OPEN ACCESS

An analysis of electronic health record-related patient safety concerns

Derek W Meeks,[1,2] Michael W Smith,[1,3] Lesley Taylor,[4] Dean F Sittig,[5] Jean M Scott,[4] Hardeep Singh[1,3]

[1]Houston VA Center for Innovations in Quality, Effectiveness and Safety, Michael E DeBakey Veterans Affairs Medical Center, Houston, Texas, USA
[2]Department of Family and Community Medicine, Baylor College of Medicine, Houston, Texas, USA
[3]Section of Health Services Research, Department of Medicine, Baylor College of Medicine, Houston, Texas, USA
[4]Informatics Patient Safety, Office of Informatics and Analytics, Veterans Health Administration, Ann Arbor, MI and Albany, NY, USA
[5]University of Texas School of Biomedical Informatics and UT-Memorial Hermann Center for Healthcare Quality and Safety, Houston, Texas, USA

Correspondence to
Dr Hardeep Singh, Houston VA Center for Innovations in Quality, Effectiveness and Safety (152), 2002 Holcombe Boulevard, Houston, TX 77030, USA; hardeeps@bcm.edu

ABSTRACT

Objective A recent Institute of Medicine report called for attention to safety issues related to electronic health records (EHRs). We analyzed EHR-related safety concerns reported within a large, integrated healthcare system.
Methods The Informatics Patient Safety Office of the Veterans Health Administration (VA) maintains a non-punitive, voluntary reporting system to collect and investigate EHR-related safety concerns (ie, adverse events, potential events, and near misses). We analyzed completed investigations using an eight-dimension sociotechnical conceptual model that accounted for both technical and non-technical dimensions of safety. Using the framework analysis approach to qualitative data, we identified emergent and recurring safety concerns common to multiple reports.
Results We extracted 100 consecutive, unique, closed investigations between August 2009 and May 2013 from 344 reported incidents. Seventy-four involved unsafe technology and 25 involved unsafe use of technology. A majority (70%) involved two or more model dimensions. Most often, non-technical dimensions such as workflow, policies, and personnel interacted in a complex fashion with technical dimensions such as software/hardware, content, and user interface to produce safety concerns. Most (94%) safety concerns related to either unmet data-display needs in the EHR (ie, displayed information available to the end user failed to reduce uncertainty or led to increased potential for patient harm), software upgrades or modifications, data transmission between components of the EHR, or 'hidden dependencies' within the EHR.
Discussion EHR-related safety concerns involving both unsafe technology and unsafe use of technology persist long after 'go-live' and despite the sophisticated EHR infrastructure represented in our data source. Currently, few healthcare institutions have reporting and analysis capabilities similar to the VA.
Conclusions Because EHR-related safety concerns have complex sociotechnical origins, institutions with long-standing as well as recent EHR implementations should build a robust infrastructure to monitor and learn from them.

BACKGROUND AND SIGNIFICANCE

Investments in health information technology (HIT) can enhance the safety and efficiency of patient care and enable knowledge discovery.[1] However, emerging evidence suggests that HIT may cause new patient safety concerns and other unintended consequences due to usability issues, disruptions of clinical processes, and unsafe work-arounds to circumvent technology-related constraints.[2–16] In particular, rapid adoption of electronic health records (EHRs) has revealed potential safety concerns related to EHR design, implementation, and use.[12 17–21] Patient safety concerns are broadly defined as adverse events that reached the patient, near misses that did not reach the patient, or unsafe conditions that increase the likelihood of a safety event.[22 23] Detecting and preventing EHR-related safety concerns is challenging because concerns are often multifaceted, involving not only potentially unsafe technological features of the EHR but also EHR user behaviors, organizational characteristics, and rules and regulations that guide EHR-related activities. Thus, comprehensive and newer 'sociotechnical' approaches that account for these elements are required to address the complexities of EHR-related patient safety.[24–27]

Despite a clear need to define and understand EHR-related safety concerns,[28] data that describe the nature and magnitude of these concerns are scarce. A few studies have attempted to quantify and classify EHR-related safety concerns by mining patient safety incident reporting databases.[18 29–31] In addition, conceptual frameworks or models have been developed to incorporate the breadth of technical and non-technical factors into the analysis of EHR safety and effectiveness.[21 25 27 32 33] For instance, we previously developed a sociotechnical model that proposes eight interdependent dimensions that are essential to understand EHR-related safety (table 1; Sittig and Singh model).[24 34] The model accounts for the complexities of technology, its users, the involved workflow, and the larger external or organizational policies and context in assessment of EHR-related safety concerns.[35 36]

We conducted a qualitative 'sociotechnical analysis' of completed EHR-related safety investigations based on voluntary reports collected within a large, integrated healthcare system. Using Sittig and Singh's sociotechnical model as a guiding framework, our aim was to describe common EHR-related safety concerns and understand the nature and context of these safety concerns in order to build a foundation for future work in this area.

METHODS
Design and setting
We performed a retrospective analysis of completed investigation reports about EHR-related safety concerns from healthcare facilities within the Department of Veterans Affairs (VA). The VA operates the largest integrated healthcare system in the USA with over 1700 sites of care (eg, hospitals, clinics, community living centers, domiciliaries, readjustment counseling centers).[37] A comprehensive EHR, nationally mandated in 1999, is used at

Table 1 EHR-related safety concerns categorized by sociotechnical dimensions and phases of EHR implementation and use

Sociotechnical dimension	Phase 1 (n=74)	Phase 2 (n=25)	Phase 3 (n=1)	Total
Hardware and software: the computing infrastructure used to power, support, and operate clinical applications and devices	67	9	0	76
Clinical content: the text, numeric data, and images that constitute the 'language' of clinical applications	22	15	1	38
Human-computer interface: all aspects of technology that users can see, touch, or hear as they interact with it	16	12	1	29
People: everyone who interacts in some way with technology, including developers, users, IT personnel, and informaticians	5	15	0	20
Workflow and communication: processes to ensure that patient care is carried out effectively	24	11	0	35
Internal organizational features: policies, procedures, work environment, and culture	4	2	0	6
External rules and regulations: federal or state rules that facilitate or constrain preceding dimensions	1	1	0	2
System measurement and monitoring: processes to evaluate both intended and unintended consequences of health IT implementation and use	1	0	0	1

Phase 1, unsafe technology or technology failures; phase 2, unsafe or inappropriate use of technology; phase 3, lack of monitoring of safety concerns.
EHR, electronic health record; IT, information technology.

all its facilities to provide care to approximately 8.3 million Veterans.[38] The VA is considered a leader in the design, development, and use of EHRs to address healthcare quality.[39–41] The established EHR infrastructure comprises internally developed and commercially procured systems that provide a range of applications (eg, laboratory, pharmacy, radiology, patient record, scheduling, registration, billing). VA facilities have the ability to partially customize the available administrative, financial, and clinical applications to match local processes and practice conditions, while the core functionality is centrally updated and distributed. In conjunction with other patient safety initiatives such as sentinel event monitoring, root cause analysis, and proactive risk assessment, the VA created an Informatics Patient Safety (IPS) Office in 2005 to establish a mechanism for non-punitive, voluntary reporting of EHR-related safety concerns.

The IPS reporting system, which includes only health IT-related reports, is the foundation for a rigorous approach that includes not only incident investigation and analysis, but also feedback to reporters and developers of solutions to mitigate future risks to patients. Clinical or administrative EHR users along with EHR developers can report EHR-related patient safety concerns through an intranet website or by using the national VA IT helpdesk system. The most common process for clinical users to report a safety concern is by notification of local IT staff. The local IT staff investigates the safety concern, determines if national support is needed, and reports the incident to the helpdesk. At the national level, if the incident is related to patient safety, an initial IPS report (see supplementary online Appendix A) is populated with the initial reporter's contact information, the description of the incident, the applications in use at the time of the incident, any harm or potential for harm, and any known corrective actions. IPS analysts with healthcare, safety, and informatics training along with human factors specialists investigate reports; on average, it takes about 30 days per incident for such an investigation. The goals of investigation are to understand system states and user actions preceding the safety concern, identifying the underlying root causes, and, if possible, safely replicating the incident with 'test' patients in the 'live' EHR system. At a minimum, an account of the incident is elicited from the person who detects it and this description is further reviewed by an IPS analyst and a human factors specialist. In addition to reviewing logs of EHR applications and discussing the case with technical specialists, the IPS team attempts to replicate the safety concern in the EHR by recreating the circumstances of the reported incident. The

reports are analyzed and scored according to potential severity, frequency, and detectability (see supplemental online Appendix B). The score provides a safety assessment and guides development of the solution action plan. A solution for 'low score' incidents, although not mandatory, may be considered depending on available resources; for 'intermediate score' incidents, a solution such as training or request for software modification is mandatory; for 'high score' incidents, an immediate action, such as a software patch or safety notice to affected users, is required. After analysis, the IPS makes recommendations to software developers, individual medical facilities, or other relevant stakeholders within the VA healthcare system to mitigate the risk of error or harm.[42] Investigation-related information is maintained in a database and tracked until the investigation is 'closed.' The final closed investigation for each report contains a narrative of the reported incident, the details of the investigation conducted by IPS and IT staff, and any solution that might have been identified. Thus, a completed investigation provides additional contextual details pertinent to the incident under study as compared with traditional event reports.

Data collection
We searched the IPS database for closed investigations that contained full analyses and narratives that provided meaningful information, excluding duplicate entries. We also excluded safety concerns related to erroneous editing or merging of patient records resulting in comingled or overlaid records. Although these are known safety concerns,[43] they were excluded because they are not routinely analyzed by IPS and are handled primarily by a separate office in the VA. We extracted 100 consecutive records that met our search criteria. An example is provided online as supplemental Appendix C. Previous exploratory studies in patient safety have been able to shed powerful light on contributory factors with a similar sample size.[44] Given the rich nature of the qualitative data, we believed this number was both valuable and feasible.

Data analysis
We analyzed narrative data in the completed investigation reports using the framework analysis method which allows emerging themes to be incorporated into a previously established framework.[45–47] Framework analysis consists of five stages: familiarization, thematic analysis, indexing, charting, and mapping and interpretation. First, two authors (DWM and MWS) independently reviewed and summarized the

investigation reports to become familiar with the data, but at this secondary stage of analysis, we made no further effort to replicate the safety concern or investigation, determine additional causes, or offer additional solutions. Thematic analysis was guided primarily by the application of the eight-dimension sociotechnical model. A coding scheme was created so that each concern could be described and indexed according to one or more sociotechnical dimensions that underlay or contributed to the safety concern. Additionally, we categorized concerns by 'phases' of safety related to EHR implementation and use: concerns related to inherently unsafe technology or technology failures ('phase 1'), concerns related to unsafe or inappropriate use of technology ('phase 2'), and concerns related to lack of using technology to monitor for potential safety concerns before harm occurs ('phase 3').[48]

Our coding scheme allowed a safety concern to be classified in multiple dimensions from the sociotechnical model but in only one of the EHR safety phases. When more than one sociotechnical dimension was involved in a safety incident, we noted this interaction by counting co-occurring dimensions. The two coding authors (ie, a physician with informatics training and a human factors engineer) independently indexed each safety concern after reviewing the results of the IPS investigation. Discrepancies in coding were then resolved by consensus. The emergent safety concerns were generated via collaborative, iterative analysis of the whole set of coding results. This included rereading and rearranging the data (charting) to allow groupings of reports that represented a common theme. Members of our multidisciplinary project team, whose areas of expertise included clinical medicine, patient safety, informatics, human factors, and information technology, provided guidance on the content of the themes. Finally, emergent and recurring safety concerns were identified and described (mapping and interpretation) according to their sociotechnical origins and EHR safety phase. We do not report inter-rater reliability because the aim of the study was to describe the nature and context of common EHR-related safety concerns, not solely classification according to the sociotechnical models.[47 49]

We used the software package Atlas.ti V.6.2 to facilitate coding of the investigation narratives, and Microsoft Excel to arrange and structure the data.

RESULTS
We extracted 100 consecutive, unique, closed investigations between August 2009 and May 2013 from 344 reported incidents. The selected incidents were reported from 55 unique VA facilities. On the IPS-assessed safety scores, 48 investigations were scored low, 38 intermediate, and 14 were scored high. Table 1 summarizes our analysis of the safety concerns along the sociotechnical model's dimensions and EHR safety phases. Approximately three-quarters of safety concerns were categorized as phase 1 (ie, concerns related to unsafe technology). Sociotechnical dimensions of phase 1 concerns most commonly involved hardware and software, workflow and communication, and clinical content. One-quarter were classified as phase 2 (ie, unsafe EHR use) and most commonly involved the dimensions of people, clinical content, workflow and communication, and human–computer interface. Only one safety concern involving phase 3 (ie, failure to use the EHR to monitor patient safety) was represented in our analysis. Incidents frequently reflected occurrence of more than one sociotechnical dimension: 40 incidents were classified with two sociotechnical dimensions, 23 incidents had three, and seven involved four dimensions.

During charting, mapping, and interpretation of the interactions of social and technical components of EHR use, several distinct (although not mutually exclusive) safety concerns emerged. We classified these concerns into four types: unmet display needs in the EHR, safety concerns with software modifications or upgrades, concerns related to data transmission at system–system interfaces, and concerns of 'hidden dependencies' in distributed systems (ie, when one EHR component unexpectedly or unknowingly is affected by the state or condition of another). Table 2 provides definitions and examples of these four types of concerns, which accounted for 94% of the incidents analyzed. All four types of safety concerns affected, or had the potential to affect, multiple patients, although we did not further analyze outcome data except as noted below.

Concerns related to unmet data display needs in the EHR
Unmet display needs was the most common type of concern observed (36 incidents). This category represented a pattern of incidents in which human–EHR interaction processes did not adequately support the tasks of the end users. These incidents reflected a poor fit between information needs and the task at hand, the nature of the content being presented (eg, patient-specific information requiring action, such as drug-allergy warnings or information required for successful order entry), and the way the information was displayed. As a result of this poor fit, the displayed information available to the end user failed to reduce uncertainty or led to increased potential for patient harm.

As an example, one incident described a situation in which a patient was administered a dose of a diuretic that exceeded the prescribed amount. This error occurred due to a number of interacting sociotechnical factors. First, a pharmacist made a data entry error while approving the order for a larger-than-usual amount of diuretic. Although a dose error warning appeared on order entry, this particular warning was known to have a high false positive rate. Owing to diminished user confidence in the warning's reliability, the warning was over-ridden. The over-ride released the incorrect dose for administration by nursing staff. The nurse, unaware of the discrepancy between the prescribed amount and the amount approved by the pharmacist, administered the larger dose. This example highlights complex interactions between the hardware and software, human–computer interface, people, and workflow and communication dimensions, which served to either prevent or obscure the users' receipt of appropriate information. Across the 36 concerns within this concern type, the contributory dimensions were hardware and software (22 incidents), human–computer interface (22 incidents), workflow and communication (10 incidents), clinical content (9 incidents), people (9 incidents), organizational policies and procedures (2 incidents), and system measurement and monitoring (1 incident). Most (22 of 36) of these concerns were classified as phase 1 issues, followed by 13 phase 2, and one phase 3.

Concerns related to both intended and unintended software modifications
The second most common concern type involved upgrades to the EHR or one of its components, or improperly configured software (24 incidents). One configuration error involved a disease management package that, after local implementation, was found to have erroneously escalated user privileges to place and sign orders. Another concern involved 'legacy' software (ie, an older system that has not evolved despite newer technologies[50]) that needed an upgrade or maintenance, but support staff did not have sufficient knowledge of these systems. For example, one incident described an inadvertent change to a configuration file

Table 2 EHR-related safety concerns with definitions and examples

Category of concern	Definition	Examples
Unmet display needs (n=36)	Mismatch between information needs and content display	▶ User required to review multiple screens to determine status of orders or review active medications ▶ EHR allows simultaneous order entry on two different patients with subsequent medication order for wrong patient ▶ User interface wording and function inconsistent throughout EHR ▶ Order entry dialog allows conflicting information to be entered
Software modifications (n=24)	Concerns due to upgrades, modifications, or configuration	▶ Software designed at remote facility conflicts with local software use ▶ Despite testing, a new feature allows unauthorized users to sign orders ▶ Corrupted files or databases prevent entry of diagnoses and orders ▶ Corrupted files or databases prevent retrieval of complete patient information
System–system interface (n=17)	Concerns due to failure of interface between EHR systems or components	▶ Failure of patient context manager ▶ Remote internal server failure prevents patient data from being retrieved ▶ Radiology studies canceled in EHR remain active in Picture Archiving and Communication System (PACS) workflow ▶ Interface flaw causing duplicate patient record creation from external source
Hidden dependencies in distributed system (n=17)	One component of the EHR is unexpectedly or unknowingly affected by the state or condition of another component	▶ Transition of patients between wards or units not reflected in EHR, resulting in missed medications or orders ▶ Bulk ordering of blood products results in prolonged delay due to matching algorithm ▶ Template completion depends on remote data, and user is unaware that network delays have caused incomplete data retrieval ▶ User assigns surrogate signer for patient alerts, but alerts not forwarded because of logic error not known by user

EHR, electronic health record.

during an update to the EHR that prevented the EHR from communicating with the printing system used to label laboratory specimens. Since these printers were installed and configured before recruitment of the current staff, the configuration error was not immediately recognized. This example demonstrates how a complex interaction of a technical dimension with non-technical dimensions can potentially develop into a safety concern. The main contributing sociotechnical dimensions of this concern type were hardware and software (21 incidents), clinical content (10 incidents), and workflow and communication (5 incidents). This concern type was most often associated with phase 1 EHR safety (21 incidents). Three concerns were classified as phase 2, and none were phase 3.

Concerns related to system–system interfaces
We analyzed 17 cases where the primary safety concern involved system–system interfaces, the means by which information is transferred from one EHR component to another. Patient safety concerns in this category often involved maintaining a unique patient's context, a process designed to keep various individual EHR components centered on a single patient as the user traverses the EHR components.[51] For example, if patient context is not maintained between the user's EHR screen and the radiology viewing screen, a different patient's data will be shown in the two EHR components and the user may incorrectly assume the data are associated with the original patient. Patient context-related concerns were caused by network failures, conflicts created by non-EHR software, and EHR upgrades that were not compliant with context protocols.

Another example of a system–system interface concern occurred when a patient who was allergic to ACE inhibitors presented to an emergency department with raised blood pressure. The patient was prescribed an ACE inhibitor and subsequently required treatment for allergic reactions and angioedema. Although the patient's medication allergy list at a remote facility included ACE inhibitors, a network problem prevented remote allergy checking. As highlighted in this example, the system–system interface concern involved interactions from multiple sociotechnical dimensions: hardware and software (17 incidents), workflow (6 incidents), and content (5 incidents). All incidents of this concern category were coded as phase 1 EHR use.

Concern of hidden dependencies in distributed systems
Concerns may develop not only because the EHR fails to support a particular task, but also because other processes within the EHR system conflict with the safe execution of that task. The concern of hidden dependencies or 'cascading' effects[52] occurs if one component of the EHR system is unexpectedly or unknowingly affected by the state or condition of another component. Safety concerns involving hidden dependencies and system–system interfaces are not mutually exclusive. As compared with system–system interfaces, hidden dependencies are unknown, and therefore potential points of failure and possible safety concerns may not be readily identified. An example of hidden dependencies occurred when medications were ordered for a patient who was admitted to the hospital but was temporarily placed in an outpatient unit. Once the patient was transferred to the regular inpatient unit, certain medications were automatically removed from the active medication list because they were previously ordered on an 'outpatient' status. This 'hidden dependency' (ie, between the patient's physical location and medication order status) can be potentially harmful to the patient because there was no clear expectation that medications would need to be reordered. Another example of a hidden dependency was a blood product compatibility matching algorithm that was not equipped to

handle an incoming bulk order, which exponentially delayed the processing of blood products. This delay resulted in a disruption of the blood bank workflow by preventing further entry of blood product orders through the EHR and delaying release of blood products to the requesting clinical services. The hidden dependency of all blood product-related processes in the EHR on the compatibility-matching algorithm was not known until this incident occurred.

The concerns of hidden dependencies primarily involved the dimensions of hardware and software (14 of 17 incidents), workflow (14 incidents), clinical content (9 incidents), and people (5 incidents). Incidents in this category were also noted to be largely dependent on multiple interactions between these dimensions, and only one incident was coded with a single dimension. These incidents also spanned both phase 1 (11 incidents) and phase 2 (6 incidents) of EHR safety.

DISCUSSION

We analyzed 100 unique, consecutive investigations of EHR-related safety concerns reported to and investigated by the VA's Informatics Patient Safety Office. Although the reports documented a variety of EHR-related safety incidents, four broad types of safety concerns were prominent: unmet data display needs within the EHR; problems with software modifications or upgrades; concerns related to system–system interfaces; and hidden dependencies within the EHR. Safety concerns typically emerged from complex interactions of multiple sociotechnical aspects of the EHR system. Although it is challenging to detect these concerns, let alone prevent them, our findings may be useful in guiding proactive efforts to monitor and improve safety as more institutions adopt EHRs.[53 54]

A novel feature and strength of our study is the use of an information-rich data source. Previous studies have largely used isolated event reports without benefit of an independent human factors and informatics investigation to analyze safety concerns in the EHR.[18 29–31 55] Conversely, we analyzed the contents of both initial incident reports and the findings of the safety investigations and analyses conducted by the VA IPS office. Our data sources included detailed narratives that explained the circumstances in which safety concerns arose, the actions of users and EHR systems at the time of the concerns, efforts to replicate or reproduce the safety concern by IPS investigators, and, when possible, the final determination of causes or preventive strategies. This level of detail enabled a more robust analysis in terms of understanding the larger sociotechnical context in which an incident occurred.

Our sociotechnical analysis of completed IPS investigations provides additional opportunities for safety improvement. While studies using self-reported data, including this one, are limited by the possibility of reporters' recall bias or knowledge,[56] our methods may allow for a more complete representation of an incident and the underlying safety concern. Additional strengths of our study include the nationwide distribution of our sample of EHR-related safety incidents and the relatively sophisticated implementation and use of the EHR across the VA healthcare system.[39] As an early adopter of EHRs, the VA has evolved into a 'learning system' that dedicates resources to investigating safety concerns and making EHR-related safety improvements decades after first launch.[42]

Our findings underscore the importance of continuing the process of detecting and addressing safety concerns long after EHR implementation and 'go-live' has occurred. Having a mature EHR system clearly does not eliminate EHR-related safety concerns, and a majority of reported incidents were phase 1 or unsafe technology. However, few healthcare systems have robust reporting and analytic infrastructure similar to the VA's IPS. In light of increasing use of EHRs, activities to achieve a resilient EHR-enabled healthcare system should include a reporting and analysis infrastructure for EHR-related safety concerns. Proactive risk assessments to identify safety concerns, such as through the use of SAFER guides released recently by The Office of the National Coordinator for Health Information Technology, can be used by healthcare organizations or EHR users to facilitate meaningful conversations and collaborative efforts with vendors to improve patient safety, including developing better and safer EHR designs.[53 57 58]

Although we cannot make specific claims about the prevalence of various EHR-related concerns, we were able to decipher some common types of problems. The four categories that emerged from our analysis appear to represent significant safety concerns that need to be addressed with current and future EHR implementations. Some safety concerns had relatively straightforward origins, such as simultaneous use of multiple instances of an EHR application by a single user, leading to order entry on the wrong patient. Other problems had more complex origins, such as user misinterpretation of information presented through the EHR's user interface. Our study suggests that technology-based solutions alone will only partially mitigate concerns and that interventions to improve EHR-related safety

Table 3 EHR-related safety concerns and suggested mitigating procedures

Category of concern	Mitigating procedures
Unmet display needs	▶ Testing information display in the context of 'real-world' tasks ▶ Validating display with all expected information and reasonable unexpected information ▶ Ensuring essential information is complete and clearly visible on the screen ▶ System messages and labels are unambiguously worded
Software modifications	▶ Availability and testing of appropriate hardware and software occurs at the unit level and as-installed before go-live ▶ Testing changes with full range of clinical content ▶ Exploring impact of changes on workflows
System–system interface	▶ Understanding, documenting, and testing content and workflow requirements on both sides of interface ▶ Ensuring communication is complete (disallow partial transmission of information) ▶ Developing workflows that incorporate back-up methods to transmit information
Hidden dependencies in distributed system	▶ Documenting ideal actions of EHR or components ▶ Documenting assumptions or making dependencies explicit in software, workflows ▶ Establishing monitoring and measurement practices with system-wide scope

EHR, electronic health record.

should encompass the people, organizations, systems, and policies that influence how EHRs are used. We suggest several general mitigating procedures that could be used to address these concerns in table 3.

This study has several limitations. All incidents were related to use of the same EHR within a single, albeit very large, healthcare system. Although the sample size is smaller than that of some other studies, the case descriptions were rich (ie, 2–4 single-spaced pages), spanned a period of 3 years, and represented a continuum of care from home-based primary care to large, urban medical centers. Nevertheless, our findings may not represent all types of EHR-related safety concerns and might not be generalizable to other institutions with different organizational characteristics, EHR infrastructure, or patient safety reporting mechanisms. The data used for our analysis were composed of safety concerns that ranged from unsafe conditions to patient harm. Although the analysis of unsafe conditions or near misses is useful to illustrate concerns in EHR-enabled care, we acknowledge that their circumstances or implications may be different from adverse events that result in patient harm. All four emergent safety concerns affected, or had the potential to affect, multiple patients, but we did not analyze additional data on patient outcomes as a result of these concerns. In general, fewer than 10% of medical errors are captured through reporting, and such data do not allow us to calculate prevalence rates.[56 59 60] Our study was unable to capture the universe of EHR-related safety concerns that might be occurring. Despite capturing a low percentage of errors, we were able to gain insight about non-technical aspects of EHR-related safety concerns that may not be routinely considered in technology-focused investigations.

In conclusion, our study demonstrates the potential utility of analyzing patient safety concerns using a sociotechnical approach to account for the complexities of using EHRs. We found that, even within a well-established EHR infrastructure, many significant EHR-related safety concerns related to both unsafe technology and unsafe use of technology remain. The predominant concerns we identified can help to focus future safety assessment activities and, if confirmed in other studies, can be used to prioritize ongoing interventions for further research. Safety concerns we identified had complex sociotechnical origins and would need multifaceted strategies for improvement. Thus, institutions with long-standing EHRs as well as those currently implementing EHRs should consider building a robust infrastructure to monitor and learn from EHR-related safety concerns.

REFERENCES

1 Institute of Medicine (IOM). *Crossing the quality chasm a new health system for the 21st century*. The National Academy Press, 2001.
2 Sittig DF, Singh H. Legal, ethical, and financial dilemmas in electronic health record adoption and use. *Pediatrics* 2011;127:e1042–7.
3 Ash JS, Berg M, Coiera E. Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. *J Am Med Inform Assoc* 2004;11:104–12.
4 Balka E, Doyle-Waters M, Lecznarowicz D, *et al.* Technology, governance and patient safety: systems issues in technology and patient safety. *Int J Med Inform* 2007;76(Suppl 1):S35–47.
5 Bates W, Cohen M, Leape L, *et al.* Reducing the frequency of errors in medicine using information technology. *J Am Med Inform Assoc* 2001;8:299–308.
6 Coleman RW. Translation and interpretation: the hidden processes and problems revealed by computerized physician order entry systems. *J Crit Care* 2004;19:279–82.
7 Hundt AS, Adams JA, Schmid JA, *et al.* Conducting an efficient proactive risk assessment prior to CPOE implementation in an intensive care unit. *Int J Med Inform* 2013;82:25–38.
8 Patterson ES, Cook RI, Render ML. Improving patient safety by identifying side effects from introducing bar coding in medication administration. *J Am Med Inform Assoc* 2002;9:540–53.
9 Pirnejad H, Niazkhani Z, van der SH, *et al.* Impact of a computerized physician order entry system on nurse-physician collaboration in the medication process. *Int J Med Inform* 2008;77:735–44.
10 Fairbanks RJ, Wears RL. Hazards with medical devices: the role of design. *Ann Emerg Med* 2008;52:519–21.
11 Karsh BT, Weinger MB, Abbott PA, *et al.* Health information technology: fallacies and sober realities. *J Am Med Inform Assoc* 2010;17:617–23.
12 Institute of Medicine (IOM). *Health IT and Patient Safety: Building Safer Systems for Safer Care*. Washington, DC: The National Academies Press, 2012.
13 Middleton B, Bloomrosen M, Dente MA, *et al.* Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from AMIA. *J Am Med Inform Assoc* 2013;20:e2–8.
14 Han YY, Carcillo JA, Venkataraman ST, *et al.* Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. *Pediatrics* 2005;116:1506–12.
15 Koppel R, Metlay JP, Cohen A, *et al.* Role of computerized physician order entry systems in facilitating medication errors. *JAMA* 2005;293:1197–203.
16 Ash JS, Sittig DF, Poon EG, *et al.* The extent and importance of unintended consequences related to computerized provider order entry. *J Am Med Inform Assoc* 2007;14:415–23.
17 Singh H, Mani S, Espadas D, *et al.* Prescription errors and outcomes related to inconsistent information transmitted through computerized order entry: a prospective study. *Arch Intern Med* 2009;169:982–9.
18 Myers RB, Jones SL, Sittig DF. Review of reported clinical information system adverse events in US food and drug administration databases. *Appl Clin Inform* 2011;2:63–74.
19 Weiner JP, Kfuri T, Chan K, *et al.* "e-Iatrogenesis": the most critical unintended consequence of CPOE and other HIT. *J Am Med Inform Assoc* 2007;14:387–8.
20 Harrington L, Kennerly D, Johnson C. Safety issues related to the electronic medical record (EMR): synthesis of the literature from the last decade, 2000–2009. *J Healthc Manag* 2011;56:31–43.
21 Meeks DW, Takian A, Sittig DF, *et al.* Exploring the sociotechnical intersection of patient safety and electronic health record implementation. *J Am Med Inform Assoc* 2014;21(e1)e28–34.
22 Veterans Health Administration. *VHA National Patient Safety Improvement Handbook*. Washington, DC, 2011. Report No.: VHA Handbook 1050.1.
23 Clancy CM. Common formats allow uniform collection and reporting of patient safety data by patient safety organizations. *Am J Med Qual* 2010;25:73–5.
24 Sittig DF, Singh H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *Qual Saf Health Care* 2010;19(Suppl 3):i68–74.
25 Harrison MI, Koppel R, Bar-Lev S. Unintended consequences of information technologies in health care—an interactive sociotechnical analysis. *J Am Med Inform Assoc* 2007;14:542–9.

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

27 Carayon P, Schoofs Hundt A, Karsh BT, *et al*. Work system design for patient safety: the SEIPS model. *Quality and Safety in Health Care* 2006;15(suppl 1):i50–8.

28 Health Information Technology Safety Action & Surveillance Plan. The Office for the National Coordinator of Health Information Technology 2013 July 2 [cited 2013 Jul 11]; http://www.healthit.gov/sites/default/files/safety_plan_master.pdf

29 Magrabi F, Ong MS, Runciman W, *et al*. Using FDA reports to inform a classification for health information technology safety problems. *J Am Med Inform Assoc* 2012;19:45–53.

30 Magrabi F, Ong MS, Runciman W, *et al*. An analysis of computer-related patient safety incidents to inform the development of a classification. *J Am Med Inform Assoc* 2010;17:663–70.

31 Sparnon E, Marella WM. The role of the electronic health record in patient safety events. Harrisburg, PA: Pennsylvania Patient Safety Authority; 2012.

32 Henriksen K, Kaye R, Morisseau D. Industrial ergonomic factors in the radiation oncology therapy environment. Advances in Industrial Ergonomics and Safety V. *Taylor and Francis* 1993;325.

33 Charles V, Sally T, Nicola S. Framework for analysing risk and safety in clinical medicine. *BMJ* 1998;316.

34 Sittig DF, Singh H. Defining health information technology-related errors: new developments since to err is human. *Arch Intern Med* 2011;171:1281–4.

35 Singh H, Wilson L, Petersen LA, *et al*. Improving follow-up of abnormal cancer screens using electronic health records: trust but verify test result communication. *BMC Med Inform Decis Mak* 2009;9:49.

36 Singh H, Thomas EJ, Sittig DF, *et al*. Notification of abnormal lab test results in an electronic medical record: do any safety concerns remain? *Am J Med* 2010;123:238–44.

37 U.S. Department of Veterans Affairs. About VHA. 2014 [cited 2014 Jan 15]. http://www.va.gov/health/aboutVHA.asp

38 Brown SH, Lincoln MJ, Groen PJ, *et al*. VistA-U.S. department of veterans affairs national-scale HIS. *Int J Med Inform* 2003;69:135–56.

39 Spetz J, Burgess JF, Phibbs CS. What determines successful implementation of inpatient information technology systems? *Am J Manag Care* 2012;18:157–62.

40 Perlin JB, Kolodner RM, Roswell RH. The veterans health administration: quality, value, accountability, and information as transforming strategies for patient-centered care. *Am J Manag Care* 2004;10:828–36.

41 Bonner LM, Simons CE, Parker LE, *et al*. 'To take care of the patients': qualitative analysis of veterans health administration personnel experiences with a clinical informatics system. *Implement Sci* 2010;5:63.

42 Taylor L, Wood SD, Chapman R. *Analysis and Mitigation of Reported Informatics Patient Safety Adverse Events at the Veterans Health Administration*. Human Factors and Ergonomics Society, 2012.

43 McCoy AB, Wright A, Kahn MG, *et al*. Matching identifiers in electronic health records: implications for duplicate records and patient safety. *BMJ Quality & Safety* 2013;22:219–24.

44 Graber ML, Franklin N, Gordon R. Diagnostic error in internal medicine. *Arch Intern Med* 2005;165:1493–9.

45 Green J, Thorogood N. *Qualitative methods for health research. Introducing qualitative methods*. London: SAGE, 2004. p. xv, 262.

46 Pope C, Ziebland S, Mays N. Qualitative research in health care. Analysing qualitative data. *BMJ* 2000;320:114–16.

47 Gale N, Heath G, Cameron E, *et al*. Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Med Res Methodol* 2013;13:117.

48 Sittig DF, Singh H. Electronic health records and national patient-safety goals. *N Engl J Med* 2012;367:1854–60.

49 Reliability. In: Given LM. ed. *The SAGE Encyclopedia of Qualitative Research Methods*. 2nd ed. Thousand Oaks, CA: SAGE Publications; 2008:753–4.

50 Brodie ML, Stonebraker M. Migrating legacy systems: gateways, interfaces & the incremental approach. Morgan Kaufmann Publishers Inc., 1995.

51 Sittig DF, Teich JM, Yungton JA, *et al*. Preserving context in a multi-tasking clinical environment: a pilot implementation. *Proc AMIA Annu Fall Symp* 1997; 784–8.

52 Patterson ES, Roth EM, Woods DD. Facets of complexity in situated work. Macrocognition Metrics and Scenarios: Design and Evaluation for Real-World Teams Ashgate Publishing ISBN, 2010:978.

53 Singh H, Ash J, Sittig D. Safety assurance factors for electronic health record resilience (SAFER): study protocol. *BMC Med Inform Decis Mak* 2013;13:46.

54 Wright A, Henkin S, Feblowitz J, *et al*. Early results of the meaningful use program for electronic health records. *N Engl J Med* 2013;368:779–80.

55 Warm D, Edwards P. Classifying health information technology patient safety related incidents—an approach used in Wales. *Appl Clin Inform* 2012;3:248–57.

56 Holden RJ, Karsh BT. A review of medical error reporting system design considerations and a proposed cross-level systems research framework. *Hum Factors* 2007;49:257–76.

57 The Office of the National Coordinator for Health Information Technology. SAFER Guides. 2014 [cited 2014 Apr 10]. http://www.healthit.gov/safer/safer-guides

58 Sittig DF, Ash JS, Singh H. ONC issues guides for SAFER EHRs. *J AHIMA* 2014;50–2.

59 Sari AB-A, Trevor AS, Alison C, *et al*. Sensitivity of routine system for reporting patient safety incidents in an NHS hospital: retrospective patient case note review. *BMJ* 2007;334.

60 Brubacher JR, Hunte GS, Hamilton L, *et al*. Barriers to and incentives for safety event reporting in emergency departments. *Healthc Q* 2011;14:57–65.