Analysis and Mitigation of Reported Informatics Patient Safety Adverse Events at the Veterans Health Administration

Lesley Taylor, Scott D. Wood, PhD
Informatics Patient Safety (IPS), Office of Informatics and Analytics (OIA), Veterans Health Administration (VHA), USA

Roger Chapman, PhD
Collaborative Work Systems, Inc., Plant City, FL, USA

Collecting reports of adverse events is a critical part of a comprehensive patient safety program. However, there is no standard practice for translating such reports into design changes. This paper describes the process used by the Department of Veterans Affairs (VA) Informatics Patient Safety (IPS) Office, within the Office of Informatics and Analytics, for analyzing informatics-based adverse events that pose a risk to patient safety. Development of effective design interventions comes from a consistent, systematic process including use of multi-disciplinary analysis teams, standardized tools, and human factors principles. This paper describes the IPS process, presents design-intervention examples, and discusses lessons learned. While challenges remain, the IPS process represents an effective, human-centric process that contributes to a positive culture of safety in VA.

INTRODUCTION

Informatics and Patient Safety

Modern Electronic Health Record (EHR) systems are typically composed of more than just patient data. They also include applications to support treatment, such as clinical decision support, communications, order entry, and medication management (Carter, 2008). For example, the VA Computerized Patient Record System (CPRS) consists of over 100 such applications and components, integrated into Veterans Health Information Systems and Technology Architecture (VistA), the underlying health record infrastructure (VHA, 2008). CPRS played a significant role in VA transformation in the mid-1990s, which resulted in improvements to quality of care (Jha, Perlin, Kizer, & Dudley, 2003), cost of care, and provider productivity (Evans, Nichol, & Perlin, 2006).

Despite the potential for health care improvements, EHR use also brings the potential for increased risk, often in the form of unintended consequences resulting from well-intentioned changes to EHR components (Koppel et al., 2005). This increased risk stems from the inherent complexity of modern medicine and health care, the design- and architectural-complexity of current EHRs, and the processes by which we develop, deploy, and maintain EHR components.

The combination of many interacting design factors makes comprehensive EHRs such as CPRS too complex to fully predict the ramifications of incremental design changes. Much of this stems from the inherent complexity of health care and the broad scope of necessary functionality for which we design. Additionally, software architecture aspects such as tight coupling between system components make it difficult to predict side effects of incremental component updates (Stevens, Myers, & Constantine, 1974). Furthermore, CPRS components are often developed piecemeal to meet ever-changing functional needs and integrated through system patches – as often happens with long-standing, legacy systems, such incremental changes increase system complexity over time, making them more brittle and difficult to modify. Finally, VA medical centers have wide latitude over CPRS deployment options to configure the EHR to fit local processes, and individual providers have the ability to configure some options based on personal preference. This flexibility comes at the price of added system complexity, both in terms of developing safe systems and in understanding the full context surrounding adverse events.

The dynamic and flexible nature of CPRS deployment, without strict configuration management, affords providers the ability to use whichever set of system components they choose, meaning that no set of static design requirements can be valid for long; mismatches between user need and the EHR user interface are inevitable. The scope and complexity of CPRS means that fully testing the effects of incremental changes for all possible application deployments is practically impossible. With these types of development and operational environments, there is always a risk that design or implementation errors will slip through testing and that some of them will put patients at risk. To mitigate these risks organizations must be vigilant in all stages of EHR system development and deployment and must have processes in place to handle the inevitability of EHR-related adverse events (Walker et al., 2008).

A well-established process for detecting and identifying adverse events is a post-deployment reporting system, which allows anyone connected to, or involved with, the health care system to report medical errors, close calls, and other risks to patient safety. Such reporting systems are key to continuous process improvement, a characteristic of mature high-reliability organizations (Humphrey, 1988; HIMSS 2011). In 2000, VA collaborated with the National Aeronautics and Space Administration (NASA) to develop the VA-NASA Patient Safety Reporting System (PSRS). Modeled after NASA's successful Aviation Safety Reporting System, PSRS is a voluntary, confidential reporting system for gathering detailed accounts of anything that poses a risk to patients (Bagian et al., 2001).

Detecting problems, however, is only the beginning. As stated in the Institute of Medicine report, *To Error is Human: Building a Safer Healthcare System (*Kohn, 2000*)*,

> "Receiving reports is only the first step in the process of reducing errors. Sufficient attention must be devoted to analyzing and understanding the causes of errors in order to make improvements."

Reporter narratives need to be analyzed by experts in the domain to determine all relevant details surrounding an adverse event, including why it happened and under what specific conditions. Reported events can represent a wide range of potential harm to patients, from minor to catastrophic, so cases must also be prioritized so that the most critical risks are addressed first. Only then does it make sense to consider possible interventions. Ultimately, practical and effective EHR design changes must be developed from analyzed cases using a combination of techniques adapted from human factors, systems engineering, software engineering, and health informatics. This paper describes the process used by the VA to analyze and correct informatics-based adverse events to continuously improve patient safety.

PRACTICE INNOVATION

The IPS office is responsible for processing, investigating, analyzing, and maintaining all reported cases of informatics-related adverse events. Informatics-based adverse events are typically reported through one of four main avenues: local incident reporting at medical centers, an adverse drug event reporting system, the VA National Center for Patient Safety, and the VA National Information Technology (IT) Help Desk Incident Reporting System (Figure 1).

Medical Centers
- Local incident reporting database
- Broad range of facility-specific incidents, including informatics patient safety events

Adverse Drug Event Reporting
- VHA database to collect reports specific to adverse drug events

National IT Help Desk Incident Reporting
- Broad range of software-specific incidents, including informatics patient safety events

National Center for Patient Safety
- Collection of Safety Reports and Root Cause Analyses from all VA sites

Figure 1. VHA avenues for adverse event reporting

IPS Analysis Process Overview

VA utilizes a well-defined software development process that includes rigorous testing. However, despite everyone's best intentions and efforts, adverse event are inevitable. The IPS office responds to adverse events using a well-defined process (Figure 2). The process begins with the reporting of the event or close call and then proceeds to an investigation phase followed by a human factors analysis, risk analysis, and intervention analysis. It is important to note that, as with VA's other adverse event reporting avenues, IPS's process includes close calls, those cases that did not involve patient harm but which had the potential to do so. This practice is similar to that followed in other domains, such as commercial flight and nuclear power, where high reliability is essential; VA considers the reporting and analysis of close calls just as important as those events that led to catastrophic outcomes.

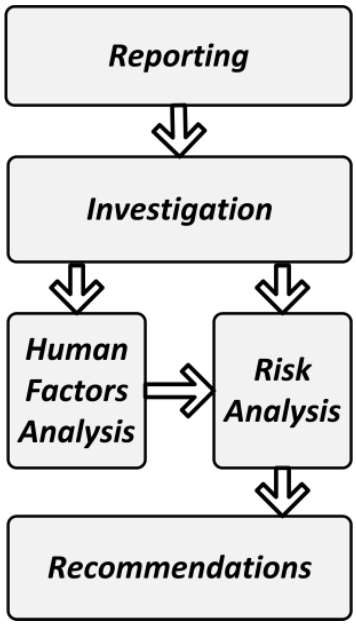

Figure 2. IPS Adverse Event Analysis Process

It is also important to note that VA strives for a "culture of safety" in health care (Weeks & Bagian, 2000), a key component of which is a blame-free reporting system, where systems and processes are the focus of safety investigations, not people (Bagian & Gosbee, 2000).

Reporting

The most common avenue for receiving reported informatics-based adverse events is via VA's National Help Desk Incident Reporting System. This tool enables IPS to collaborate with developers, product support personnel and reporting sites to investigate and analyze the adverse event cases. The Incident Reporting System is primarily used for VA-wide IT issue tracking and technical support, however there is a section within the reporting submission dialog that allows the reporter to indicate whether the reported problem affects patient safety. Once an incident is marked as presenting a potential patient safety risk, the reporter is asked a series of additional questions, such as:

- "How is this issue related to patient safety?"
- "How was the problem identified?"

The answers to these questions become the foundation for the IPS office's investigation. When an issue flagged as patient safety-related is submitted through the National IT Help Desk, IPS is notified and the case is logged in the IPS Case Tracking System, a case-tracking database customized for the IPS analysis process. This initiates the IPS case investigation.

Investigation

An IPS Domain Analyst and IPS Human Factors Specialist are assigned to each issue. The domain analyst's role is to conduct a fact-finding investigation by communicating with the national software support staff (at the VA National IT Help Desk) that are most familiar with the issue, the reporting site, and often the software developers.

The IPS analyst continues to investigate the case by using other tools, such as test accounts, to attempt to replicate reported issues. This is a key step in the investigation to isolate the conditions under which the software behaves erroneously. The analyst also conducts a search for similar incidents that may have been reported previously – this can also yield important clues to determine incident frequency and necessary conditions for occurrence. The databases searched include the National IT Help Desk Incident Reporting System (for similar cases that might not have been flagged as patient safety issues), as well as the IPS Case Tracking Database. The result of the investigation is a comprehensive case report that includes not just the what, why, and when, but also information necessary to determine:

1. How the issue was detected (such as who detected the event and what they were doing when they detected the problem).
2. The frequency with which it may occur nationwide (such as how often the enabling conditions occur per month, how many sites are affected, and how many patients may be at risk).
3. The severity of the issue (such as a likely worst-case scenario and level of potential).

This information enables a human factors analysis to begin, and provides the key elements to conduct a risk analysis. The result of the investigation is a clear understanding of the sequence of events in clinical terms that led up to and precipitated the adverse event.

Human Factors Analysis

When the clinical (or contextual) accounting of the adverse event is complete, an IPS Human Factors Specialist analyzes the events from a cognitive perspective. The human factors analysis typically begins with a summary of events at a psychological level to describe the specific issues in terms of human-computer interaction. For example, where the earlier investigation might describe an incorrect clinical step, the human factors analysis might also include whether there was sufficient information available for the user to make a good decision. IPS is developing a Patient Safety Informatics – Cognitive Analysis Model (PSI-CAM), a classification framework for characterizing adverse events (Chapman, Taylor, & Wood, 2012) using a variation of Norman's Gulfs Model (Norman, 1986). In a broad sense, the PSI-CAM model considers errors involving evaluation of information and execution of actions. In practice, using the PSI-CAM model to characterize problematic user-interactions helps to pinpoint the source of latent software design flaws.

Figure 3 shows the basic user-interaction cycle within the PSI-CAM framework (from Chapman *et al*, 2012). Simplistically, goal-driven behavior flows from intention through execution and some post-action evaluation of progress towards the goal. Event- or data-driven behavior flows in the opposite direction. Using this framework, human factors specialists map clinical actions from the earlier investigation to the functionality afforded by the user interface and gauge the effectiveness of the software to meet user needs. When cognitive mismatches are found as a result of the human factors analysis, a set of candidate interventions can be proposed. Specific recommendations, however, must be weighed against other design goals and the level of risk actually presented by the reported event.

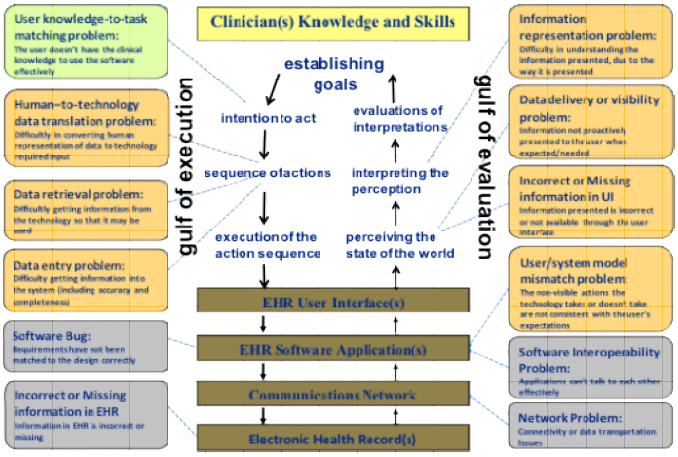

Figure 3: Human Factors Evaluation Model

Risk Analysis

After the initial investigation and analyses are complete, an IPS risk assessment team assesses the overall risk that an adverse event presents to patient safety. Risk here is defined as the product of three key aspects: severity, frequency and detectability (see Figure 4).

Risk = Severity x Frequency x Detectability

Figure 4. IPS Risk Assessment

Severity can range from Minor (no harm to the patient) with a value of 1, to Catastrophic (the potential of death) with a value of 4. Frequency can range from Remote (less than once per year) with a value of 1, to Frequent (at least once per month) with a value of 4. These risk factors are similar to those defined for the Severity Assessment Code, developed by the VA National Center for Patient Safety (DeRosier, Stalhandske, Bagian, & Nudell, 2002) and used to assess non-informatics-based adverse events. In addition to severity and frequency, IPS also explicitly considers the aspect of problem detectability.

In the risk scoring equation, detectability can range from Remote (information necessary to detect an error is missing or incorrect) with a value of 4, to High (information or process ensures an error will always be detected) with a value of 1. Detectability is considered essential for assessing informatics-based risk because it can easily change potential for patient harm. For example, a critical lab result that is missed by a clinician could have catastrophic (Severity = 4) results, but if it was reasonably guaranteed that the clinician or another provider would detect the error prior to any possible harm to the patient, then the effects of the error are dramatically reduced. Similarly, if even minor errors are not detected in a timely manner, they can result in a latent risk whose effect is only seen sometime in the future. For example, mis-entering a slightly abnormal lab result may not directly harm a patient when it happens, but if it results in a provider missing a downward trend in the patient's health, it could cause a delay of care, which is not a minor event.

IPS risk assessment teams typically consist of the analyst, one or more domain experts, a human factors specialist, and occasionally software developers or other system stakeholders. Using the final understanding from the earlier investigation and subsequent analyses as a foundation, the three risk components (severity, frequency, and detectability) are individually assessed according to well-defined scoring criteria. These individual scores are then multiplied to determine the final risk score.

Recommendations

As shown in Table 2, a case's final risk score is used to help determine what type of intervention to recommend, the priority of solving the problem, and the steps necessary for IPS to follow up with developers and stakeholders. Low risk scores represent minor, infrequent, and easily detectable problems that do not require immediate intervention or software change. Scores above 24 do represent a major patient safety risk and require immediate action to correct the problem and possibly a VA-wide patient safety alert or advisory to warn users of the danger to mitigate the risk as soon as possible.

IPS recommendations are made directly to system stakeholders and developers (those responsible for developing and maintaining a particular software application). These recommendations are derived from human factors, systems safety, computer science and health informatics principles, reflecting best practices such as user-centered design, standardization, and error-tolerant system-design.

Table 1. Required actions based on risk score.

Risk Score	Required Actions
< 12	Action not required
12 - 24	Recommendations made to stakeholders for software or process change
> 24	Software change must be made in next possible update. Consider VA-wide advisory.

Example recommendations made by IPS include:

- Correction of a software defect that is causing a specific, replicable problem.
- Change to a software requirement when the software is working as designed but the design requirement does not meet user needs. Two common types include:
  - Error message revisions, where the error message is confusing.
  - Information display change, where information is not presented in a way that supports perception or decision making.
- Patient Safety notification distributed to all of VHA, alerting users to the problem and specific mitigation steps.
- User instruction guide updates or user training on software functionality.
- Monitoring of future incident reports for similar cases of an adverse event, if the problem that cannot be replicated.

Of course, all mitigations are not created equal – some are more effective than others, but perfect solutions are often not possible or practical. For example, training system users to enter dates in the correct format (e.g., "10/12/2012") may reduce data entry errors but it will not prevent such errors as well as will a forcing function that prevents incorrect data entry (e.g., a calendar widget). However, significant software changes often take much longer to implement than other interventions, so stakeholders must choose between a simple solution sooner versus a more effective solution later. Thus IPS recommendations are developed in collaboration with system stakeholders to effectively weigh the practicality and timeliness of various interventions against the effectiveness of those interventions to prevent patient harm. To close the loop on case analysis, IPS also provides feedback to the original reporter, to inform on the case results and the interventions that will be made to correct the problems. In the next section we present examples for ranking the effectiveness, or strength, of an intervention for reducing risk.

FINDINGS

The IPS office investigates and analyzes over 100 informatics-based adverse events per year. In this section we illustrate the IPS process with several case examples. These

examples are discussed in terms of strength of the intervention to help describe how the IPS process helps make informed decisions about which intervention to apply.

Strength of Intervention

The National Center for Patient Safety (NCPS) has developed a *Hierarchy of Actions* (NCPS 2012) for ranking the effectiveness of various patient safety interventions. Based on earlier work by the National Institute for Occupational Safety and Health (Robson, Shannon, Goldenhar, & Hale, 2001) the hierarchy classifies interventions as stronger, intermediate or weaker regarding their effectiveness at reducing the likelihood of reoccurrence of the adverse events. Stronger interventions are those that eliminate or nearly eliminate the vulnerabilities by making it difficult to do the task incorrectly (e.g., a forcing function). Intermediate interventions are those that reduce the reliance of an individual's memory or vigilance to do a task (e.g., perceptual indicators). Weaker interventions are those that still rely on individual vigilance and adherence to process to mitigate the risk. (e.g., training, warnings, or new rules).

Several cases from IPS regarding a recent upgrade to CPRS help illustrate how strength of intervention translates to design changes. These cases are described in terms of the earlier version (before the upgrade) and the later version (after the upgrade).

Weaker Intervention

One case involved CPRS use of notifications to communicate patient health and treatment information between providers and other health care staff. In the earlier version, the CPRS "Remove Pending Notification" button created a problem. When the button was selected by one of many providers that received the notification, the software was coded to delete the notifications for all other recipients without indicating that it had done so. This meant there was a risk that the intended recipient would not see the notification, which could subsequently lead to a delay in treatment for the patient. To help mitigate the patient safety risk involved with this problem, the CPRS User Guide was updated to include a warning about removal of pending notifications. This is a weaker type of intervention because it relies on the user skill, knowledge, and vigilance regarding a training document to prevent future occurrences. A stronger software modification is targeted for a future version of CPRS.

Intermediate Intervention

Another reported case involved CPRS functionality to annotate patient records with warnings that are important for providers, such as whether the patient is suicidal or a violence risk. These annotations, known as Category (CAT) II, or CAT II Patient Flags, are displayed in a pop-up dialog when a provider first opens the patient EHR. In the earlier version of CPRS, only two such flags could be visible in the dialog without scrolling. The concern was that if the providers did not notice the scroll bar, they might only consider the visible portion for CAT II information (only the first two flags were visible) and not scroll down to see the other flags. At sites that have several CAT II flags on a patient, flags like "Suicidal" would not be displayed without scrolling because the display is alphabetical. This created the potential for inappropriate or contraindicated treatment, and a risk to the provider. For this reported problem the recommendation was to change the display to improve flag visibility and indicate the number of flags that were attached to the record. This is an example of an intermediate intervention because the solution involved improving the user's ability to perceive the information that was displayed. This type of solution is considered stronger than a training or documentation solution, but still leaves a risk that the information could be missed if the provider habitually closes the dialog without reading the contents. A stronger intervention might be to always have CAT II flags visible, obviating the need for a separate dialog box. However, implementing the strongest possible intervention is not always practical in the short-term because there is always a risk that any system change can expose or create additional system vulnerabilities. IPS provides a range of intervention options, with varying strengths, to help developers and stakeholders make more informed design decisions.

Stronger Intervention

A third reported case involved confusion regarding which patient record was active. In the earlier version of CPRS, if while working with a patient record the provider-user requested a specific form of patient detail (called a Patient Inquiry) but then tried to open a different patient's record before the requested detail screen loaded, the first patient's information could be displayed under the second patient's name. This, of course, created a risk for patient misidentification, and for either patient to receive an incorrect diagnosis or treatment. Since the problem occurred when two system processes were concurrently attempting to display information on the same screen at the same time, developers modified CPRS to disable the ability to request another patient record until the prior request was complete. This is an example of a stronger intervention because it eliminated the vulnerability of an erroneous system state, and prevented reoccurrence of that type of adverse event.

LESSONS LEARNED AND CONCLUSIONS

Two interdependent themes are pervasive in the IPS process and contribute to its effectiveness. First, the IPS process both supports and benefits from a culture of safety in VA. That culture puts the highest value on patient safety and guides all aspects of the process toward the common goal of safe care. Second, the IPS process embodies human-centered design in all phases, tailoring the process and tools to the needs of those analyzing adverse events, as well as to the

needs of end users. Taking a human focus at each stage helps ensure that both the analysis process and the resulting recommendations are each designed to help capitalize on human strengths and overcome human limitations. This human focus is, in turn, necessary for developing a culture of safety.

In the Reporting phase of the IPS process, the positive safety culture is evident both in VA's blame-free reporting policy and in the mechanisms designed to capture adverse event reports. Blame-free reporting encourages the identification of unsafe conditions from every aspect of patient care. From a human-centric perspective, VA simplifies the reporting process for end users by allowing them to report informatics-based adverse events through the National IT Helpdesk system, without the need to duplicate their report through a separate patient safety reporting mechanism. Simpler processes encourage more reporting. Furthermore, the structured questionnaire for reporting patient safety issues helps reporters focus on those aspects of events that are critical for analysis, making the reported information more valuable and enabling a more effective and efficient analysis. Finally, providing feedback to the reporter establishes an element of trust that every report is important and that the time spent reporting actually contributes to patient safety.

In the Investigation phase of the IPS process, domain analysts focus on the reported information to piece together a coherent picture; that is, the sequence of events that led up to the adverse event from a clinician perspective. In this necessarily human-centric analysis, IPS also attempts to replicate the problem using a test account to fully understand the context and contributing factors. As with the Human Factors Analysis phase that follows, the culture of safety ensures that the focus is on process- and system-flaws and does not attribute fault to human limitations. In both phases, IPS utilizes a set of standardized tools to simplify analysis and bring consistency to the results. Domain analysts use checklists, timelines, and investigation templates to help standardize the investigation process and improve results. Human Factors specialists are developing similar tools, including a cognitive analysis model (PSI-CAM; Chapman, et al., 2012), to help classify human-system interaction errors revealed by the domain analysis and to drive scoring and design recommendations from human factors principles.

Similarly, in the Scoring and Recommendation phases, analysts use a set of well-defined guidelines for assessing the risk presented by a case and the strength of the recommended system changes (interventions). As with other human-centric approaches, these guidelines undergo continuous improvement, as ambiguous or difficult scoring challenges feed the next iteration of guideline development. The multi-disciplinary nature of the risk assessment contributes to the culture of safety by exposing developers and other stakeholders to the blame-free scoring process. The culture of safety goes further though, in that the main goal is to reduce the potential for harm to patients. This means that although a range of recommendations are provided to the system stakeholders, IPS analysts help developers weigh the difficulty of implementing a particular system change with the potential improvement in patient safety. A practical but effective intervention is better than a perfect one that will never be implemented.

The VA IPS office analysis process is an effective approach to identifying, analyzing, and correcting informatics-based adverse events. Key to this success are clearly defined terminology and assessment criteria, utilization of multi-disciplinary analysis and assessment teams, and involvement of all stakeholders throughout the process. As a result, this process both improves patient safety and provides an informed, human-centric driver for continuous EHR-related improvements.

ACKNOWLEDGEMENTS

We would like to acknowledge the support of everyone in the Informatics Patient Safety office, who improve patient safety every day, and of all those who helped develop and refine this process.

The views expressed here are those of the authors and not necessarily those of the Department of Veterans Affairs.

REFERENCES

ASRS *(asrs.arc.nasa.gov) accessed 2/21/12.*

Bagian, J. P. (2001). Patient safety--the VA's experience. Mich Health Hosp, 37(4), 62-63.

Bagian, J. P., & Gosbee, J. W. (2000). Developing a culture of patient safety at the VA. Ambul Outreach, 25-29.

Bagian, J. P., Lee, C., Gosbee, J., DeRosier, J., Stalhandske, E., Eldridge, N., . . . Burkhardt, M. (2001). Developing and deploying a patient safety program in a large health care delivery system: you can't fix what you don't know about. Jt Comm J Qual Improv, 27(10), 522-532.

Bagian, J. P. (2005). Patient safety: what is really at issue? Front Health Serv Manage, 22(1), 3-16.

Carter, J. H., & American College of Physicians (2003-). (2008). Electronic health records : a guide for clinicians and administrators (2nd ed.). Philadelphia: ACP Press.

Chapman R. J., Taylor, L. M., & Wood, S. D. (2012). Cataloging Errors from Reported Informatics Patient Safety Adverse Events. Proceedings of Human Factors and Ergonomics Society Healthcare Symposium, Baltimore, MD.

Department of Veterans Affairs. (2008). VistA-HealtheVet Monograph 2008 - 2009 Retrieved from http://www.va.gov/vista_monograph/

DeRosier, J., Stalhandske, E., Bagian, J. P., & Nudell, T. (2002). Using health care Failure Mode and Effect Analysis: the VA National Center for Patient Safety's prospective risk analysis system. Jt Comm J Qual Improv, 28(5), 248-267, 209.

Evans, D. C., Nichol, W. P., & Perlin, J. B. (2006). Effect of the implementation of an enterprise-wide Electronic Health Record on productivity in the Veterans Health Administration. Health Econ Policy Law, 1(Pt 2), 163-169. doi: 10.1017/S1744133105001210

HIMSS. (2011). Promoting Usability in Healthcare Organizations: Initial Steps and Progress Toward a Usability Maturity Model. Retrieved from http://www.himss.org/content/files/HIMSS_Promoting_Usability_in_Health_Org.pdf.

Humphrey, W. S. (1988). Characterizing the Software Process: A Maturity Framework. IEEE Softw., 5(2), 73-79. doi: 10.1109/52.2014

Jha, A. K., Perlin, J. B., Kizer, K. W., & Dudley, R. A. (2003). Effect of the transformation of the Veterans Affairs Health Care System on the quality of care. N Engl J Med, 348(22), 2218-2227. doi: 10.1056/NEJMsa021899

Kohn, L. et. al. To Error is Human: Building a Safer Healthcare System. Institute of Medicine (2000).

Koppel, R., Metlay, J. P., Cohen, A., Abaluck, B., Localio, A. R., Kimmel, S. E., & Strom, B. L. (2005). Role of computerized physician order entry systems in facilitating medication errors. JAMA, 293(10), 1197-1203.

NCPS *(www.patientsafety.gov) accessed 2/21/12.*

Norman, D. A. (1986). Cognitive Engineering. In D. A. Norman & S. W. Draper (Eds.), User Centered System Design. Hillsdale, NJ: Lawrence Erlbaum Associates.

Robson, L. S., Shannon, H. S., Goldenhar, L. M., & Hale, A. R. (2001). Guide to Evaluating the Effectiveness of Strategies for Preventing Work Injuries:

How to Show Whether a Safety Intervention Really Works: CDC, Department of Health and Human Services.

Stevens, W. P., Myers, G. J., & Constantine, L. L. (1974). Structured Design. IBM Systems Journal, 13(2), 115 - 139.

Walker, J. M., Carayon, P., Leveson, N., Paulus, R. A., Tooker, J., Chin, H., . . . Stewart, W. F. (2008). EHR safety: the way forward to safe and effective systems. J Am Med Inform Assoc, 15(3), 272-277. doi: 10.1197/jamia.M2618

Weeks, W. B., & Bagian, J. P. (2000). Developing a culture of safety in the Veterans Health Administration. Eff Clin Pract, 3(6), 270-276.