in a medication error or wrong-site surgery, respectively. But like a slice of Swiss cheese, these defenses are imperfect and active failures can slip through unnoticed. The more slices, the less chance of something slipping through.

Figure 2 represents the trajectory of a PSE or accident as it travels through holes in defenses or safeguards represented by slices of Swiss cheese. For any safety event or accident that results in harm, the holes through the barriers are in alignment. This is the only time a safety event can occur. Defenses or safeguards can be facility design, automatic systems, policies, processes, and optimizing interfaces to accommodate for

human factors. Automated medication dispensing systems, CPOE, and CDS are examples of health IT that act as safeguards to prevent medication errors. The model depicts a snapshot of a period of time when the event or accident occurs. In real time the model would be dynamic, the defenses may shift in position, and the holes in defenses open and close.

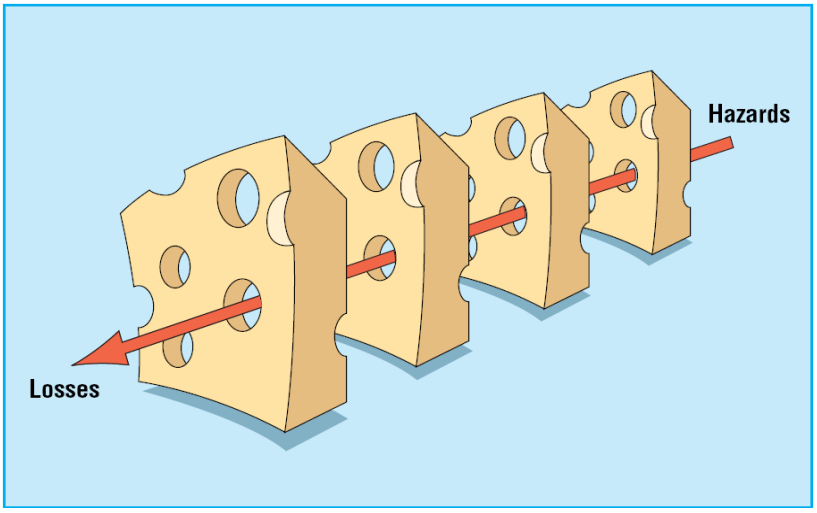



Figure 2. Reason's Swiss cheese model.

Latent conditions are so-called "resident pathogens" in the system that arise from system design, leadership, or organizational culture. These conditions occur at the "blunt" end of the system. Latent conditions can include inadequate processes, poor workstation design, insufficient training, hazardous work environment, unsuitable tools, unsupportive management, or lack of safety culture.

## 4. Sociotechnical model for health information technology

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. Models can help decide what to study, identify measures of effectiveness, and identify conditions that promote or block effectiveness (Harrison, 2005). They help users to identify what to focus on (such as areas or components that have been problematic in the past); to identify what areas require better definition; and to evaluate potential interactions and changes between different components. The sociotechnical system helps researchers and practitioners focus on the critical characteristics of the work environment and the interactions among clinicians, administration, staff, and patients (Harrison, Henriksen, & Hughes, 2007). The end result is a model that is tailored to the specific users and applications.

Sociotechnical system models emerged from the application of management theory to the study of factory workers. The term “sociotechnical” originated from Trist and Bamforth from the Tavistock Institute of Human Relations in London (Cummings & Srivastva, 1977). They studied the impact of a change to the social system at the Glacier Metal Works in the 1950s and found that changes in the social system without the corresponding changes in the technological system limited the success of those changes and, ultimately, limited the effect on the organization as a whole.

Cummings and Srivastva (1977, p. 1) argue that in order to understand and manage work, it should be described in the context of the work environment and

people's interactions with each other and with technology: "The management of work is concerned with how people structure their relationship to technology for productive achievement." They argue that this perspective offers two distinct advantages over other management theories. First, the model views the social and technological aspects of work as a system in which people relate to technology for task performance. The second aspect of the model is that it is open to the environment, meaning that the social system and the technological system are susceptible to and can be affected by internal forces and by forces from outside the organization. When there is a poor fit among the interdependent components or functions, effectiveness of the system is reduced, leading to poor outcomes (Harrison, 2005).

The social system refers to a relationship between people who interact with each other in a given environment for the basic purpose of achieving an agreed-upon task or goal (Cummings & Srivastva, 1977). The technological system is composed of the tools, techniques, and methods employed for task performance. The technological system is dependent on the social system for creation and operation, meaning people make and operate the technology, making people responsible for the outcome. The technological system operates only as a reaction to the behavior of the social system. Harrison characterizes the components of the model as follows (Harrison, 2005):

- Inputs—raw materials, money, people, equipment, knowledge;
- Outputs—products, services, outcomes. Productivity and performance measures examine the quantity and quality of the outputs. Outputs can be subjective outcomes as well;
- Organizational behavior and processes—prevailing patterns of interaction between individuals and groups that may contribute directly or indirectly to transforming inputs into outputs;
- Technology—tools, equipment, and techniques used to process inputs, and transform them into outputs;
- Environment—the close (task) environment, which includes external organizations and conditions that are directly related to the system's transformative processes and technologies;
- Structure—enduring relations between individuals, groups, and larger units, including role assignments (such as job descriptions), divisions, departments, policies. Emergent structural patterns (e.g., informal cliques, coalitions) can differ substantially from officially mandated ones. Structure constrains and focuses behavior without determining it;
- Culture—shared norms, values, beliefs, assumptions including associated artifacts and behaviors; and
- System dynamics—major changes in any system component during recent and more distant past.

Applying the sociotechnical system model to healthcare, Harrison et al. (2007) highlights its unique components. In addition to the social and technical components, there are regulatory forces such as government, accreditors, or professional societies, payers, markets, suppliers, science, and culture. Model outcomes include quality of healthcare for patients; behavioral outcomes such as caregiver health, stress, or well-being; and organizational outcomes such as cost, efficiency, and financial performance.

When applied to health IT, the sociotechnical system model offers a more detailed depiction of the dynamics involved between the technology, people, and environment. Sittig and Singh (2010) offer a model that specifically addresses the design, development, implementation, use, and evaluation of health IT. In creating their model they adapt components of other related sociotechnical models (Carayon et al., 2006; Harrison, Koppel, & Bar-Lev, 2007; Henriksen, Kaye, & Morisseau, 1993;

Hripcsak, 1993; Rector, 1999; Vincent, Taylor-Adams, & Stanhope, 1998), and further delineate 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 (Figure 3):

- 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; 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.

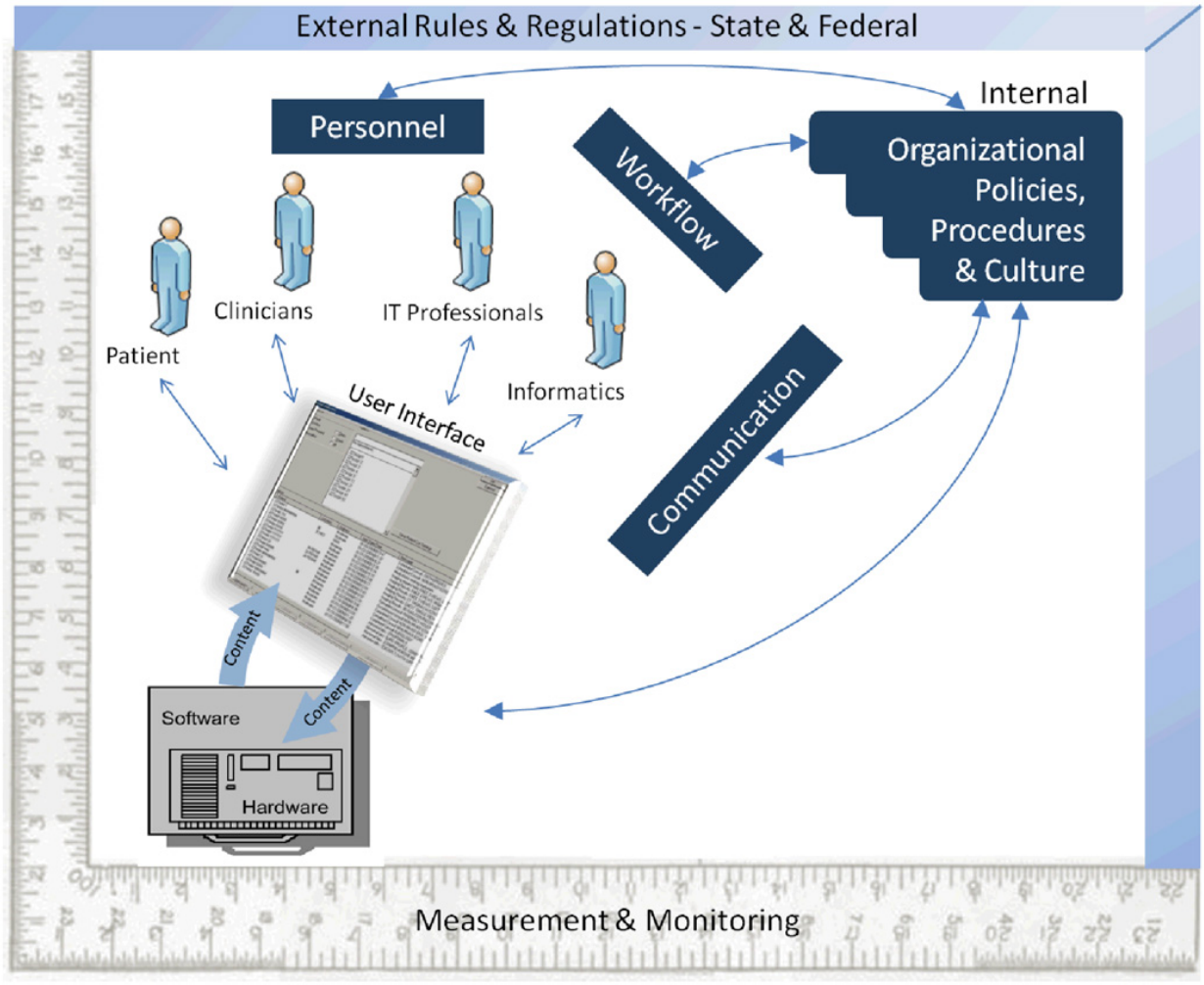



Figure 3. Sociotechnical model for health IT.

Examining health IT incidents within the context of the sociotechnical model enables individuals and organizations to look beyond the incident to understand it in the context of the people who use the system and the other technologies and processes affected by health IT.

## 5. Justification for this project

In response to the recommendations of the IOM's report *Health IT and Patient Safety: Building Safer Systems for Better Care*, the ONC drafted its Health IT Patient Safety Action and Surveillance Plan that summarizes the US Department of Health and Human Services patient safety activities as they relate to health IT (Office of the National Coordinator for Health Information Technology, 2014). The plan has two objectives: (1) promote the healthcare industry's use of health IT to make care safer, and (2) continuously improve the safety of health IT. The first objective focuses on the use of health IT to prevent adverse events and unsafe conditions through systems such as clinical decision support to warn providers of drug allergies. The second objective relates to preventing adverse events and unsafe conditions that are caused by or related to health IT.

To achieve these objectives, Singh and colleagues (2011) proposed the creation of a national EHR oversight program dedicated to the surveillance of identified EHR-related errors, hazards, close calls, and adverse events. The authors proposed a national, independent oversight body to ensure the safety of EHRs, similar in goal, charge and organization to National Transportation Safety Board for transportation safety. Reporting and then classifying EHR-related events in this manner is an essential component of learning how to safely implement and use health IT systems; reporting and classification enable aggregation and analysis of EHR-related event data, which facilitate the development of preventive strategies.

## B. **Review of Related Literature**

Unfortunately, there are a number of challenges. Relatively few studies have focused on health IT-related events in large PSE databases. While preparing its 2011 report on health IT, the IOM found little published evidence quantifying the types of risk associated with health IT (Chuo & Hicks, 2008; Joint Commission on Accreditation of Healthcare Organizations, USA, 2008; Magrabi, Ong, Runciman, & Coiera, 2010; Myers, Jones, & Sittig, 2011; Santell, Kowiatek, Weber, Hicks, & Sirio, 2009; Walsh et al., 2006; Zhan, Hicks, Blanchette, Keyes, & Cousins, 2006). Magrabi et al. (2010) examined 899,768 reports submitted to the FDA MAUDE database between 2008 and 2010 and only uncovered 436 health IT-related events. Analysis of the 436 events revealed 712 problems, of which 682 (96%) were machine-related and 30 (4%) were problems at the human-computer interface. Almost half (46%) of the events were related to hazards or unsafe conditions, with 46 events (11%) leading to patient harm. Four deaths were linked to health IT problems (0.9%). The authors used these findings to expand on their existing health IT classification, adding four new categories to describe problems with software functionality, system configuration, interface with devices, and network configuration.

The ECRI Institute PSO reviewed 171 health IT-related events submitted by 36 healthcare facilities over a nine-week period and identified the following problems: inadequate data transfer from one health IT system to another; data entry in the wrong patient record; incorrect data entry in the patient record; failure of the health IT system to function as intended; and configuration of the system that can lead to mistakes (ECRI Institute PSO, 2012). The majority of the reported events (61%, 105 events) were

classified as incidents that reached the patient. The remaining events were close calls (23%, 39 events) that did not reach the patient and unsafe conditions (16%, 27 events). The reports identified issues with a number of health IT systems including CPOE systems, clinical documentation systems, eMAR, laboratory information systems, pharmacy systems, human interface devices, radiology/diagnostic imaging systems (including PACS), automated dispensing systems, and clinical decision support systems. Using Magrabi's taxonomy (2010), the ECRI Institute PSO identified the top five health IT-related safety issues as system interface issues, wrong input, software issue-system configuration, wrong-record retrieval, and software issue-functionality.

The Pennsylvania Patient Safety Authority queried the Pennsylvania Patient Safety Reporting System (PA-SRS) for EHR-related PSEs using keywords such as "EMR," or "EHR," with EHR vendor names (Sparnon & Marella, 2012). The query resulted in 8,003 reports from June 2, 2004 to May 18, 2012. Using a combination of manual review and automated event recognition, 3,099 reports were confirmed as relevant to EHRs. The great majority of these reports resulted in no harm (89% or 2,763), with a smaller number characterized as unsafe conditions (10% or 320). The remaining events (<1%) resulted in temporary harm (15 reports), and one report was of significant harm to the patient. The investigators found that the "vast majority of reported events (81%) involved medication errors—mostly wrong-drug, -dose, -time, -patient, or -route errors (50%) or omitted dose (10%). The only other event type with a significant number of reports was complications of procedures, treatments, or tests (13%)—most of which involved lab test errors (7%)" (Sparnon & Marella, 2012). Similar to the ECRI Institute PSO study, Sparnon used Magrabi's taxonomy to identify safety issues. The

top five safety issues identified were wrong input, failure to update data, software issue-system configuration, output device down or unavailable, and output/display error.

Meeks et al. (2014) performed an analysis of 100 EHR-related safety concerns reported to the Informatics Patient Safety Office of the Veterans Health Administration. The Informatics Patient Safety Office maintains a voluntary reporting system of health IT-related safety concerns that includes all types of PSEs (i.e., adverse events, no-harm events, close calls, and hazards). Reports are investigated and analyzed by Informatics Patient Safety analysts. The researchers qualitatively analyzed the reports' narrative data and categorized the concerns by phases of safety related to EHR implementation and use: unsafe technology or technology failures (phase 1); unsafe or inappropriate use of technology (phase 2); and lack of using technology to monitor for potential safety concerns (phase 3) (Sittig & Singh, 2012). The concerns were also classified using the dimensions of Sittig and Singh's (2010) sociotechnical model. Approximately three-quarters of safety concerns were categorized as related to unsafe technology or technology failures (phase 1), with the remaining quarter classified as unsafe use of EHR (phase 2). The phase 1 concerns most commonly involved the sociotechnical dimensions hardware and software, workflow and communication, and clinical content. The phase 2 concerns commonly involved the dimensions people, clinical content, workflow and communication, and human-computer interface. They found that 94% of the safety concerns fell into four broad types: unmet display needs, problems with software modifications or upgrades, concerns related to system-system interfaces, and hidden dependencies within the EHR.

The examples above demonstrate the need to continue to work toward Singh's proposed system for health IT surveillance (Singh et al., 2011) and to enhance Magrabi's taxonomy. Analyzing a PSE using the WHO ICPS conceptual framework (World Health Organization, Alliance for Patient Safety, 2008) as a model for improving patient safety helps to describe the event characteristics in a standard format and facilitates the understanding of the relationship between the different classes. Organizations implement “actions to reduce risk” to the corresponding “contributing factors” that are identified through reporting and/or analysis. Study of individual incidents can help uncover dysfunctional processes, organizational vulnerabilities, or behaviors that undermine safety culture. However, when information on individual incidents is aggregated, systematic organizational vulnerabilities can be uncovered that would not have been discovered at the individual level. Aggregate or cluster event analysis are applied where certain events appear to have common characteristics, in order to identify patterns of performance and system vulnerabilities (Leotsakos et al., 2014). Systematic analysis of what happened in the individual incident and learning from trends and patterns associated with the incidents in aggregate help to identify actions and interventions to reduce the risk of similar incidents occurring. Learning from incident reports is not only essential for preventing incidents from reoccurring, but also for determining where to focus future improvement efforts.

The dimensions of Sittig and Singh’s sociotechnical model are compatible with the ICPS, expanding ICPS subclasses for health IT-related contributing factors. Current classifications of health IT-related PSEs are insufficient because they are focused on specific categories of health IT (i.e., EHR, medical devices, computer interfaces) and do

not relate to some of the sociotechnical aspects of health IT. Accurately describing the contributing and causal factors that contribute to the risk of a health IT-related PSE will improve identification of the specific aspects of the health IT system that requires improvement. Patterns and characteristics can be discerned for these factors from studying health IT-related PSEs in aggregate. The contribution of health IT to PSEs can also be better defined.

# III. Methods

## A. Design

The methodology chosen to develop this classification consists of queries of a PSE database, followed by content and confirmatory analysis of the results. This approach was used to develop the WHO ICPS (Runciman et al., 2009; Thomson et al., 2009; World Alliance for Patient Safety Drafting Group et al., 2009) and by Magrabi et al. (2010; Magrabi, Ong, Runciman, & Coiera, 2012), Sparnon and Marella (2012), and Meeks (2014). Thus, it has been validated through saturation (multiple studies) and verification (multiple users) for use in this manner.

For this study, a sample of sentinel events reported to The Joint Commission was used in a two-step process: (1) database queries, and (2) content analysis of the full sentinel event incident reports. The results of the content analysis were then used by the investigator to perform a confirmatory analysis on a composite health IT classification of contributing factors. As each sentinel event report is composed of categorical and narrative data, analysis of the sentinel event data in this way identifies both the health IT-related factors that are currently captured and what other health IT-related factors need to be captured. The end result is a more robust classification that enables the accurate description of the adverse event as well as the contributing and causal factors related to health IT to (1) inform and influence organizational actions taken to reduce risk, and (2) help prioritize resources.

## B. Sample

De-identified data from sentinel events reported to The Joint Commission by accredited organizations from January 1, 2010 to June 30, 2013, (n=3,375) were used in the analysis. 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 patient safety incidents 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' RCAs. 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) RCA.

### 1. Overview of The Joint Commission Sentinel Event Policy

The Joint Commission defines a sentinel event as an unexpected occurrence involving death or serious physical or psychological injury, or risk thereof (The Joint Commission, 2014a). 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 an RCA of each event meeting this definition. In

contrast, events that are reviewable by The Joint Commission, so-called “reviewable sentinel events,” are a subset of sentinel events that healthcare organizations are strongly encouraged to voluntarily report to The Joint Commission as part of the sentinel event reporting program. A reviewable sentinel event is defined as 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 healthcare 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); and
- 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 are events in the event types specifically 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 (The Joint Commission, 2014a). This results in a mix of voluntary and mandatory reported events. This distinction has important ramifications for the project that will be described in the Limitations section.

Approximately 1,000 sentinel events are reported annually to The Joint Commission. 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. A focused site visit by specially trained surveyors is another rarely used option, but since it is officially treated as an accreditation survey findings are not included in the sentinel event database. For all of these mechanisms, a Joint Commission "Patient Safety Specialist" (minimally, a master's prepared nurse) works with the organization, reviews the organization's RCA, assures that the analysis meets the criteria for being "thorough and credible," and abstracts information from the organization's RCA for entry into the sentinel event database. Identifying information on the patient, provider, and organization are not included or removed before entry into the database. Information gleaned from the sentinel event database is used for alerts and prioritization of risk reduction strategies.

Notably, there are self-reporting accredited healthcare organizations in each of the 50 states, regardless of whether their state mandates reporting to a state agency. Approximately two-thirds of events in The Joint Commission database have been self-reported by the organization that experienced the event. In addition to the media and patients or families reporting events to The Joint Commission, reports of sentinel events may come from employees and medical staff of healthcare organizations, other healthcare organizations, social service agencies, government agencies, and Joint Commission surveyors who happen upon such information during survey activity.

While some organizations, by their own policy, choose to self-report all reviewable events, other organizations determine whether or not to voluntarily report events on a case-by-case basis. As an example, if the organization recognizes that it is likely the event will receive wide media coverage or thinks it likely that the family will contact The Joint Commission about the event, they will pro-actively self-report even if by their own policy they do not typically report voluntarily.

A Root Cause Analysis Framework (The Joint Commission, 2013) (Appendix B) is used to ensure that the organization has addressed the active failures and latent conditions (Reason, 2000b) associated with the sentinel event. The RCA Framework consists of 24 questions 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 ("RCA question responses").

After the sentinel event data are submitted by the organization and reviewed by the Patient Safety Specialist, he/she categorizes the event and summarizes the event in a narrative “Synopsis.” The sentinel event is categorized by “Sentinel event type” (e.g., wrong person procedure, anesthesia event resulting in death, fall resulting in permanent loss of function), causative and contributing factors or “Root cause category” (e.g., communication, human factors, patient monitoring), clinical service, and clinical setting. The sentinel event incident report typically also includes the organization’s narrative description of the sentinel event (“Incident summary”). If the sentinel event originated as a complaint from a patient or staff person, the original complaint is included in the incident summary.

2. **Identifying health information 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 (1996). Two clinical coders manually reviewed the dataset for any inadvertently retained identifiable information and redacted the identifiable information. The sentinel event database was then queried with Microsoft SQL Server 2012 Report Builder 3.0 using an iterative combination of categorical and keyword searches to maximize the likelihood of identifying health IT-related sentinel events. The categories “Sentinel event type” and “Root cause category” were used in the categorical query.

The following criteria were used:

- Reported between January 1, 2010 and June 30, 2013; and
- Sentinel Event Type = Medical equipment-related event; or
- Root Cause Category = Information Management: Confidentiality; or

- Root Cause Category = Information Management: Security of Information; or
- Root Cause Category = Information Management: Data Definitions; or
- Root Cause Category = Information Management: Availability of Information; or
- Root Cause Category = Information Management: Technical Systems; or
- Root Cause Category = Information Management: Patient Identification; or
- Root Cause Category = Information Management: Medical Records; or
- Root Cause Category = Information Management: Aggregation of Data; or
- Root Cause Category = Information Management: Use of Comparative Data; or
- Root Cause Category = Information Management: Other IM Issues.

Keyword queries were performed on the narrative components of the sentinel event report “Incident Summary” and “RCA question responses,” adapting an approach developed by Sparnon (Sparnon & Marella, 2012). 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. See Appendix C for the full list of keywords used in the keyword query. The query was semi-structured using the listed keywords and variations of the keywords (“electronic medical record” in addition to “EMR,” for example) to be inclusive of more events in order to ensure that potential health-IT related events were not missed. The results of the query were continually assessed and used to inform subsequent iterations of keyword queries.

A purposive sample from the sentinel events identified in the categorical and keyword queries was used for this dissertation. Purposive sampling is a method by which units are selected to be in a sample by a deliberate method that is not random (Shadish, Cook, & Campbell, 2001). Due to the high volume of sentinel events identified in the categorical and keyword queries, an abbreviated review of only the sentinel event “Incident summary,” “Synopsis,” “Root cause category,” and subcategories was

performed by the investigator to determine potential health IT involvement. The investigator applied criteria based on the AHRQ Common Format (Figure 4) 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.

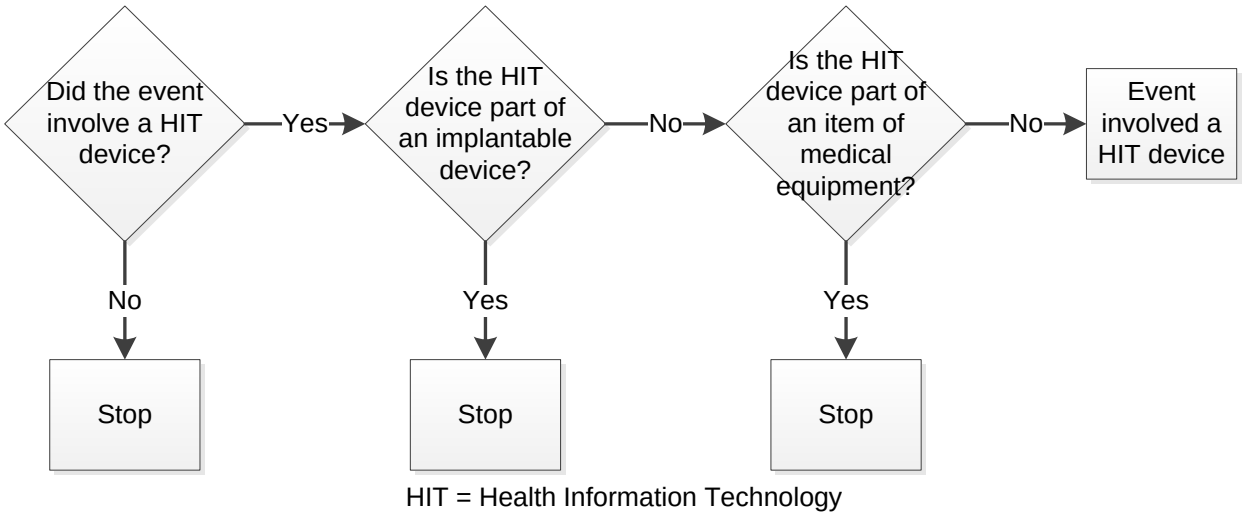



Figure 4. Algorithm for identifying health IT-related events.

Full incident reports of the potential health IT-related sentinel events identified through the categorical and keyword queries were prepared for the next stage of review. Full incident reports contain details of the sentinel event including the “Incident summary,” setting, service, patient’s age, patient’s outcome, “Sentinel event type” categories and subcategories, “Root cause category” and subcategories, and the organization’s “RCA question responses” (see Appendix B).

Two master's-level nurses and the investigator performed content analysis of all the full sentinel event incident reports indentified through the queries 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. Content analysis is the quantitative and/or qualitative analysis of text documents to identify patterns or themes in the text (Trochim & Donnelly, 2008). Typically, content analysis includes several phases beginning with determining the sample for analysis and then dividing the text into segments or "chunks" that will be treated as separate units of analysis. The next phase is coding themes or text segments uncovered during the content analysis. The final phase is to analyze the coded data quantitatively and qualitatively to determine which themes occur most frequently and in what contexts.

The algorithm for identifying health IT-related events was used as the starting point for determining if health IT contributed to or caused the event (Figure 4). Each reviewer independently reviewed all of the full incident reports. The reviewers then discussed each event to reach consensus on whether or not health IT contributed to or caused the event, and, if so, how and why. Disagreements on events were discussed until consensus was obtained. Concepts and themes for contributing and causal factors for health IT-related events (including close calls, hazards, and unsafe conditions), identified through the organization's RCA, were documented and saved in a Microsoft Access 2007 database.

The investigator performed a qualitative confirmatory analysis on the details captured by the reviewers of how and why health IT contributed to or caused the event in addition to the identified concepts and themes. A qualitative confirmatory analysis

involves a literature review that defines the relevant factors and categories to corroborate the themes uncovered during the analysis (Trochim & Donnelly, 2008). Using existing classifications of health IT-related contributing factors, including the AHRQ Common Formats (Agency for Healthcare Research and Quality, 2013), AHRQ Hazard Manager Ontology (Walker, Hassol, Bradshaw, & Rezaee, May 2012), Magrabi's classification (2012), and Sittig and Singh's sociotechnical model (2010), the investigator created a composite classification of health IT-related contributing factors organized by sociotechnical dimensions (Appendix D). This classification was used to code the contributing and causal factors identified during the review.

When reviewing the identified contributing factors the following characteristics were assessed (Shadish et al., 2001):

- Surface similarity—assess the apparent similarities between study operations and the prototypical characteristics of the target of generalization;
- Irrelevancies—identify those things that are irrelevant because they do not change a generalization;
- Discrimination—clarify key discriminations that limit generalization;
- Interpolation and extrapolation—make interpolations to un-sampled values within the range of the sampled instances and, much more difficult, explore extrapolations beyond the sampled range; and
- Causal explanation—develop and test explanatory theories about the pattern of effects, causes, and mediational processes that are essential to the transfer of a causal relationship.

These characteristics are neither independent nor sufficient for generalized causal inference, but help to describe potential relationships between the contributing factors and other variables such as sentinel event type or type of health IT system involved.

The sentinel events were also categorized using a component of the AHRQ Common Format Hospital Version 1.2 for "Device or Medical/Surgical Supply, including Health Information Technology" (Agency for Healthcare Research and Quality, 2013).

Specifically, the classification of health IT devices related to the event or unsafe condition in Question 21 of the abovementioned Common Format was used to categorize what type of devices were involved in the sentinel event.

## IV. Results

Categorical and keyword queries of the sentinel event incident reports reported between January 1, 2010 and June 30, 2013 (n=3,375) resulted in 195 potentially health IT-related sentinel events (Figure 5). Content analysis by the project team of the full incident reports of these events yielded 120 sentinel events where health IT was a contributing factor. Of the remaining potential health IT-related sentinel events, health IT-related risks or unsafe conditions were identified in 57 sentinel events. Either health IT was not a contributing factor or there was not information in the report to confirm whether or not health IT was a contributing factor for the remaining 18 sentinel events.

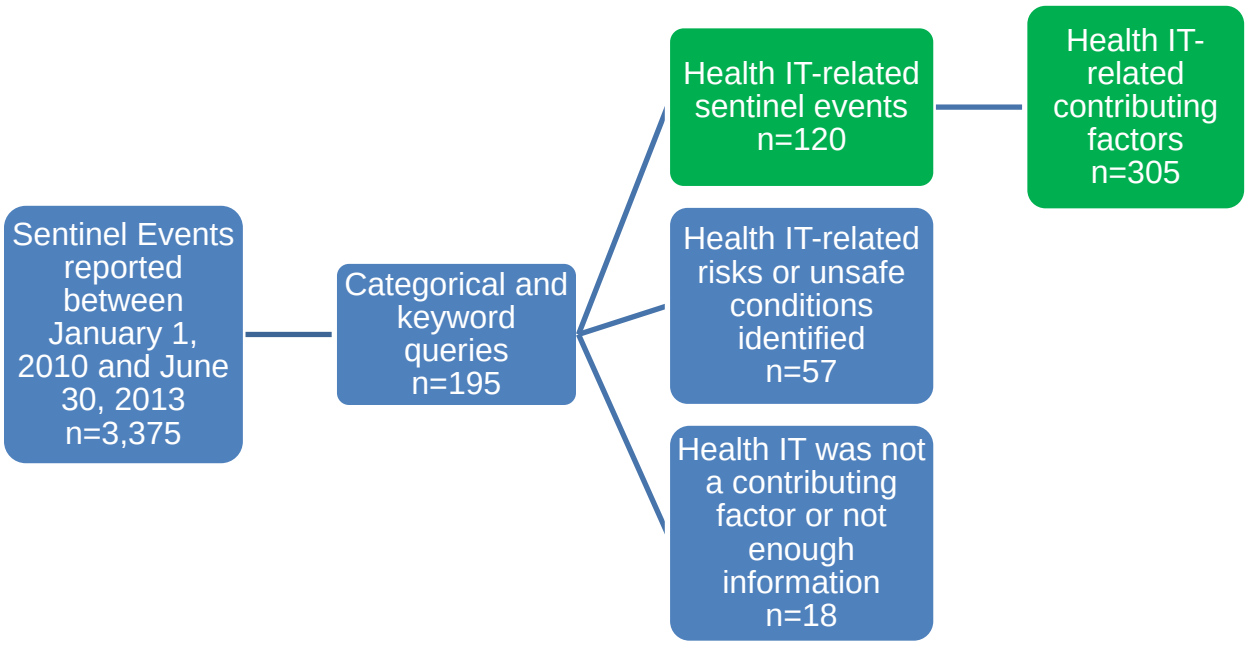



Figure 5. Query and content analysis results.

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 6 for a comparison of patient outcomes.

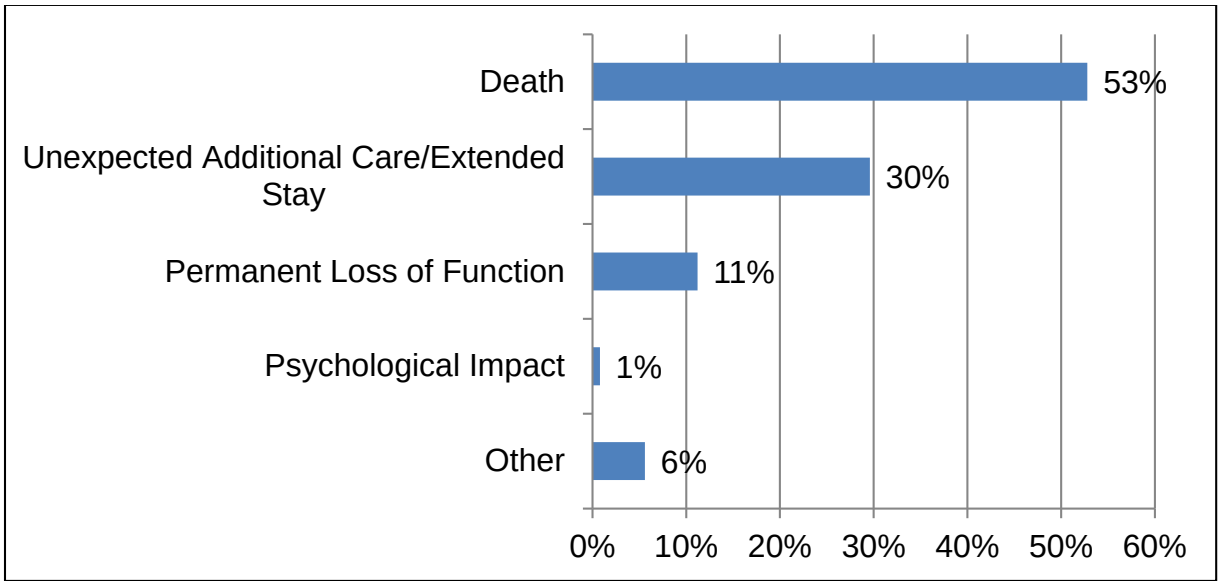



Figure 6. Patient outcomes for health it-related sentinel events.

Each sentinel event has multiple contributing factors. Three hundred five health IT-related contributing factors were identified (Table II). When 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 contributing factors related to the “Human-computer interface” primarily involved inaccurate data entry or erroneous data selection, representing 32% of the contributing factors categorized in this sociotechnical dimension. The distribution of human-computer interface contributing factors is listed in Table III. Other contributing factors related to the human-computer interface dimension included difficulty locating information (14%), display of information or interpretation of that information (13%), unexpected software design related with the human-computer interface (11%), and the location of the hardware (10%). All contributing factors related to the human-computer interface are listed in the Table III.

**TABLE III**
HUMAN-COMPUTER INTERFACE CONTRIBUTING FACTORS

| Contributing factors | % (n=101) |
|---|---|
| Ergonomics—Data entry or selection (e.g., entry or selection of wrong patient, wrong provider, wrong drug, wrong dose) | 32% (32) |
| Ergonomics—Information hard to find | 14% (14) |
| Ergonomics—Information display or interpretation (e.g., font size, color of font, location of information in display screen) | 13% (13) |
| Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) related to the human-computer interface | 11% (11) |
| Ergonomics—Hardware location (e.g., awkward placement for use) | 10% (10) |
| Ergonomics—Alert fatigue/alarm fatigue | 6% (6) |
| Ergonomics—Inadequate feedback to the user | 4% (4) |
| Ergonomics—Data retrieval error—(human) missing data (i.e., did not look at complete record) | 4% (4) |
| Ergonomics—Difficult data entry | 3% (3) |
| Equipment/device function—Image orientation incorrect | 2% (2) |
| Equipment/device function—Image measurement/corruption | 1% (1) |
| Ergonomics—Excessive demands on human memory | 1% (1) |

Workflow- and communication-related contributing factors primarily focused on communication among team members (51%), and suboptimal support of teamwork (31%). Mismatches between user expectations and the technology were related to 17% of the contributing factors associated with workflow and communication. Communication between staff and family was only identified once as a contributing factor. The contributing factors distribution is listed in Table IV.

**TABLE IV**
WORKFLOW AND COMMUNICATION CONTRIBUTING FACTORS

| **Contributing factors** | **% (n=72)** |
|---|---|
| Communication—Among team members | 51% (37) |
| Suboptimal support of teamwork (situation awareness) | 31% (22) |
| Mismatch between user mental models/expectations and health IT | 17% (12) |
| Communication—Staff to patient or family | 1% (1) |

Health IT clinical content-related contributing factors centered on unexpected software design associated with the clinical content (39%) and missing decision support (29%). Others included the availability of data (13%), loss or delay of data (9%), and incorrect software programming calculation (4%). The contributing factors associated with clinical content are listed in Table V.

**TABLE V**
CLINICAL CONTENT CONTRIBUTING FACTORS

| **Contributing factors** | **% (n=70)** |
|---|---|
| Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) related to clinical content | 39% (27) |
| Decision support—Missing recommendation or safeguard | 29% (20) |
| Loss or delay of data—availability | 13% (9) |
| Loss or delay of data—missing | 9% (6) |
| Incorrect software programming calculation | 4% (3) |
| Unpredictable elements of the patient's record available only on paper/scanned documents | 3% (2) |
| Incorrect or inappropriate alert | 1% (1) |
| Loss or delay of data—accuracy | 1% (1) |
| Decision support—Inadequate clinical content | 1% (1) |

Overall, the contributing factors associated with the remaining sociotechnical dimensions were identified less frequently, comprising less than 20% of all contributing factors. Contributing factors associated with internal organizational policies, procedures, and culture primarily focused on the presence or clarity of relevant policies and procedures (Table VI). People-related contributing factors, listed in Table VII, were associated with human factors, training, and failure to “carry out duty,” (i.e., not following established process). Specific cognitive aspects of human factors were uncovered. These included inattention and cognitive load, including multitasking and interruption. Hardware and software issues were attributed mostly to unexpected software design issues. Hardware failures or problems, device incompatibility, and inadequately secured data were the next most frequently identified factors (Table VIII). Contributing factors associated with the sociotechnical dimensions “external rules, regulations, and pressures” and “system measurement and monitoring” were identified least frequently. The external factors (Table IX, n=3) were associated with vendor-related issues such as vendor configuration of the software, inadequate vendor management of changes or updates, and software that was non-configurable. System measurement and monitoring was only identified as a contributing factor twice (n=2).

**TABLE VI**
INTERNAL ORGANIZATIONAL POLICIES, PROCEDURES, AND CULTURE CONTRIBUTING FACTORS

| Contributing factors | % (n=20) |
|---|---|
| Policies and Procedures, including clinical protocols—Presence of policies | 25% (5) |
| Policies and Procedures, including clinical protocols clarity of policies | 20% (4) |
| Supervision/support—Clinical supervision | 15% (3) |
| Environment—Culture of safety | 10% (2) |
| Environment—Physical surrounding (e.g., lighting, noise) | 10% (2) |
| Supervision/support—Managerial supervision | 5% (1) |
| Local implementation—Inadequate control of user access | 5% (1) |
| Local implementation—Inadequate local testing | 5% (1) |
| Local implementation—Suboptimal interface management | 5% (1) |

**TABLE VII**
PEOPLE-RELATED CONTRIBUTING FACTORS

| Contributing factors | % (n=19) |
|---|---|
| Human factors—Inattention | 37% (7) |
| Staff qualifications—Training | 21% (4) |
| Fail to carry out duty | 21% (4) |
| Human factors—Cognitive load, multitasking | 16% (3) |
| Human factors—Cognitive load, interruption | 5% (1) |

**TABLE VIII**
HARDWARE AND SOFTWARE COMPUTING INFRASTRUCTURE

| Contributing factors | % (n=18) |
|---|---|
| Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) | 44% (8) |
| Hardware failure or problem (e.g., device did not turn on or powered off independently during use) | 17% (3) |
| Incompatibility between devices | 11% (2) |
| Inadequately secured data | 11% (2) |
| Equipment/device maintenance | 6% (1) |
| Interactions with other (non-health IT) care systems | 6% (1) |
| Software not available | 6% (1) |

**TABLE IX**
EXTERNAL RULES, REGULATIONS, AND PRESSURES

| Contributing factors | % (n=3) |
|---|---|
| Vendor factors—Faulty vendor configuration recommendation | 33% (1) |
| Vendor factors—Inadequate vendor software change control | 33% (1) |
| Vendor factors—Non-configurable software | 33% (1) |

The AHRQ Common Format 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. The specific component of EHR was categorized into subcategories (i.e., CPOE, CDS) if it was identified in the report. 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 X.

**TABLE X**
HEALTH IT DEVICE INVOLVED

| **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) |

For the sentinel events associated specifically with EHRs (n=32), communication and suboptimal support of teamwork were the more frequently reported contributing factors. Other contributing factors included missing decision support, unexpected software design issues, and difficulty locating information. The top ten identified contributing factors associated with EHRs are listed in Table XI. The full list of contributing factors can be found in Appendix D.

**TABLE XI**
CONTRIBUTING FACTORS ASSOCIATED WITH EHRS

| **Contributing factors** | **Count (n=32)** |
|---|---|
| Communication—Among team members | 12 |
| Suboptimal support of teamwork (situation awareness) | 9 |
| Decision support—Missing recommendation or safeguard | 7 |
| Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) related to clinical content | 6 |
| Ergonomics—Information hard to find | 6 |
| Loss or delay of data—Availability | 4 |
| Mismatch between user mental models/expectations and health IT | 3 |
| Ergonomics—Information display or interpretation (e.g., font size, color of font, location of information in display screen) | 3 |
| Ergonomics—Hardware location (e.g., awkward placement for use) | 3 |
| Policies and Procedures, including clinical protocols—Presence of policies | 3 |

Frequently identified contributing factors associated with CPOE systems (n=29) were associated with data entry or selection, and communication. Other contributing factors included unexpected software design issues, missing decision support, and suboptimal support of teamwork. The top ten identified contributing factors associated with CPOEs are listed in Table XII.

**TABLE XII**
CONTRIBUTING FACTORS ASSOCIATED WITH CPOE

| **Contributing factors** | **Count (n=29)** |
|---|---|
| Ergonomics—Data entry or selection (e.g., entry or selection of wrong patient, wrong provider, wrong drug, wrong dose) | 16 |
| Communication—Among team members | 10 |
| Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) related to clinical content | 7 |
| Decision support—Missing recommendation or safeguard | 6 |
| Suboptimal support of teamwork (situation awareness) | 5 |
| Mismatch between user mental models/expectations and health IT | 5 |
| Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) related to human-computer interface | 4 |
| Fail to carry out duty | 3 |
| Loss or delay of data—Availability | 2 |
| Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) | 2 |

# V. Discussion

The 120 health IT-related sentinel events resulted in the identification of more than 300 contributing factors that are classified into 50 different types of contributing factors (Table XIII, Appendix E) from a possible 77 contributing factors in the classification (Appendix D). Health IT-related contributing factors were identified in all eight sociotechnical dimensions with no identified contributing factors falling outside the dimensions. This suggests that the model suggested by Sittig and Singh is sufficient for capturing relevant health IT-related contributing factors.

As previously discussed, when accredited organizations report the findings from its RCA to The Joint Commission, they utilize an RCA framework that ensures that the organization has addressed the active failures and latent conditions involved in the event (Reason 2000). These include human, environmental, organizational, and cultural contributing factors. The structured process for collecting and reporting information on these types of contributing factors clearly illustrates aspects of Reason's Swiss cheese model, and is what makes data from the Sentinel Event Database unique from other PSE reporting systems.

## A. 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 will 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.

## B. **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.

## C. **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.

## D. 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 identified 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.

## E. 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 (Tables XI and XII). 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.

## F. Limitations

In this study, de-identified sentinel event data submitted to The Joint Commission are used to describe how health IT contributed to or caused a PSE. The study of sentinel event data is unique because the events must first meet the definition of "reviewable sentinel event" before they are accepted for reporting to The Joint Commission. As previously described, the definition for "reviewable sentinel event" is

specific and deals with 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 (see Figure 7).

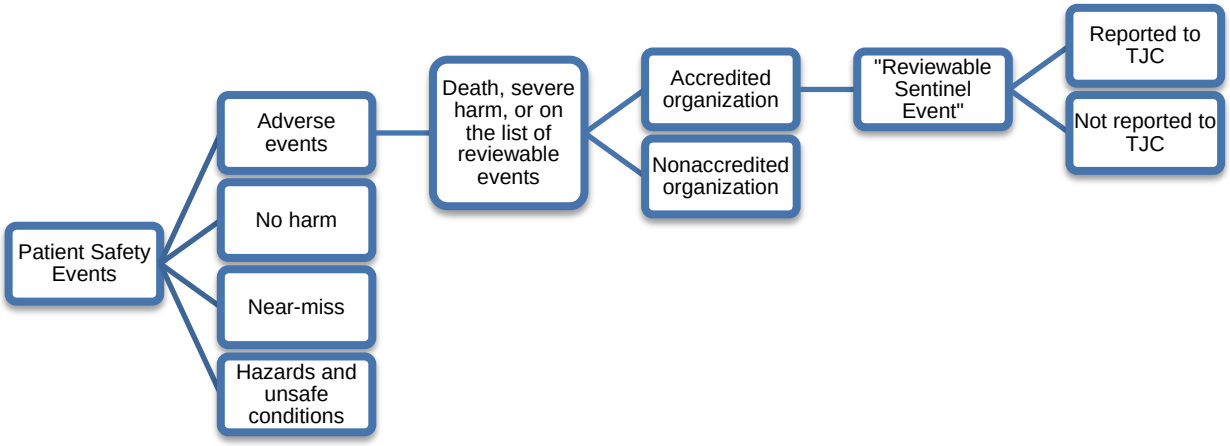



Figure 7. “Reviewable sentinel Event” as a subset of patient safety events.

Reporting to The Joint Commission is in most cases voluntary; thus, the sample represents a small proportion of all PSEs that occur in accredited organizations (The Joint Commission, 2014b). The rate of reporting for some high profile event types, such as suicides, wrong site surgeries, or unintended retained foreign objects, is out of proportion relative to other event types and not indicative of true rates of events. Further, these incidents are not a representative sample of all reported PSEs because organizations’ accreditation by The Joint Commission is voluntary. Variation in state

laws for protection from legal discoverability may also restrict an organization's willingness to share PSE reports with The Joint Commission (Suydam, Liang, Anderson, & Weinger, 2005).

The Joint Commission's voluntary reporting process entails sharing the findings of an accredited organization's "root cause" analysis to provide a richer description of the incident than would traditional incident reporting. In this, it is similar to other research on PSE reporting, but it differs in purpose and mechanism for reporting. As an example, Sparnon (2012) in her study queried the PA-PSRS for reports related to EHRs and associated health IT. The PA-PSRS system is run by an independent state agency established by the state of Pennsylvania known as the Pennsylvania Patient Safety Authority. By law, all Pennsylvania hospitals, ambulatory surgery centers, birthing centers, and certain abortion facilities must report all adverse events and near misses to the Authority (Pennsylvania Patient Safety Authority, n.d.). Contrast this to Magrabi's study (2012) of the FDA MAUDE, a national database that captures data from mandated manufacturer and voluntary clinical, patient, and consumer reports of device failure. Thus, given their scope and purpose, these specific reporting processes may limit the generalizability of findings based on PSE reporting databases.

Under the current Sentinel Event Policy, RCA is the required method for incident investigation. Anecdotal evidence suggests that healthcare organizations have difficulty performing effective RCAs and that implementation of actions to reduce risk of a future event is inconsistent (Wu, Lipshutz, & Pronovost, 2008). In addition, there are many different models, tools, and techniques for performing RCAs, which leads to confusion. As a result, many RCAs are performed incorrectly or incompletely and do not produce

usable results. Further, performing a thorough and credible RCA can be time-consuming and resource-intensive, limiting the number of analyses an organization will perform on PSEs.

Current definitions and categorization of sentinel events, their root causes, and the actions captured in the Sentinel Event Database do not include commonly used health IT-related concepts and terms. This limitation could have impacted the investigator's identification of health IT-related sentinel events. The keywords used to query the database were not exhaustive, which could lead to the failure to identify some health IT-related sentinel events in the database.

# VI. Conclusion

The classification of health IT-related contributing factors clearly indicates that health IT-related sentinel events are primarily associated with the sociotechnical dimensions of human interface and workflow and communication. This is corroborated by Sparnon's (2012) finding that the majority of reports to the Pennsylvania Patient Safety Authority involved errors in human data entry such as entry of wrong data or the failure to enter data. Only a few reports to the Authority indicated technical failures of the health IT system. Meeks et al. (2014) in their analysis of patient safety concerns reported to the Veterans Health Administration found social dimensions such as workflow, policies, and personnel interacted in a complex fashion with technical dimensions of software/hardware, clinical content, and user interface to produce safety concerns. This supports the conclusion that health IT-related sentinel events are associated with the sociotechnical dimensions of human interface and workflow and communication. These findings contrast to Magrabi's study (2012) of 436 events from the FDA MAUDE database, which resulted in the identification of 712 problems, 96% of which were machine-related and 4% were problems at the human-computer interface. These differences are likely due to the differing scope and purpose of the patient safety databases and the people who report events (Sparnon & Marella, 2012). This suggests that the design of a PSE reporting system can influence the characterization of the events that are reported.

The health IT-related contributing factor classification accommodated all sentinel events (Table XIII, Appendix E), suggesting that the classification is sufficient. Some

contributing factors were not represented in the analysis, but that does not mean they should be eliminated from the classification. The 27 contributing factors from the classification not identified in the analysis of sentinel events were focused on more technical issues such as detailed aspects of decision support, vendor factors, network failures, and computer viruses. These factors may not have been identified because, in general, the person completing the report of the sentinel event is a clinician and not as familiar with how the technical aspects could have contributed to the event. The full list of contributing factors, including those not identified in the sentinel event analyses can be found in Appendix D.

Erroneous or inaccurate entry or selection of data was a clearly identified factor that is primarily associated with CPOE systems, leading to communication issues between clinicians. These communication issues lead to medication errors and wrong-site surgeries, ultimately harming the patient. Communication issues were also associated with the EHR systems, leading to a loss of a complete clinical picture of the patient. The abovementioned relationships among contributing factors, health IT systems, and types of events that occur provide validation of the sociotechnical model and classification of health IT-related contributing factors.

The frequent identification of erroneous or inaccurate entry or selection of data as a contributing factor, however, may incorrectly lead one to think that the event was caused solely by a person making a mistake. Upon greater inspection these events were caused by the correct “orderable” or medication “order sets” not being available as a selection in the drop-down menu, details of the intended procedure entered in the notes section, or a selection “auto-populated” with incorrect information in CPOE

systems (considered a component of the EHR). Thoughtful design, careful implementation, safe use, and monitoring health IT in the context of a sociotechnical system can help prevent and mitigate problems before they cause patient harm.

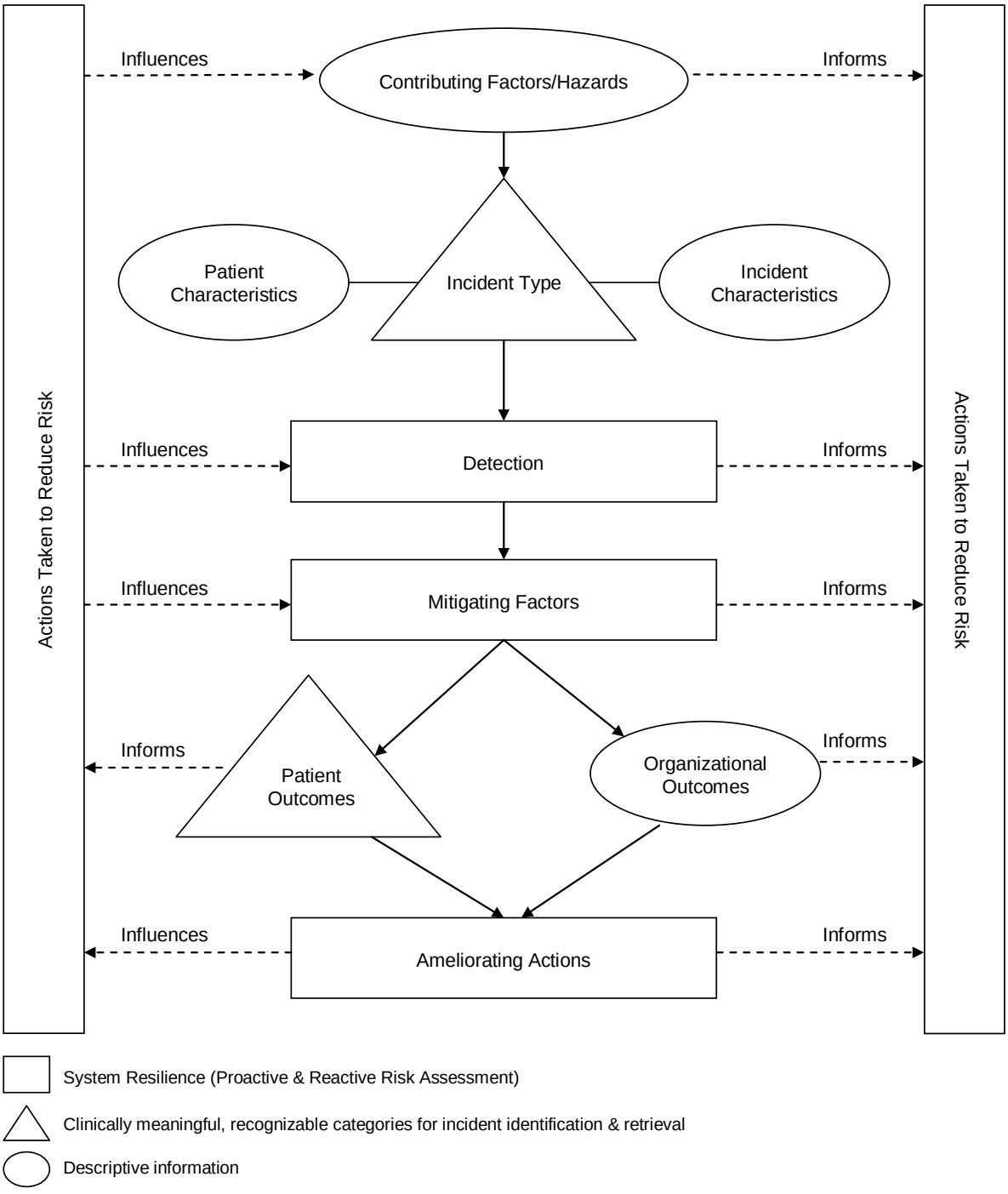
A single healthcare organization can control some aspects of the continuum of safe health IT design, implementation, use, and monitoring but not all. Some design features of the user interface can only be changed by the software developer for example. Comprehensive health IT safety can only be achieved through a concerted collaboration of software developers, equipment manufacturers, clinicians, IT professionals, patient safety organizations, professional associations, accreditors, and government agencies. The FDA in their *FDASIA Health IT Report* proposed this type of collaboration with actions coordinated through a Health IT Safety Center (Food and Drug Administration, 2014a).

An opportunity for future research includes deeper analysis of health IT-related contributing factors associated with specific types of events. Comparison of the results of this type of analysis with other large PSE reporting systems—participating in the FDA's proposed Health IT Safety Center for example—would help to validate the findings of this research. Improved identification of health IT contributing factors would help improve the characterization of sentinel events and the identification of problems to be addressed by software developers, equipment manufacturers, and end users in healthcare organizations. This also presents the opportunity to apply these findings proactively in identifying vulnerabilities and hazards in systems. The classification of health IT contributing factors, coupled with Sittig and Singh's sociotechnical model, can characterize critical health IT-related contributing factors and their interactions with

greater detail across the continuum of health IT design, implementation, use, and monitoring. The classification provides the necessary foundation for learning how to ensure that the technology we use to treat patients is safe and is used safely.

# APPENDICES

## APPENDIX A




The solid lines represent the semantic relationships between the classes. The dotted lines represent the flow of information.

Figure 8. World Health Organization International Classification for Patient Safety

## APPENDIX B

**ROOT CAUSE ANALYSIS AND ACTION PLAN FRAMEWORK TEMPLATE**

**The Joint Commission Root Cause Analysis and Action Plan tool has 24 analysis questions. The following framework is intended to provide a template for answering the analysis questions and aid organizing the steps in a root cause analysis. All possibilities and questions should be fully considered in seeking "root cause(s)" and opportunities for risk reduction. Not all questions will apply in every case and there may be findings that emerge during the course of the analysis. Be sure, however, to enter a response in the "Root Cause Analysis Findings" field for each question #. For each finding continue to ask "Why?" and drill down further to uncover why parts of the process occurred or didn't occur when they should have. Significant findings that are not identified as root causes themselves have "roots."**

**As an aid to avoid "loose ends," the two columns on the right are provided to be checked off for later reference:**

- **"Root cause" should be answered "Yes" or "No" for each finding. A root cause is typically a finding related to a process or system that has a potential for redesign to reduce risk. If a particular finding is relevant to the event is not a root cause, be sure that it is addressed later in the analysis with a "Why?" question such as "Why did it contribute to the likelihood of the event" or "Why did it contribute to the severity of the event?" Each finding that is identified as a root cause should be considered for an action and addressed in the action plan.**
- **"Plan of action" should be answered "Yes" for any finding that can reasonably be considered for a risk reduction strategy. Each item checked in this column should be addressed later in the action plan.**

## APPENDIX B (continued)

**When did the event occur?**

| **Date:** | **Day of the week:** | **Time:** |
|---|---|---|

**Detailed Event Description Including Timeline:**

| |
|---|
| |

**Diagnosis:**

| |
|---|
| |

**Medications:**

| |
|---|
| |

**Autopsy Results:**

| |
|---|
| |

**Past Medical/Psychiatric History:**

| |
|---|
| |

## APPENDIX B (continued)

| # | Analysis Question | Prompts | Root Cause Analysis Findings | Root cause | Plan of Action |
|---|---|---|---|---|---|
| 1 | **What was the intended process flow?** | **List the relevant process steps as defined by the policy, procedure, protocol, or guidelines in effect at the time of the event. You may need to include multiple processes.**<br>***Note:*** **The process steps *as they occurred in the event* will be entered in the next question.**<br>**Examples of defined process steps may include, but are not limited to:**<br>• **Site verification protocol**<br>• **Instrument, sponge, sharps count procedures**<br>• **Patient identification protocol**<br>• **Assessment (pain, suicide risk, physical, and psychological) procedures**<br>• **Fall risk/fall prevention guidelines** | | | |
| 2 | **Were there any steps in the process that did not occur as intended?** | **Explain in detail any deviation from the intended processes listed in Analysis Item #1 above.** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| **3** | **What human factors were relevant to the outcome?** | **Discuss staff-related human performance factors that contributed to the event. Examples may include, but are not limited to:**<br>• **Boredom**<br>• **Failure to follow established policies/procedures**<br>• **Fatigue**<br>• **Inability to focus on task**<br>• **Inattentional blindness/ confirmation bias**<br>• **Personal problems**<br>• **Lack of complex critical thinking skills**<br>• **Rushing to complete task**<br>• **Substance abuse**<br>• **Trust** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| 4 | **How did the equipment performance affect the outcome?** | **Consider all medical equipment and devices used in the course of patient care, including such items as AED devices, crash carts, suction, oxygen, instruments, monitors, infusion equipment. In your discussion, provide information on the following, as applicable:**<br>• **Descriptions of biomedical checks**<br>• **Availability and condition of equipment**<br>• **Descriptions of equipment with multiple or removable pieces**<br>• **Location of equipment and its accessibility to staff and patients**<br>• **Staff knowledge of or education on equipment, including applicable competencies**<br>• **Correct calibration, setting, operation of alarms, displays, and controls** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| **5** | **What controllable environmental factors directly affected this outcome?** | **What environmental factors within the organization's control affected the outcome?**<br>**Examples may include, but are not limited to:**<br>• **Overhead paging that cannot be heard**<br>• **Safety or security risks**<br>• **Risks involving activities of visitors**<br>• **Lighting or space issues**<br>**The response to this question may be addressed more globally in Question #17.This response should be specific to this event.** | | | |
| **6** | **What uncontrollable external factors influenced this outcome?** | **Identify any factors the organization cannot change that contributed to a breakdown in the internal process, for example natural disasters.** | | | |
| **7** | **Were there any other factors that directly influenced this outcome?** | **List any other factors not yet discussed.** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| 8 | **What are the other areas in the organization where this could happen?** | **List all other areas in which the potential exists for similar circumstances. For example:**<br>• **Inpatient surgery/outpatient surgery**<br>• **Inpatient psychiatric care/outpatient psychiatric care**<br>**Identification of other areas within the organization that have the potential to impact patient safety in a similar manner. This information will help drive the scope of your action plan.** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| **9** | **Was the staff properly qualified and currently competent for their responsibilities at the time of the event?** | **Include information on the following for all staff and providers involved in the event. Comment on the processes in place to ensure staff is competent and qualified. Examples may include but are not limited to:**<br>• **Orientation/training**<br>• **Competency assessment (What competencies do the staff have and how do you evaluate them?)**<br>• **Provider and/or staff scope of practice concerns**<br>• **Whether the provider was credentialed and privileged for the care and services he or she rendered**<br>• **The credentialing and privileging policy and procedures**<br>• **Provider and/or staff performance issues** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| **10** | **How did actual staffing compare with ideal levels?** | **Include ideal staffing ratios and actual staffing ratios along with unit census at the time of the event. Note any unusual circumstance that occurred at this time. What process is used to determine the care area's staffing ratio, experience level, and skill mix?** | | | |
| **11** | **What is the plan for dealing with staffing contingencies?** | **Include information on what the organization does during a staffing crisis, such as call-ins, bad weather, or increased patient acuity.**<br>**Describe the organization's use of alternative staffing. Examples may include, but are not limited to:**<br>• **Agency nurses**<br>• **Cross-training**<br>• **Float pool**<br>• **Mandatory overtime**<br>• **PRN pool** | | | |
| **12** | **Were such contingencies a factor in this event?** | **If alternative staff were used, describe their orientation to the area, verification of competency, and environmental familiarity.** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| **13** | **Did staff performance during the event meet expectations?** | **Describe whether staff performed as expected within or outside of the processes. To what extent was leadership aware of any performance deviations at the time? What proactive surveillance processes are in place for leadership to identify deviations from expected processes? Include omissions in critical thinking and/or performance variance(s) from defined policy, procedure, protocol and guidelines in effect at the time.** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| 14 | **To what degree was all the necessary information available when needed? Accurate? Complete? Unambiguous?** | **Discuss whether patient assessments were completed, shared, and accessed by members of the treatment team, to include providers, according to the organizational processes.**<br>**Identify the information systems used during patient care.**<br>**Discuss to what extent the available patient information (e.g., radiology studies, lab results, or medical record) was clear and sufficient to provide an adequate summary of the patient's condition, treatment, and response to treatment.**<br>**Describe staff utilization and adequacy of policy, procedure, protocol, and guidelines specific to the patient care provided.** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| **15** | **To what degree was the communication among participants adequate for this situation?** | **Analysis of factors related to communication should include evaluation of verbal, written, electronic communication or the lack thereof. Consider the following in your response, as appropriate:**<br>• **The timing of communication of key information**<br>• **Misunderstandings related to language/cultural barriers, abbreviations, terminology**<br>• **Proper completion of internal and external hand-off communication**<br>• **Involvement of patient, family, and/or significant other** | | | |

| | | | | | |
|---|---|---|---|---|---|
| **16** | **Was this the appropriate physical environment for the processes being carried out for this situation?** | **Consider processes that proactively manage the patient care environment. This response may correlate to the response in question 6 on a more global scale. What evaluation tool or method is in place to evaluate process needs and mitigate physical and patient care environmental risks? How are these process needs addressed organization-wide? Examples may include, but are not limited to:**<br>• **alarm audibility testing**<br>• **evaluation of egress points**<br>• **patient acuity level and setting of care managed across the continuum**<br>• **preparation of medication outside of pharmacy** | | | |
| **17** | **What systems are in place to identify environmental risks?** | **Identify environmental risk assessments.**<br>• **Does the current environment meet codes, specifications, regulations?**<br>• **Does staff know how to report environmental risks?**<br>• **Was there an environmental risk involved in the event that was not previously identified?** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| 18 | **What emergency and failure-mode responses have been planned and tested?** | **Describe variances in expected process due to an actual emergency or failure-mode response in connection to the event.**<br>**Related to this event, what safety evaluations and drills have been conducted and at what frequency (e.g., mock code blue, rapid response, behavioral emergencies, patient abduction, or patient elopement)?**<br>**Emergency responses may include, but are not limited to:**<br>• **Fire**<br>• **External disaster**<br>• **Mass casualty**<br>• **Medical emergency**<br>**Failure-mode responses may include, but are not limited to:**<br>• **Computer downtime**<br>• **Diversion planning**<br>• **Facility construction**<br>• **Power loss**<br>• **Utility issues** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| **19** | **How does the organization's culture support risk reduction?** | **How does the overall culture encourage change, suggestions, and warnings from staff regarding risky situations or problematic areas?**<br>• **How does leadership demonstrate the organization's culture and safety values?**<br>• **How does the organization measure culture and safety?**<br>• **How does leadership establish methods to identify areas of risk or access employee suggestions for change?**<br>• **How are changes implemented?** | | | |
| **20** | **What are the barriers to communication of potential risk factors?** | **Describe specific barriers to effective communication among caregivers that have been identified by the organization. For example, residual intimidation or reluctance to report coworker activity.**<br>**Identify the measures being taken to break down barriers (e.g., use of SBAR). If there are no barriers to communication discuss how this is known.** | | | |

## APPENDIX B (continued)

| | | | | | |
|---|---|---|---|---|---|
| 21 | **How is the prevention of adverse outcomes communicated as a high priority?** | **Describe the organization's adverse outcome procedures and how leadership plays a role within those procedures.** | | | |
| 22 | **How can orientation and in-service training be revised to reduce the risk of such events in the future?** | **Describe how orientation and ongoing education needs of the staff are evaluated and discuss its relevance to event. (e.g., competencies, critical thinking skills, use of simulation labs, evidence based practice)** | | | |
| 23 | **Was available technology used as intended?** | **Examples may include, but are not limited to:**<br>• **CT scanning equipment**<br>• **Electronic charting**<br>• **Medication delivery system**<br>• **Tele-radiology services** | | | |
| 24 | **How might technology be introduced or redesigned to reduce risk in the future?** | **Describe any future plans for implementation or redesign. Describe the ideal technology system that can help mitigate potential adverse events in the future.** | | | |

## APPENDIX B (continued)

| Action Plan | Organization Plan of Action<br>Risk Reduction Strategies | Position/Title<br>Responsible Party | Method: Policy, Education, Audit, Observation & Implementation |
|---|---|---|---|
| **For each of the findings identified in the analysis as needing an action, indicate the planned action expected, implementation date, and associated measure of effectiveness. OR. …**<br>**If after consideration of such a finding, a decision is made not to implement an associated risk reduction strategy, indicate the rationale for not taking action at this time.**<br>**Check to be sure that the selected measure will provide data that will permit assessment of the effectiveness of the action.**<br>**Consider whether pilot testing of a planned improvement should be conducted.** | **Action Item #1:** | | |
| | **Action Item #2:** | | |
| | **Action Item #3:** | | |
| | **Action Item #4:** | | |

**Bibliography: Cite all books and journal articles that were considered in developing this root cause analysis and action plan.**

## APPENDIX C

### QUERY KEYWORDS

- Information systems
- Health IT
- HIT
- Information technology
- EHR
- electronic health record
- EMR
- electronic medical record
- EDIS
- electronic document information system
- Computerized physician order entry
- CPOE
- Laboratory information system
- LIS
- Data display
- data
- Data retrieval
- Graphic
- Dropdown
- Decision support
- Medication list
- Alert fatigue
- Automated
- Wireless
- Bar-coding
- Barcoding
- Interoperable
- Picture archiving and communication systems
- Communication systems
- PACS
- Administrative billing system
- Practice management
- Automated dispensing system
- Interface device
- Keyboard
- Mouse
- Touchscreen
- Speech recognition system
- Display
- Printer
- Electronic medication administration records
- eMARs
- Clinical documentation system
- Software
- Data retrieval
- Network
- Computer
- Truncate
- Paste [i.e., “copy and paste”]
- Allscripts
- GE Healthcare
- Centricity
- eClinicalWorks
- Practice fusion
- NextGen
- Aprima
- Athenahealth
- AthenaClinicals
- Cerner
- CureMD
- DocPatient Network
- Doctations
- DocApp
- Epic
- EpicCare
- MyChart
- Greenway
- Primesuite
- McKessson
- Horizon Ambulatory
- Medisoft Clinical
- Medical Communication Systems
- iPatientCare
- Meditech
- Medsphere
- OpenVista
- Sage Software
- Intergy

## APPENDIX D

## HEALTH IT-RELATED CONTRIBUTING FACTORS

**CH =** Common Formats—HERF, PIF, or SIR[1]
**CD =** Common Formats—Device or Medical/Surgical Supply, including Health Information Technology[2]
**H =** Hazard Manager Ontology[3]
**M =** Magrabi Classification[4]

**Hardware and software computing infrastructure—**required to run the healthcare applications

- Incompatibility between devices (CD—4.3.1, H, M—2.2, 4.4.3)
- Equipment/device maintenance (CD—4.3.3)
- Hardware failure or problem (e.g., device did not turn on or powered off independently during use) (CD—4.3.4, H, M—1.1, M—3.1, 3.3, 4.1)
- Network failure or problem (CD—4.3.5, M—2.1, 4.4.4)
- Security, virus, or other malware issue (CD—4.3.7, H, M—4.3)
- Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) related to hardware and software computing infrastructure (CD—4.3.8, M—2.2, 4.4.1, 4.4.2)
- Interactions with other (non-health IT) care systems (H)
- Inadequately secured data (H) [similar concept to "Security, virus, or other malware issue"]
- Software not available (M—4.2)
- Data retrieval error—(Machine) Not alerted (M—3.4.4)

**Clinical content—**data, information, and knowledge entered, displayed, or transmitted

- Equipment/device function (CD—4.3.2, M—3.3)
    - Loss or delay of data (CD—4.3.2.1, H, M—3.2, 3.3, M—4.5)
        - Availability (CH—2.3.9, M—3.2)
        - Accuracy (CH—2.3.10, M—3.3)

---

[1] Agency for Healthcare Research and Quality. (2013). Hospital common formats version 1.2: event descriptions, sample reports, and forms. Retrieve, 2013, Retrieved from: https://www.psoppc.org/web/patientsafety/version-1.2_documents.

[2] Agency for Healthcare Research and Quality. (2013). Hospital common formats - version 1.2: Event descriptions, sample reports, and forms. https://www.psoppc.org/web/patientsafety/version-1.2_documents#SupplyRetrieved, 2013, Retrieved from

[3] Walker, J., Hassol, A., Bradshaw, B., & Rezaee, M. (May 2012). *Health IT hazard manager beta-test: Final report. (prepared by ABT Associates and Geisinger Health System, under contract no. HHSA290200600011i, #14).* Rockville, MD: Agency for Healthcare Research and Quality.

[4] Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E. (2012). Using FDA reports to inform a classification for health information technology safety problems. *Journal of the American Medical Informatics Association: JAMIA*, 19(1), 45-53. doi:10.1136/amiajnl-2011-000369 [doi]

        - Legibility (CH—2.3.11)
    - System returns or stores data that do not match patient (CD—4.3.2.2, H)
    - Incorrect software programming calculation (CD—4.3.2.6)
    - Incorrect or inappropriate alert (CD—4.3.2.7)
- IT contributed to entry of data in the wrong patient's record (H, M—3.4.1)
- Patient information/results routed to the wrong recipient (H)
- Faulty reference information (H)
- Unpredictable elements of the patient's record available only on paper/scanned documents (H)
- Inaccurate natural language processing (H)
- Decision support (H)
    - Excessive nonspecific recommendations/alerts
    - Faulty recommendation
    - Missing recommendation or safeguard
    - Inadequate clinical content
    - Inappropriate level of automation
- Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) related to clinical content (CD—4.3.8)

**Human -computer interface**—aspects of the system that users can see, touch, or hear

- Ergonomics, including human/device interface issue (CD—4.3.6, M—2.2)
    - Hardware location (e.g., awkward placement for use) (CD—4.3.6.1)
    - Data entry or selection (e.g., entry or selection of wrong patient, wrong provider, wrong drug, wrong dose) (CD—4.3.6.2, H, M—1.2.1, 1.2.2, 1.2.3)
    - Information display or interpretation (e.g., font size, color of font, location of information in display screen) (CD—4.3.6.3, H, M—3.3)
    - Data retrieval error—(Human) Missing data (i.e., did not look at complete record) (M—3.4.2)
    - Alert fatigue/alarm fatigue (CD—4.3.6.4)
    - Information hard to find (H)
    - Difficult data entry (H)
    - Excessive demands on human memory (H)
    - Inadequate feedback to the user (H)
- Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) related to the human computer interface (CD—4.3.8)
- Equipment/device function (CD—4.3.2)
    - Image measurement/corruption issue (CD—4.3.2.3, M—3.3)
    - Image orientation incorrect (CD—4.3.2.4, M—3.3)
    - Incorrect test results (CD—4.3.2.5)

## APPENDIX D (continued)

**People**—the humans involved in the design, development, implementation, and use of health IT including patient

- Human Factors
  - Stress (CH—2.3.16)
  - Inattention (CH—2.3.17)
  - Health issues (CH—2.3.19)
  - Cognitive load (CH—2.3.18, M—5.2.2, H)
    - Interruption (M—5.2.1)
    - Multitasking (M—5.2.2)
  - Fail to carry out duty (M—5.3, 1.2.4)
    - Fail to log-off (M—5.3.1)
- Data retrieval error—Did not look (M—3.4.3)
- Staff qualifications
  - Competence (e.g., qualifications, experience) (CH—2.3.3)
  - Training (CH—2.3.4, H, M—5.1)
- Mismatch between user mental models/expectations and health IT (H)

**Workflow and communication**—the steps needed to ensure that each patient receives the care they need at the time they need it

- Communication
  - Supervisor to staff (CH—2.3.12, H)
  - Among team members (CH—2.3.13, H)
  - Staff to patient or family (CH—2.3.14)
- Suboptimal support of teamwork (situation awareness) (H)
- Mismatch between real workflows and health IT (H)

**Internal organizational policies, procedures, and culture—**internal culture, structures, policies, and procedures that affect all aspects of health IT management and healthcare

- Environment
  - Culture of safety (CH—2.3.1)
  - Management (CH—2.3.1, H)
  - Physical surroundings (e.g., lighting, noise) (CH—2.3.2, H)
- Supervision/Support
  - Clinical supervision (CH—2.3.5)
  - Managerial supervision (CH—2.3.6)
- Policies and Procedures, including clinical protocols
  - Presence or policies (CH—2.3.7)
  - Clarity of policies (CH—2.3.8, H)
- Local Implementation (H)
  - Faulty local configuration or programming
  - Inadequate local testing
  - Inadequate software change control
  - Inadequate control of user access

    - Suboptimal interface management

- Organizational policy contributed to entry of data in the wrong patient's record (H)

**External rules, regulations, and pressures**—external forces that facilitate or place constraints on the design, development, implementation, use, and evaluation of health IT in the clinical setting

- Vendor factors (H)
    - Faulty vendor configuration recommendation
    - Unusable software implementation tools
    - Non-configurable software
    - Inadequate vendor testing
    - Inadequate vendor software change control
    - Inadequate control of user access
    - Faulty software design (specification)

**System measurement and monitoring**—evaluation of system availability, use, effectiveness, and unintended consequences of system use

## APPENDIX E

### TABLE XIII

CLASSIFICATION OF HEALTH IT-RELATED CONTRIBUTING FACTORS

| Health IT-related Contributing Factors (n=305) | Percentage of Total |
|---|---|
| Communication—Among team members | 12% |
| Ergonomics—Data entry or selection (e.g., entry or selection of wrong patient, wrong provider, wrong drug, wrong dose) | 11% |
| Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) related to clinical content | 9% |
| Suboptimal support of teamwork (situation awareness) | 7% |
| Decision support—Missing recommendation or safeguard | 7% |
| Ergonomics—Information hard to find | 5% |
| Ergonomics—Information display or interpretation (e.g., font size, color of font, location of information in display screen) | 4% |
| Mismatch between user mental models/expectations and health IT | 4% |
| Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) related to the human-computer interface | 4% |
| Ergonomics—Hardware location (e.g., awkward placement for use) | 3% |
| Loss or delay of data—Availability | 3% |
| Unexpected software design issue (i.e., event in which the safety issue is caused by an unforeseen or unexpected aspect of the software design) | 3% |
| Human factors—Inattention | 2% |
| Ergonomics—Alert fatigue/alarm fatigue | 2% |
| Loss or delay of data | 2% |
| Policies and Procedures, including clinical protocols—Presence of policies | 2% |
| Fail to carry out duty | 1% |
| Policies and Procedures, including clinical protocols clarity of policies | 1% |
| Staff qualifications—training | 1% |
| Ergonomics—Inadequate feedback to the user | 1% |
| Ergonomics—Data retrieval error—(human) missing data (i.e., did not look at complete record) | 1% |
| Hardware failure or problem (e.g., device did not turn on or powered off independently during use) | 1% |
| Ergonomics—Difficult data entry | 1% |
| Human factors—Cognitive load, multitasking | 1% |
| Supervision/support—Clinical supervision | 1% |
| Incorrect software programming calculation | 1% |
| Incompatibility between devices | 1% |
| Equipment/device function—Image orientation incorrect | 1% |
| Environment—Culture of safety | 1% |
| Environment—Physical surrounding (e.g., lighting, noise) | 1% |

## APPENDIX E (continued)

CLASSIFICATION OF HEALTH IT-RELATED CONTRIBUTING FACTORS

| Health IT-related Contributing Factors (n=305) | Percentage of Total |
|---|---|
| Inadequately secured data | 1% |
| Unpredictable elements of the patient's record available only on paper/scanned documents | 1% |
| System measurement and monitoring | 1% |
| Communication—Staff to patient or family | <1% |
| Vendor factors—Inadequate vendor software change control | <1% |
| Local implementation—Suboptimal interface management | <1% |
| Supervision/support—Managerial supervision | <1% |
| Software not available | <1% |
| Incorrect or inappropriate alert | <1% |
| Decision support—Inadequate clinical content | <1% |
| Equipment/device function—Image measurement/corruption | <1% |
| Ergonomics—Excessive demands on human memory | <1% |
| Human factors—Cognitive load, interruption | <1% |
| Loss or delay of data—Accuracy | <1% |
| Equipment/device maintenance | <1% |
| Vendor factors—Faulty vendor configuration recommendation | <1% |
| Interactions with other (non-health IT) care systems | <1% |
| Vendor factors—Non-configurable software | <1% |
| Local implementation—Inadequate control of user access | <1% |
| Local implementation—Inadequate local testing | <1% |

## APPENDIX F

LICENSE FOR FIGURE 2



**BMJ PUBLISHING GROUP LTD. LICENSE TERMS AND CONDITIONS**

Jul 07, 2014

This is a License Agreement between Gerard M Castro ("You") and BMJ Publishing Group Ltd. ("BMJ Publishing Group Ltd.") provided by Copyright Clearance Center ("CCC"). The license consists of your order details, the terms and conditions provided by BMJ Publishing Group Ltd., and the payment terms and conditions.

**All payments must be made in full to CCC. For payment instructions, please see information listed at the bottom of this form.**

| | |
|---|---|
| License Number | 3423750420942 |
| License date | Jul 07, 2014 |
| Licensed content publisher | BMJ Publishing Group Ltd. |
| Licensed content publication | The BMJ |
| Licensed content title | Human error: models and management |
| Licensed content author | James Reason |
| Licensed content date | Mar 18, 2000 |
| Volume number | 320 |
| Type of Use | Dissertation/Thesis |
| Requestor type | Individual |
| Format | Electronic |
| Portion | Figure/table/extract |
| Number of figure/table/extracts | 1 |
| Description of figure/table/extracts | The Swiss cheese model of how defences, barriers, and safeguards may be penetrated by an accident trajectory |
| Will you be translating? | No |
| Circulation/distribution | 1 |
| Title of your thesis / dissertation | Classification of Health Information Technology-Related Contributing Factors to Patient Safety Events |
| Expected completion date | Aug 2014 |
| Estimated size(pages) | 107 |
| BMJ VAT number | 674738491 |
| Billing Type | Invoice |
| Billing address | 1009 South Butternut Circle<br>FRANKFORT, IL 60423<br>United States |

**APPENDIX F (continued)**

## APPENDIX F (continued)

LICENSE FOR FIGURE 3

## APPENDIX F (continued)

LICENSE FOR FIGURE 8, APPENDIX A

## LITERATURE CITED


Agency for Healthcare Research and Quality. (n.d.). AHRQ patient safety network—glossary. Retrieved, 2011, Retrieved from http://www.psnet.ahrq.gov/glossary.aspx?indexLetter=P

Agency for Healthcare Research and Quality. (2013). AHRQ common formats—version 1.2: Event descriptions, sample reports, and forms. Retrieved, 2013, Retrieved from https://www.psoppc.org/web/patientsafety/version-1.2_documents#Supply

Anderson, J. G., Ramanujam, R., Hensel, D., Anderson, M. M., & Sirio, C. A. (2006). The need for organizational change in patient safety initiatives. *International Journal of Medical Informatics, 75*(12), 809–817. doi:10.1016/j.ijmedinf.2006.05.043

Ash, J. S., Sittig, D. F., Dykstra, R. H., Guappone, K., Carpenter, J. D., & Seshadri, V. (2007). Categorizing the unintended sociotechnical consequences of computerized provider order entry. *International Journal of Medical Informatics, 76 Suppl 1*, S21–7. doi:10.1016/j.ijmedinf.2006.05.017

Aspden, P., Corrigan, J., Wolcott, J., & Erickson, S. (Eds.). (2004). *Patient safety: Achieving a new standard for care*. Washington, DC: National Academies Press.

B&W Pantex—U.S. Department of Energy. (2008). *Causal factors analysis: An approach for organizational learning*. Washington, DC: US Government Printing Office.

Carayon, P., Schoofs Hundt, A., Karsh, B. T., Gurses, A. P., Alvarado, C. J., Smith, M., & Flatley, Brennan, P. (2006). Work system design for patient safety: The SEIPS model. *Quality & Safety in Health Care, 15 Suppl 1*, i50–8. doi:15/suppl_1/i50 [pii]

Centers for Medicare and Medicaid Services. (2014). 2014 definition stage 1 of meaningful use—centers for Medicare & Medicaid services. Retrieved, 2014, Retrieved from http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html

Chassin, M. R., & Loeb, J. M. (2011). The ongoing quality improvement journey: Next stop, high reliability. *Health Affairs (Project Hope), 30*(4), 559–568. doi:10.1377/hlthaff.2011.0076 [doi]

Chassin, M. R., & Loeb, J. M. (2013). High-reliability health care: Getting there from here. *The Milbank Quarterly, 91*(3), 459–490. doi:10.1111/1468–0009.12023 [doi]

Chuo, J., & Hicks, R. W. (2008). Computer-related medication errors in neonatal intensive care units. *Clinics in Perinatology, 35*(1), 119–39, ix. doi:10.1016/j.clp.2007.11.005 [doi]

## LITERATURE CITED (continued)


Classen, D., Bates, D. W., & Denham, C. R. (2010). Meaningful use of computerized prescriber order entry. *Journal of Patient Safety, 6*(1), 15–23. doi:10.1097/PTS.0b013e3181d108db; 10.1097/PTS.0b013e3181d108db

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

Cummings, T., & Srivastva, S. (1977). *Management of work: A sociotechnical systems approach*. Kent, OH: Comparative Administration Research Institute: Distributed by Kent State University Press.

ECRI Institute PSO. (2012). *ECRI instiitute PSO deep dive: Health information technology.*

Federal food, drug, and cosmetic act of 1938, 21 U.S.C. § 321[h].

Food and Drug Administration. (2014a). *FDASIA health IT report: Proposed strategy and recommendations for a risk-based framework.*

Food and Drug Administration. (2014b). MAUDE—manufacturer and user facility device experience. Retrieved, 2014, Retrieved from http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm

Gandhi, T. K., Graydon-Baker, E., Huber, C. N., Whittemore, A. D., & Gustafson, M. (2005). Closing the loop: Follow-up and feedback in a patient safety program. *Joint Commission Journal on Quality and Patient Safety / Joint Commission Resources, 31*(11), 614–621.

Haimes, Y. Y. (2009). *Risk modeling, assessment, and management [electronic resource]* (3rd ed.). Hoboken, NJ: John Wiley & Sons.

Harrison, M. I. (2005). *Diagnosing organizations: Methods, models, and processes* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Harrison, M. I., Henriksen, K., & Hughes, R. G. (2007). Improving the health care work environment: A sociotechnical systems approach. *Joint Commission Journal on Quality and Patient Safety / Joint Commission Resources, 33*(11 Suppl), 3–6, 1.

Harrison, M. I., Koppel, R., & Bar-Lev, S. (2007). Unintended consequences of information technologies in health care—An interactive sociotechnical analysis. *Journal of the American Medical Informatics Association : JAMIA, 14*(5), 542–549. doi:10.1197/jamia.M2384

## LITERATURE CITED (continued)


Health insurance portability and accountability act of 1996, § 1320d–9.

Henriksen, K., Kaye, R., & Morisseau, D. (1993). Industrial ergonomic factors in the radiation oncology therapy environment. In R. Nielsen, & K. Jorgensen (Eds.), *Advances in industrial ergonomics and safety* (pp. 325–335)

Hripcsak, G. (1993). Monitoring the monitor: Automated statistical tracking of a clinical event monitor. *Computers and Biomedical Research, an International Journal, 26*(5), 449–466. doi:S0010480983710323 [pii]

Joint Commission on Accreditation of Healthcare Organizations, USA. (2008). *Safely implementing health information and converging technologies.* (No. 42).

Leotsakos, A., Zheng, H., Croteau, R., Loeb, J. M., Sherman, H., Hoffman, C., . . . Munier, B. (2014). Standardization in patient safety: The WHO high 5s project. *International Journal for Quality in Health Care : Journal of the International Society for Quality in Health Care / ISQua, 26*(2), 109–116. doi:10.1093/intqhc/mzu010 [doi]

Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E. (2010). An analysis of computer-related patient safety incidents to inform the development of a classification. *Journal of the American Medical Informatics Association : JAMIA, 17*(6), 663–670. doi:10.1136/jamia.2009.002444 [doi]

Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E. (2012). Using FDA reports to inform a classification for health information technology safety problems. *Journal of the American Medical Informatics Association : JAMIA, 19*(1), 45–53. doi:10.1136/amiajnl–2011–000369 [doi]

Meeks, D. W., Smith, M. W., Taylor, L., Sittig, D. F., Scott, J. M., & Singh, H. (2014). An analysis of electronic health record-related patient safety concerns. *Journal of the American Medical Informatics Association : JAMIA,* doi:amiajnl–2013–002578 [pii]

Myers, R. B., Jones, S. L., & Sittig, D. F. (2011). Review of reported clinical information system adverse events in US Food and Drug Administration databases. *Applied Clinical Informatics, 2*(1), 63–74. doi:10.4338/ACI–2010–11–RA–0064 [doi]

Office of the National Coordinator for Health Information Technology. (2009a). Health IT rules and regulations. Retrieved, 2014, Retrieved from http://www.healthit.gov/policy-researchers-implementers/health-it-legislation-and-regulations

## LITERATURE CITED (continued)


Office of the National Coordinator for Health Information Technology. (2009b). What is an electronic health record (EHR)? Retrieved, 2014, Retrieved from http://www.healthit.gov/providers-professionals/faqs/what-electronic-health-record-ehr

Office of the National Coordinator for Health Information Technology. (2014). Health IT patient safety action and surveillance plan. Retrieved, 2014, Retrieved from http://www.healthit.gov/sites/default/files/safety_plan_master.pdf

Payne, T. H., Bates, D. W., Berner, E. S., Bernstam, E. V., Covvey, H. D., Frisse, M. E., . . . Ozbolt, J. (2013). Healthcare information technology and economics. *Journal of the American Medical Informatics Association : JAMIA, 20*(2), 212–217. doi:10.1136/amiajnl–2012–000821 [doi]

Pennsylvania Patient Safety Authority. (n.d.). Who we are. Retrieved, 2014, Retrieved from http://patientsafetyauthority.org/NewsAndInformation/Brochures/Documents/Who_We_Are_Update.pdf

Reason, J. (1990). *Human error*. New York, NY: Cambridge University Press.

Reason, J. (2000a). *Managing the risks of organizational accidents.* Burlington, VT: Ashgate Publishing.

Reason, J. (1997). *Managing the risks of organizational accidents.* Burlington, VT: Ashgate.

Reason, J. (2000b). Human error: Models and management. *BMJ (Clinical Research Ed.), 320*(7237), 768–770.

Rector, A. L. (1999). Clinical terminology: Why is it so hard? *Methods of Information in Medicine, 38*(4–5), 239–252. doi:10.1267/METH99040239 [doi]

Runciman, W., Hibbert, P., Thomson, R., Van Der Schaaf, T., Sherman, H., & Lewalle, P. (2009). Towards an international classification for patient safety: Key concepts and terms. *International Journal for Quality in Health Care : Journal of the International Society for Quality in Health Care / ISQua, 21*(1), 18–26. doi:10.1093/intqhc/mzn057 [doi]

Santell, J. P., Kowiatek, J. G., Weber, R. J., Hicks, R. W., & Sirio, C. A. (2009). Medication errors resulting from computer entry by nonprescribers. *American Journal of Health-System Pharmacy : AJHP : Official Journal of the American Society of Health-System Pharmacists, 66*(9), 843–853. doi:10.2146/ajhp080208 [doi]

## LITERATURE CITED (continued)


Shadish, W., Cook, T., & Campbell, D. (2001). *Experimental and quasi-experimental designs for generalized causal inference*. Boston, MA: Houghton Mifflin.

Singh, H., Classen, D., & Sittig, D. (2011). Creating an oversight infrastructure for electronic health record-related patient safety hazards. *Journal of Patient Safety, 7*(4), 169–174. doi:10.1097/PTS.0b013e31823d8df0 [doi]

Sittig, D. F., & Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *Quality & Safety in Health Care, 19 Suppl 3*, i68–74. doi:10.1136/qshc.2010.042085 [doi]

Sittig, D. F., & Singh, H. (2012). Electronic health records and national patient-safety goals. *The New England Journal of Medicine, 367*(19), 1854–1860. doi:10.1056/NEJMsb1205420 [doi]

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

Suydam, S., Liang, B. A., Anderson, S., & Weinger, M. B. (2005). Patient safety data sharing and Protection from legal discovery. In K. Henriksen, J. B. Battles, E. S. Marks & D. I. Lewin (Eds.), *Advances in patient safety: From research to implementation (Volume 3: Implementation issues)* (pp. 361–370). Rockville, MD: Agency for Healthcare Research and Quality (US).

The Joint Commission. (2013). Framework for conducting a root cause analysis and action plan. Retrieved, 2014, Retrieved from http://www.jointcommission.org/assets/1/6/RCA_Questions_Framework.docx

The Joint Commission. (2014a). *2014 hospital accreditation standards*. Oakbrook Terrace, IL.: Joint Commission Resources.

The Joint Commission. (2014b). Summary data of sentinel events reviewed by The Joint Commission. Retrieved, 2014, Retrieved from http://www.jointcommission.org/assets/1/18/2004_to_2Q_2013_SE_Stats_-_Summary.pdf

Thomson, R., Lewalle, P., Sherman, H., Hibbert, P., Runciman, W., & Castro, G. (2009). Towards an international classification for patient safety: A delphi survey. *International Journal for Quality in Health Care : Journal of the International Society for Quality in Health Care / ISQua, 21*(1), 9–17. doi:10.1093/intqhc/mzn055 [doi]

Trochim, W., & Donnelly, J. (2008). *Research methods knowledge base*. Mason, OH: Atomic Dog/Cengage Learning.

## LITERATURE CITED (continued)

US Department of Veterans Affairs, & Veterans Health Administration. (2011). *VHA national patient safety improvement handbook.* (No. VHA HANDBOOK 1050.01).

Vincent, C., Taylor-Adams, S., & Stanhope, N. (1998). Framework for analysing risk and safety in clinical medicine. *BMJ (Clinical Research Ed.), 316*(7138), 1154–1157.

Walker, J., Hassol, A., Bradshaw, B., & Rezaee, M. (May 2012). *Health IT hazard manager beta-test: Final report. (prepared by ABT Associates and Geisinger Health System, under contract no. HHSA290200600011i, #14).* Rockville, MD: Agency for Healthcare Research and Quality.

Walsh, K. E., Adams, W. G., Bauchner, H., Vinci, R. J., Chessare, J. B., Cooper, M. R., . . . Landrigan, C. P. (2006). Medication errors related to computerized order entry for children. *Pediatrics, 118*(5), 1872–1879. doi:118/5/1872 [pii]

World Alliance for Patient Safety Drafting Group, Sherman, H., Castro, G., Fletcher, M., World Alliance for Patient Safety, Hatlie, M., . . . Virtanen, M. (2009). Towards an international classification for patient safety: The conceptual framework. *International Journal for Quality in Health Care : Journal of the International Society for Quality in Health Care / ISQua, 21*(1), 2–8. doi:10.1093/intqhc/mzn054 [doi]

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

Wu, A. W., Lipshutz, A. K., & Pronovost, P. J. (2008). Effectiveness and efficiency of root cause analysis in medicine. *JAMA : The Journal of the American Medical Association, 299*(6), 685–687. doi:10.1001/jama.299.6.685

Zhan, C., Hicks, R. W., Blanchette, C. M., Keyes, M. A., & Cousins, D. D. (2006). Potential benefits and problems with computerized prescriber order entry: Analysis of a voluntary medication error-reporting database. *American Journal of Health-System Pharmacy : AJHP : Official Journal of the American Society of Health-System Pharmacists, 63*(4), 353–358. doi:63/4/353 [pii]

## VITA

Gerard M. Castro
1009 South Butternut Circle
Frankfort, Illinois 60423
(708) 267-0617

***Education:***

| | | | |
|---|---|---|---|
| University of Illinois at Chicago | MPH | 2000 | Health Policy and Administration |
| Loyola University Chicago | BS | 1996 | Major—Biology<br>Minor—Psychology and Chemistry |

**Publications:**

**Castro, G.** (2009a). National patient safety goals. In R. Mullner (Ed.), *Encyclopedia of health services research* (pp. 840–2). Los Angeles, CA: Sage.

**Castro, G.** (2009b). National quality forum. In R. Mullner (Ed.), *Encyclopedia of health services research* (pp. 844–7). Los Angeles, CA: Sage.

Sherman, H., Koss, R., **Castro, G.**, & Loeb, J. (2009). From the abstract to the concrete: The conceptual framework for the international classification for patient safety. In R. Mullner (Ed.), *Encyclopedia of health services* (pp. 650–4). Los Angeles, CA: Sage.

Thomson, R., Lewalle, P., Sherman, H., Hibbert, P., Runciman, W., & **Castro, G.** (2009). Towards an international classification for patient safety: A delphi survey. *International Journal for Quality in Health Care : Journal of the International Society for Quality in Health Care / ISQua, 21*(1), 9–17. doi:10.1093/intqhc/mzn055 [doi]

World Alliance for Patient Safety Drafting Group, Sherman, H., **Castro, G.**, Fletcher, M., World Alliance for Patient Safety, Hatlie, M., . . . Virtanen, M. (2009). Towards an international classification for patient safety: The conceptual framework. *International Journal for Quality in Health Care : Journal of the International Society for Quality in Health Care / ISQua, 21*(1), 2–8. doi:10.1093/intqhc/mzn054 [doi]

Fletcher, M., Jakob, R., Koss, R., Lewalle, P., Loeb, J., Perneger, T., **Castro, G**. . . . Hatlie, M. (2007). *Report on the web-based modified delphi survey of the international classification for patient safety.* Geneva, Switzerland: World Health Organization.

Sherman, H., **Castro, G**., & Loeb, J. (2006). *Comparison glossary of patient safety terms.* Geneva, Switzerland: World Health Organization.

Bondmass, M., Bolger, N., **Castro, G**., & Avitall, B. (2000a). The effect of home monitoring and telemanagement on blood pressure control among African Americans. *Telemedicine Journal,* (6), 12–23.

Bondmass, M., Bolger, N., **Castro, G**., & Avitall, B. (2000b). The effect of physiologic home monitoring and telemanagement on chronic heart failure outcomes. *The Internet Journal of Advanced Nursing Practice* 2000; Vol3N2: http://www.ispub.com/journals/IJANP/Vol3N2/chf.htm*, 3*(2). Published March 27, 2000.

**Abstracts/Presentations:**

Castro, G., Flack, M.N., Sparnon S. (2014, May). Health IT Safety Issues. Presented at AAMI 2014 Conference and Expo, Philadelphia, PA.

**Castro, G.** (2014, March). *Patient Safety Initiatives at The Joint Commission*. Presented at HFES 2014 International Symposium on Human Factors and Ergonomics in Health Care: Leading the Way, Chicago, IL.

**Castro, G.**, Jaffe**,** R., Reider, J. (2014, February). *Strategizing for Health IT Safety Surveillance and Response*. Presented at the HIMSS 14 Annual Conference and Exhibition, Orlando, FL.

**Castro, G.** (2013, May). *Get Ready! The Joint Commission's Proposed 2014 National Patient Safety Goal—What Your Hospital Can Do to Prepare Now*. Presented at 15th Annual National Patient Safety Foundation Congress, New Orleans, LA.

**Castro, G.**, Chang, A., Champagne, S., Loeb, J. (2005, October). *Identifying Clinical, Financial, and Organizational Domains that Determine the Value of Patient Safety Taxonomy and Ontology*. Presented at 22nd ISQua International Conference, Vancouver, BC Canada.

Chang, A., **Castro, G.**, Champagne, S., Loeb, J. (2005, October). *Representation of patient safety data by clinical coding systems: Adequacy of combined controlled medical vocabularies*. Presented at 22nd ISQua International Conference, Vancouver, BC Canada.

Divi, C., Chang, A., **Castro, G.**, Croteau, R., Loeb, J. (2005, October). *Language Barriers: Implications for Patient Safety Research*. Presented at 22nd ISQua International Conference, Vancouver, BC Canada.

Fan, L., Boenning, D., **Castro, G.**, Loeb, J., Chang, A. (2005, October). *Building a Hospital Incident Reporting Ontology (HIRO) in the Web Ontology Language (OWL) using the JCAHO Patient Safety Event Taxonomy (PSET).* Presented at AMIA 2005 Annual Symposium, Washington, DC.

Chang, A., **Castro, G.**, Shearer, A., Frazier, P. (2005, June). *Comparison of SNOMED-CT, Clinical LOINC, and ICD-CM coverage of patient safety terms and concepts*. Presented at Academy Health Annual Research Meeting, Boston, MA.

**Castro, G**. (2002, January). *Defining a model program*. Presented at Recognition and Prevention of Biological and Chemical Incidents: A Systems Approach at University of Illinois at Chicago, Chicago, IL.

Avitall, B., Bondmass, M., Bolger, N., Panella, M., Konhilas, J., **Castro, G**. (1997, April). *The effect of transtelephonic monitoring and telemanagement on preventing hospital admissions and improving quality of life in heart failure patents*. Presented at 4th International Symposium on Multiple Risk Factors in Cardiovascular Disease: Strategies of Prevention of Coronary Heart disease, Cardiac Failure, and Stroke, Washington, DC.

Bondmass, M., Bolger, N., **Castro, G.**, Avitall, B. (1997, September). *Does gender and race influence quality of life in heart failure patients*? Presented at First Annual Scientific Meeting—Heart Failure Society of America, Baltimore, MD.

Bondmass, M., Bolger, N., **Castro, G.,** Panella, M., Konhilas, J., Avitall, B. (1997, September). *Objective transtelephonic transmission of physiologic data with an automatic alarm system provides safe and highly efficient heart failure telemanagement and reduces hospital admissions*. Presented at First Annual Scientific Meeting—Heart Failure Society of America, Baltimore, MD.

Bondmass , M., Bolger, N., Avitall, B., **Castro, G.**, Panella, M., Konhilas, J. (1997). Objective transtelephonic transmission of physiologic data with and automatic alarm system provides safe and highly efficient heart failure telemanagement and reduces hospital readmissions. In *Circulation*, *Suppl*., 96(8).

Bondmass, M., Bolger, N., **Castro, G.,** Avitall, B. (1998). Early weight gain intervention requires less drugs to decrease heart failure readmissions. In *Journal of the American College of Cardiology*, *Suppl*., 31(2).

**Reviewer:**

The Joint Commission. (2013). *Certified Joint Commission Professional Exam Preparation Workbook*. Joint Commission Resources: Oakbrook Terrace, IL.

Wu, A.W., ed. (2011). *The Value of Close Calls in Improving Patient Safety: Learning How to Avoid and Mitigate Patient Harm*. Joint Commission Resources: Oakbrook Terrace, IL.

Croteau, R.J., ed. (2010). *Root Cause Analysis in Healthcare: Tools and Techniques* (4th Edition). Joint Commission Resources: Oakbrook Terrace, IL.

The Joint Commission. (2010). *Staff Education Tools for the 2010 National Patient Safety Goals*. Joint Commission Resources: Oakbrook Terrace, IL.

The Joint Commission. (2009). *Patient Safety Pocket Guide* (2nd Edition). Joint Commission Resources: Oakbrook Terrace, IL.

The Joint Commission. (2009). *Staff Education Tools for the National Patient Safety Goals*. Joint Commission Resources: Oakbrook Terrace, IL.

ECRI Institute. (2009). Fixing Bad Links: Preventing Misconnection in Your Hospital. *Health Devices*, 31(7), 220–3.

**Committee Service:**
National Quality Forum, Common Format Expert Panel—Member, 2011–present

Association for the Advancement of Medical Instrumentation, Coalition of Organizations for Reporting Adverse Events—Member, 2013–present

**Certifications:**
Experis Professional Development—Agile Training for the Joint Commission, 2014

The Joint Commission—Certified Green Belt, 2013

**Awards:**
Village of Oak Park, Fitzsimmons Award for Excellence in Public Health—April 2006

**Continuing Education:**
Mid-America Regional Public Health Leadership Institute, 2003–2004: Preparedness and the Future of the Public's Health. Fellow, 2003–2004

University of Illinois at Chicago Human Subject Protections Program, Initial Education, August 8, 2003

***Professional Service:***

| | |
|---|---|
| 2004–present | The Joint Commission<br>Project Director, Patient Safety Initiatives |
| 2000–2004 | Oak Park Department of Public Health<br>Health Information Coordinator |
| 2000–2002 | Physicians for a National Health Program<br>Webmaster/Consultant |
| 1999–2000 | Circle Family Care<br>Public Health Field Practicum (part-time) |
| 1996–2000 | University of Illinois at Chicago<br>Biomedical Technician/Research Information Specialist |