State of the Science Paper

# An Analysis of Electronic Health Record-Related Patient Safety Concerns

By

Derek W. Meeks, M.D

Anticipated Graduation: Spring 2014

APPROVED: 12/4/2013

Dean F. Sittig

______________________________

Dean F. Sittig, Ph.D.

______________________________

Hardeep Singh, M.D., M.P.H.

# An Analysis of Electronic Health Record-Related Patient Safety Concerns

Derek W. Meeks, M.D.[1,2], Michael W. Smith, Ph.D.[1,3], Lesley Taylor[4], Dean F. Sittig, Ph.D.[5], Jeanie Scott, CPHIMS[4], Hardeep Singh, M.D., M.P.H.[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

**Keywords**: Electronic Health Records, sociotechnical, reporting systems, medical errors, patient safety,

**Word count: 3287**

## ABSTRACT

**Importance:** Despite the benefits of electronic health records (EHRs), unintended safety risks have emerged. These risks are often challenging to identify and mitigate as they may involve multiple interacting components of the healthcare delivery system.

**Objective:** To analyze EHR-related safety concerns reported within a large, integrated healthcare system with a well-established EHR.

**Design, Setting, Measures:** The Informatics Patient Safety Office of the Veterans Health Administration maintains a non-punitive, voluntary reporting system to collect and analyze data on EHR-related adverse events, potential events, and near misses. We analyzed reports of events that received a complete investigation, categorizing the qualitative data from the reports through framework analysis. Our analysis was grounded in a previously developed sociotechnical conceptual model that accounts for both technical and non-technical dimensions of EHR-related safety. We also determined whether concerns were related to unsafe technology versus unsafe use of technology. Finally, we sought to identify underlying high-risk situations common to multiple events.

**Results:** We extracted 100 consecutive cases investigated between August 2009 and May 2013 of which 25 involved unsafe use of technology. More than two-thirds (70%) of reports involved 2 or more dimensions of our conceptual model. 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. Emergent areas of potential high-risk EHR use included unmet data display needs in the EHR, safety risks with software upgrades or modifications, risks of "hidden dependencies" within the EHR system, and risks related to data transmission across different components of the EHR. These four risk areas accounted for 94% of the reports analyzed.

**Conclusions and Relevance:** EHR-related risks related to both unsafe technology and unsafe use of technology persist despite the highly sophisticated EHR infrastructure represented in our data source. Certain types of risks appeared especially prominent and may represent high priority areas for patient safety interventions. Because these risks have complex sociotechnical origins, institutions currently implementing EHRs should consider building an infrastructure to monitor and learn from ongoing safety concerns.

## INTRODUCTION

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 risks and other unintended consequences due to usability issues, disruptions of clinical processes, and unsafe workarounds to circumvent technology-related constraints.[2-10] In particular, rapid adoption of electronic health records (EHRs) has revealed potential safety risks related to EHR design, implementation, and use.[11-15] Detecting EHR-related risks and preventing EHR-related adverse events requires an understanding of unsafe situations that occur with EHR use. This is challenging because risks 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.[16-19]

Despite a clear need to define and understand EHR-related safety risks,[20] data that describe the nature and magnitude of these risks are scarce. A few studies have attempted to quantify and classify HIT-related safety concerns by mining patient safety incident reporting databases.[12,21-23] In addition, conceptual frameworks or models have been developed to incorporate the breadth of technical and nontechnical factors into the analysis of HIT safety and effectiveness,[17;19;24-26] For instance, we previously developed a sociotechnical model that proposes eight interdependent dimensions that are essential to understand EHR-related safety (Table 1).[16;27] 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 risks.[28;29]

We conducted a qualitative "sociotechnical analysis" of EHR safety concerns that were reported voluntarily within a large integrated health system.[30] Using Sittig and Singh's sociotechnical model as a guiding framework, our aim was to describe common EHR-related safety risks 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 EHR-related patient safety reports from healthcare facilities within the Department of Veterans Affairs (VA). The VA operates the largest integrated healthcare system in the United States and uses a comprehensive EHR at all its facilities to provide care to approximately 8.3 million Veterans.[30] An established HIT infrastructure and successful EHR implementation is viewed as central to the VA system's quality goals.[31] 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 patient safety concerns. Patient safety concerns are broadly defined as incidents or adverse events that reached the patient, near misses that did not reach the patient, or unsafe conditions which increase the likelihood of a safety event.[32,33]

The IPS reporting system is the foundation for a rigorous approach that includes not only event investigation and analysis, but also feedback to reporters and development of solutions to mitigate future risks to patients. EHR users can report patient safety concerns through an intranet website or by using the national VA information technology helpdesk system. IPS analysts and human factors specialists examine safety concerns with the goals of understanding user actions that immediately preceded the safety concern, identifying the underlying root causes, and, if possible, safely replicating the event with "test" patients in the "live" EHR system. The concerns are analyzed and scored according to potential severity, frequency, and detectability. 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.[34] All investigation-related information is maintained in a database and tracked until the investigation is "closed." The final, closed report for each event contains a narrative as provided by the initial reporter, the technical narrative by IPS and information technology staff that includes details of the investigation, and any solution that might have been identified.

### *Data Collection*

We searched the IPS database for closed reports that contained full analyses and narratives that provided meaningful information, excluding duplicate entries. We also excluded safety events related to erroneous editing or merging of patient records resulting in co-mingled or overlaid records; though known risks,[35] these events were excluded because they are not routinely analyzed by IPS and are handled primarily by a separate program in the VA. We extracted 100 consecutive records that met our search criteria. Previous exploratory studies in patient safety have been able to shed powerful light on contributory factors with a similar sample size and, given the rich nature of the qualitative data, we believed this number was both optimal and feasible.[36]

*Data Analysis*

We analyzed narrative data in the reports using a framework analysis method, which allows emerging themes to be incorporated into a previously established framework.[37;38] Framework analysis consists of five stages: familiarization, thematic analysis, indexing, charting, and mapping and interpretation. First, two authors (D.W.M. and M.W.S.) independently reviewed and summarized the safety reports to become familiar with the data. 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 applied a separate classification scheme to categorize events by one of three different aspects or "phases" of safe EHR implementation: events related to inherently unsafe technology or technology failures ("phase 1"), events related to unsafe or inappropriate *use* of technology ("phase 2"), and events related to lack of monitoring of potential safety concerns before harm occurs ("phase 3").[39] Finally, we developed an additional ad hoc coding scheme to classify events more specifically according to the primary area of failure, or risk. This categorization helped derive a typology of the concerns.

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 report we noted this interaction by counting co-occurring dimensions. Re-reading and rearranging the data (charting) allowed emergent and recurring risks to be identified and described (mapping and interpretation) according to their sociotechnical origins and EHR safety phase. Coding decisions were discussed among the members of our multidisciplinary project team whose areas of expertise included clinical medicine, informatics, human factors, and information technology. All coding discrepancies were resolved by consensus. We used the software package Atlas.ti version 6.2 to facilitate coding of the report narratives and Microsoft Excel to arrange and structure the data.

## RESULTS

We extracted 100 reports of closed investigations between August 2009 and May 2013. Table 2 summarizes the categorization of the reports along the sociotechnical model's dimensions and EHR safety phases. Approximately three-fourths of reported concerns were categorized as phase 1 (i.e., concerns related to unsafe technology). Sociotechnical dimensions of phase 1 concerns most commonly involved hardware and software, workflow and communication, and clinical content. About one-quarter were classified as phase 2 (i.e., 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 (i.e., failure to use the EHR to monitor patient safety) was represented in our analysis. Reports frequently reflected occurrence of more than one sociotechnical dimension; 40 reports were classified with two sociotechnical dimensions, 23 reports had three, and 7 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 main areas of risk: unmet display needs in the EHR, safety risks with software modifications or upgrades, risks related to data transmission at system-system interfaces, and risk of "hidden dependencies" in distributed systems (i.e., when one EHR component unexpectedly or unknowingly is affected by the state or condition of another). Table 3 provides definitions and examples of these four risk types, which accounted for 94% of the reports analyzed. Below, we describe further details of the sociotechnical factors and EHR safety phases related to these specific risk types.

*Risks related to unmet data display needs in the EHR*

Unmet display needs was the most common type of risk observed (36 reports). This category represented a pattern of hazards in which human-EHR interaction processes did not adequately support the tasks of the end-users. These events reflected a poor fit between information needs and the task at hand, the nature of the content being presented (e.g., 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 these conditions, the displayed information available to the end-user failed to reduce uncertainty or led to increased risk of patient harm.

As an example, one report 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 upon order entry, this particular warning was known to have a high false positive rate. Due to diminished user confidence in the warning's reliability, the warning was overridden. The override 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 event 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 category, the contributory dimensions were hardware and software (22 reports), human-computer interface (22 reports), workflow and communication (10 reports), clinical content (9 reports), people (9 reports), organizational policies and procedures (2 reports), and system measurement and monitoring (1 report). Most (22 of 36) of these concerns were classified as phase one issues, followed by 13 reports related to phase two and 1 to phase three.

*Risks related to both intended and unintended software modifications*

The second most frequent category of risk was related to upgrades to the EHR or one of its components, or improperly configured software (24 reports). One configuration error included 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 (i.e., an older system that has not evolved despite newer technologies[40]) that needed an upgrade or maintenance, but support staff were unaware or did not have sufficient knowledge of these systems. For example, one report described an inadvertent change to a configuration file 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 prior to recruitment of the current staff, the configuration error was not immediately recognized. The main contributing sociotechnical dimensions of this risk category were hardware and software (21 reports), clinical content (10 reports), and workflow and communication (5 reports). This risk type was most often associated with phase one EHR safety (21 reports). Three reports were classified as phase two, and none were phase three.

*Risk of hidden dependencies in distributed systems*

Risks 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 risk of hidden dependencies or "cascading" effects[41] occurs if one component of the EHR system is unexpectedly or unknowingly affected by the state or condition of another component. For example, one safety concern involved medications that were ordered for a patient who was admitted to the hospital, but 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. Because medication status is not usually subject to change during an inpatient stay, there was no clear expectation that medications would need to be re-ordered. This "hidden dependency" (i.e., between the patient's physical location and medication order status) increased the risk of harm to the patient. 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 risks of hidden dependencies primarily involved the dimensions of hardware and software (14 of 17 reports), workflow (14 reports), clinical content (9 reports), and people (5 reports). Reports in this category were noted to be largely dependent on multiple interactions between these dimensions, as only one report was coded with a single dimension. Reports in this risk category consisted of 11 phase one reports and 6 phase two reports.

*Risks related to system-system interfaces*

Despite what may appear as a single, seamless system when viewed through a common user interface, EHRs are complex systems that have many interacting components, System-system interfaces are 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.[42] 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 is 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 maintenance protocols.

Another example of a system-system interface concern occurred when a patient who was allergic to angiotensin converting enzyme (ACE) inhibitors presented to an emergency department with elevated 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 risk involved interactions from multiple sociotechnical dimensions: hardware and software (17 reports), workflow (6 reports), and content (5 reports). All reports of this risk category were coded as phase one EHR use.

## DISCUSSION

We analyzed 100 consecutive reports of EHR-related patient safety concerns reported to and investigated by the VA's Informatics Patient Safety Office. Although the reports documented a variety of unexpected EHR-related safety hazards, four broad types of risk were especially prominent. These were unmet data display needs within the EHR, problems with software modifications or upgrades, hidden dependencies or unanticipated side effects from system actions, and risks related to system interfaces. Safety risks typically emerged from complex interactions of multiple sociotechnical aspects of the EHR system. Although it is challenging to detect these risks, let alone prevent them, our findings may be useful in guiding proactive efforts to monitor and improve safety as more institutions adopt EHRs.[43;44]

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 the benefits of an independent human factors assessment to analyze or replicate the event in the EHR.[12,21-23] Conversely, we analyzed the contents of both initial incident reports as well as the findings of the detailed safety investigations and analysis that followed. 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, 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 event occurred. Whereas previous studies have focused mostly on technical problems that lead to EHR safety events, our methods allowed for a more complete representation of the state of the system at the time of an event as well as underlying risks. Additional strengths of our study include the nationwide distribution of our sample of EHR-related safety events and the relatively sophisticated implementation and use of the EHR across the VA healthcare system.[31] As an early adopter of EHRs, the VA has evolved into a “learning system” that can dedicate resources to investigating safety risks and make EHR-related safety improvements decades after first launch.[34]

Our findings underscore the importance of detecting and addressing safety concerns long after EHR implementation and "go-live" has occurred. Although having a mature EHR system clearly does not eliminate EHR-related safety risks, it does facilitate oversight and monitoring activities such as those that generated our source data. However, few systems have robust reporting and analytic infrastructure similar to the VA's IPS. In light of increasing use of EHRs, reporting EHR-related safety concerns and conducting proactive assessments to identify safety risks should be essential activities to achieve a resilient EHR-enabled healthcare system.[43]

Although we cannot make specific claims about the prevalence of various EHR-related risks, it is notable that the vast majority of reports could be classified into one of four types of risk. Thus, the risk categories that emerged from our analysis appear to represent common and 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 risks and that interventions to improve EHR-related safety should encompass the people, organizations, systems, and policies that influence how EHRs are used. We list several general mitigating procedures that could be used to address these risks in Table 3.

This study has several limitations. All reports 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,[21;23] the case descriptions were rich (i.e., 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 implementations, or patient safety reporting mechanisms. Although we could not calculate prevalence rates, we were able to gain deep insights 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 risks using a sociotechnical approach to account for the complexities of using health information technology. We found that even within a well-established EHR infrastructure many significant EHR-related risks related to both unsafe technology and unsafe use or implementation of technology remain. The predominant risk categories we identified can help to focus future risk assessment activities and, if confirmed in other studies, can be used to prioritize ongoing interventions or further research. Because the risks we identified have complex sociotechnical origins, institutions currently implementing EHRs should consider building an infrastructure to monitor and learn from EHR-related safety concerns.

## Acknowledgments

We acknowledge the VA IPS for their collaboration on this work.

## Competing interests

None

## Funding

Dr. Singh is supported by the VA National Center of Patient Safety and the Agency for Health Care Research and Quality. Dr. Meeks is supported by the Baylor College of Medicine Department of Family and Community Medicine Postdoctoral Fellowship program and the Ruth L. Kirschstein National Research Service Award (T32HP10031). This material is based upon work supported (or supported in part) by the Department of Veterans Affairs, Veterans Health Administration, Office of Research and Development, and the Center for Innovations in Quality, Effectiveness and Safety (CIN 13-413).

Disclaimer: The views expressed in this article are those of the authors and do not necessarily reflect the position or policy of the Department of Veterans Affairs or the United States government.

## Contributors Statement

DWM analyzed the data, wrote the manuscript, and reviewed drafts for important intellectual content. MWS analyzed the data and reviewed drafts for important intellectual content. DFS and HS conceptualized the study and reviewed drafts for important intellectual content. LT and JS obtained the data and reviewed drafts for important intellectual content.

**Table 1. Patient 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 |

**Table 2. EHR-related Safety Risks with Definitions and Examples**

| **Category of Risk** | **Definition** | **Examples** |
|---|---|---|
| Unmet display needs (n=36) | Information needs and content display mismatch | • User required to review multiple screens to determine status of orders or review active medications<br>• User working on two patients with two instances of EHR orders medication for wrong patient<br>• User interface wording and function inconsistent throughout EHR<br>• 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<br>• Despite testing, a new feature allows unauthorized users to sign orders<br>• Corrupted files or databases prevent entry of diagnoses, orders<br>• Corrupted files or databases prevent retrieval of complete patient information |
| 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<br>• Bulk ordering of blood products results in prolonged delay due to matching algorithm<br>• Template completion depends on remote data and user is unaware that network delays have caused failure<br>• User assigning surrogate signer for patient alerts, but alerts not forwarded due to logical error not seen by user |
| System-system interface (n=17) | Concerns due to failure of interface between EHR systems or components | • Failure of patient context manager<br>• Remote internal server failure prevents relevant patient data to be retrieved<br>• Radiology studies canceled in EHR remain active in Picture Archiving and Communication System (PACS) workflow<br>• Interface flaw causing duplicate patient record creation from external source |

**Table 3. EHR-related Risk Factors and Suggested Mitigating Procedures**

| **Category of Risk** | **Mitigating Procedures** |
|---|---|
| Unmet display needs | • Testing information display in context of "real-world" tasks<br>• Validating display with all expected information and reasonably unexpected information<br>• Ensuring essential information is complete and clearly visible on the screen<br>• 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<br>• Testing changes with full range of clinical content<br>• Exploring impact of changes on workflows |
| Hidden dependencies in distributed system | • Documenting ideal actions of EHR or components<br>• Documenting assumptions or making dependencies explicit in software, workflows<br>• Establishing monitoring and measurement practices with system-wide scope |
| System-system interface | • Understanding and documenting content and workflow requirements on both sides of interface.<br>• Ensuring communication is complete (disallow partial transmission of information)<br>• Developing workflows that incorporate back-up methods to transmit information |

# Reference List

(1) Institute of Medicine (IOM). *Crossing the quality chasm a new health system for the 21st century*. 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-e1047.

(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. *Journal of the American Medical Informatics Association* 2004;11:104-112.

(4) Balka E, Doyle-Waters M, Lecznarowicz D, FitzGerald JM. Technology, governance and patient safety: Systems issues in technology and patient safety. *International Journal of Medical Informatics* 2007;76, Supplement 1:S35-S47.

(5) Bates W, Cohen M, Leape L, Marc Overhage J, Michael Shabot M, Sheridan T. Reducing the Frequency of Errors in Medicine Using Information Technology. *Journal of the American Medical Informatics Association* 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;19:279-282.

(7) Hundt AS, Adams JA, Schmid JA et al. Conducting an efficient proactive risk assessment prior to CPOE implementation in an intensive care unit. *International Journal of Medical Informatics* 2013;82:25-38.

(8) Koppel R. Role of computerized physician order entry systems in facilitating medication errors. *JAMA: The Journal of the American Medical Association* 2005;293:1197-1203.

(9) Patterson ES, Cook RI, Render ML. Improving Patient Safety by Identifying Side Effects from Introducing Bar Coding in Medication Administration. *Journal of the American Medical Informatics Association* 2002;9:540-553.

(10) Pirnejad H, Niazkhani Z, van der SH, Berg M, Bal R. Impact of a computerized physician order entry system on nurse-physician collaboration in the medication process. *Int J Med Inform* 2008;77:735-744.

(11) Singh H, Mani S, Espadas D, Petersen N, Franklin V, Petersen LA. Prescription errors and outcomes related to inconsistent information transmitted through computerized order entry: a prospective study. *Arch Intern Med* 2009;169:982-989.

(12) 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.

(13) Weiner JP, Kfuri T, Chan K, Fowles JB. "e-Iatrogenesis": the most critical unintended consequence of CPOE and other HIT. *J Am Med Inform Assoc* 2007;14:387-388.

(14) Institute of Medicine (IOM). *Health IT and Patient Safety: Building Safer Systems for Safer Care*. Washington, DC: The National Academies Press, 2012.

(15) 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.

(16) 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-i74.

(17) Harrison MI, Koppel R, Bar-Lev S. Unintended Consequences of Information Technologies in Health Care -- An Interactive Sociotechnical Analysis. *Journal of the American Medical Informatics Association* 2007;14:542-549.

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

(19) 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:i50-i58.

(20) Health Information Technology Safety Action & Surveillance Plan. *The Office for the National Coordinator of Health Information Technology* [serial online] 2013; Available from: The Office for the National Coordinator of Health Information Technology. Accessed July 11, 2013.

(21) Magrabi F, Ong MS, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. *J Am Med Inform Assoc* 2012;19:45-53.

(22) Magrabi F, Ong MS, Runciman W, Coiera E. An analysis of computer-related patient safety incidents to inform the development of a classification. *J Am Med Inform Assoc* 2010;17:663-670.

(23) Sparnon E, Marella WM. The role of the electronic health record in patient safety events. 2012. Harrisburg, Pa., Pennsylvania Patient Safety Authority. Pennsylvania patient safety advisory ; v. 9, no. 4.

(24) 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.

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

(26) Meeks DW, Takian A, Sittig DF, Singh H, Barber N. Exploring the Sociotechnical Intersection of Patient Safety and Electronic Health Record Implementation. *Journal of the American Medical Informatics Association* 2013.

(27) Sittig DF, Singh H. Defining health information technology-related errors: new developments since to err is human. *Arch Intern Med* 2011;171:1281-1284.

(28) 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.

(29) 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;123:238-244.

(30) Brown SH, Lincoln MJ, Groen PJ, Kolodner RM. VistA−U.S. Department of Veterans Affairs national-scale HIS. *International Journal of Medical Informatics* 2003;69:135-156.

(31) Spetz J, Burgess JF, Phibbs CS. What determines successful implementation of inpatient information technology systems? *Am J Manag Care* 2012;18:157-162.

(32) Veterans Health Administration. VHA National Patient Safety Improvement Handbook. VHA Handbook 1050.1. 3-4-2011. Washington, DC. 9-10-2013.

(33) Clancy CM. Common Formats Allow Uniform Collection and Reporting of Patient Safety Data by Patient Safety Organizations. *American Journal of Medical Quality* 2010;25:73-75.

(34) Analysis and Mitigation of Reported Informatics Patient Safety Adverse Events at the Veterans Health Administration. Proceedings of the 2012 Symposium on Human Factors and Ergonomics in Health Care; Human Factors and Ergonomics Society, 2012.

(35) McCoy AB, Wright A, Kahn MG, Shapiro JS, Bernstam EV, Sittig DF. Matching identifiers in electronic health records: implications for duplicate records and patient safety. *BMJ Quality & Safety* 2013;22:219-224.

(36) Graber ML, Franklin N, Gordon R. Diagnostic error in internal medicine. *Arch Intern Med* 2005;165:1493-1499.

(37) Green J, Thorogood N. Qualitative methods for health research. Introducing qualitative methods. xv, 262. 2004. London, SAGE. Introducing qualitative methods.

(38) Pope C, Ziebland S, Mays N. Qualitative research in health care. Analysing qualitative data. *BMJ* 2000;320:114-116.

(39) Sittig DF, Singh H. Electronic Health Records and National Patient-Safety Goals. *N Engl J Med* 2012;367:1854-1860.

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

(41) 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;978-0.

(42) Sittig DF, Teich JM, Yungton JA, Chueh HC. Preserving context in a multi-tasking clinical environment: a pilot implementation. *Proc AMIA Annu Fall Symp* 1997;784-788.

(43) Singh H, Ash J, Sittig D. Safety Assurance Factors for Electronic Health Record Resilience (SAFER): study protocol. *BMC Medical Informatics and Decision Making* 2013;13:46.

(44) Wright A, Henkin S, Feblowitz J, McCoy AB, Bates DW, Sittig DF. Early results of the meaningful use program for electronic health records. *N Engl J Med* 2013;368:779-780.