# Resilient Practices in Maintaining Safety of Health Information Technologies

**Michael W. Smith**, Michael E. DeBakey VA Medical Center, Houston, Texas, **Joan S. Ash**, Oregon Health and Science University, Portland, **Dean F. Sittig**, University of Texas, Houston, and **Hardeep Singh**, Michael E. DeBakey VA Medical Center, Houston, Texas

Electronic health record systems (EHRs) can improve safety and reliability of health care, but they can also introduce new vulnerabilities by failing to accommodate changes within a dynamic EHR-enabled health care system. Continuous assessment and improvement is thus essential for achieving resilience in EHR-enabled health care systems. Given the rapid adoption of EHRs by many organizations that are still early in their experiences with EHR safety, it is important to understand practices for maintaining resilience used by organizations with a track record of success in EHR use. We conducted interviews about safety practices with 56 key informants (including information technology managers, chief medical information officers, physicians, and patient safety officers) at two large health care systems recognized as leaders in EHR use. We identified 156 references to resilience-related practices from 41 informants. Framework analysis generated five categories of resilient practices: (a) sensitivity to dynamics and interdependencies affecting risks, (b) basic monitoring and responding practices, (c) management of practices and resources for monitoring and responding, (d) sensitivity to risks beyond the horizon, and (e) reflecting on risks with the safety and quality control process itself. The categories reflect three functions that facilitate resilience: reflection, transcending boundaries, and involving sharp-end practitioners in safety management.

**Keywords:** health care delivery, domains, information systems, resilience engineering, topics, naturalistic decision making

Address correspondence to Michael W. Smith, PhD, VA Medical Center (152), 2002 Holcombe Blvd, Houston, TX 77030, USA; e-mail: MS6@bcm.edu.

*Journal of Cognitive Engineering and Decision Making*
Volume 8, Number 3, September 2014, pp. 265–282
DOI: 10.1177/1555343414534242


## INTRODUCTION

The role of automation in supervisory control systems can facilitate and/or disrupt performance in many ways (e.g., Bainbridge, 1983). Likewise, the process of implementing changes in the delivery of health care can succeed or fail depending on numerous factors (Grol & Grimshaw, 2003). The volatile combination of the two can be seen in the current political, commercial, and scientific activities surrounding the adoption of electronic health records (EHRs) in the United States (Wright et al., 2013), especially the explorations and debates about EHR safety (Institute of Medicine, 2012).

Greenhalgh, Potts, Wong, Bark, and Swinglehurst (2009) describe several conceptualizations or "meta-narratives" about EHRs in the literature. The "health information systems" meta-narrative frames EHRs as tools for systematically managing clinical information, relieving health care workers of this burden, and thereby protecting patients from the associated safety risks. Technology is viewed primarily as a means of preventing mistakes by constraining human performance. This approach corresponds to a view of human error and safety that sees accidents as products of a faulty (usually human) element in proximity to the accident. Accordingly, strategies to increase safety focus primarily on the use of barriers (Dekker, 2006; Qureshi, Ashraf, & Amer, 2007).

In contrast, the "critical sociology" meta-narrative (Greenhalgh et al., 2009) conceptualizes EHRs as tools for systematically managing the work of clinical providers, imposing a model that presumes optimal efficiency and consistency while constraining the ability of clinical providers to respond to situated needs. This approach considers the underlying structure of the organization as a possible risk factor for

errors. Similarly, some models of safety, such as the "Swiss cheese" model (Reason, 1997), view accidents not simply as the fault of front-line workers but as the result of multiple failures in a series of barriers, including latent failures in the organizational environment (Dekker, 2006; Hollnagel, 2008a; Qureshi et al., 2007).

Though these two meta-narratives reflect opposing perspectives, both contain valid insights on how EHRs affect clinical work. EHRs offer many potential safety enhancements and other benefits to providers and other clinical staff (Jha & Classen, 2011). At the same time, EHRs serve in some ways as supervisory control systems for the process of care delivery. For example, EHRs may shape provider choices by presenting certain options for tests and/or treatments for selection, or they may discourage providers from ordering potentially dangerous drug combinations (Teich et al., 2000). In some systems, deviations from computer-recommended treatments require a justification (Hsieh et al., 2004).

Although the two aforementioned perspectives highlight the impact of EHRs on clinical work, both are oversimplifications. First, an EHR is not a homogenous entity. At its simplest, an EHR is a database containing the health information of patients under the care of a facility, but in practice, EHRs are sophisticated software applications that contain and/or interact with other applications, including systems for computerized provider order entry, clinical decision support, test results management, pharmacy databases, and medication administration systems (i.e., barcoding systems; Committee on Data Standards for Patient Safety, 2003). These software applications require networked hardware and clinical knowledge structures, such as decision rules and vocabularies, to operate (Sittig & Singh, 2010).

Second, EHRs are not static; rather, they are subject to change from other elements in the sociotechnical system, including providers (Hunte, Wears, & Schubert, 2013). For instance, EHRs evolve in response to changes in clinical knowledge structures and how providers encode medical problems (Aarts, 2011). Thus, the front-line providers at the "sharp end" of patient care (Cook & Woods, 1994) are not simply passive recipients but active agents in the ongoing development of the EHR. Being a technical system in people-centric health care delivery organizations, the EHR is a part of a multilevel network of pressures and influences. Patients, providers, managers, regulators, and many sociopolitical factors influence, and are influenced by, EHRs (Leveson, 2004; Rasmussen, 1997; Vicente, 2002).

Third, as dynamic systems embedded in organizations with quality, production, and resource pressures, EHRs need to be effectively managed, especially to maintain safety. Active maintenance and oversight activities are needed for adaptations in response to changes to health care systems (Reason, 1997; Reiman, 2011). Otherwise, changes may lead health care systems into unsafe states of "brittleness" in which additional stress may lead to sudden failure instead of smooth adaptation (Cook & Rasmussen, 2005; Woods & Wreathall, 2008).

The "systems approaches to risk management and integration" meta-narrative (Greenhalgh et al., 2009) acknowledges the role of EHRs as components of complex and dynamic sociotechnical systems, from whose interactions can emerge new modes of safety and risk. This conceptualization views safety as the product of complex interactions at multiple levels and the management of safety as involving awareness of risk and ongoing use of control processes. Thus it relates to a newer approach to safety where the focus is to ensure that the complex system can detect and adapt to new risks (Hale, Heming, Carthey, & Kirwan, 1997; Rankin, Lundberg, Woltjer, Rollenhagen, & Hollnagel, 2013; Saleh, Marais, Bakolas, & Cowlagi, 2010; Woods, Dekker, Cook, Johannesen, & Sarter, 2010). *Resilience* is a term that refers the capability of a complex system to maintain safe operations and the ability to fulfill its objectives despite new pressures or constraints. The resilience engineering approach to safety therefore emphasizes the system's ability to respond to changes in risk (Cook & Nemeth, 2006; Woods & Wreathall, 2008).

Functions identified as fundamental to resilience include monitoring for changes and threats, anticipating changes and being proactive, ensuring the capability to respond to disruptions, learning from past experiences (Hollnagel, 2009), management commitment, flexibility, buffering capacity, awareness of risk

(Carthey, De Leval, & Reason, 2001; Costella, Saurin, & de Macedo Guimarães, 2009; Woods, 2006), and using control systems to maintain functioning in dynamic conditions (Hollnagel, 2008b; Leveson, 2012).

Much of the empirical research on resilience has occurred in the energy, aerospace, petrochemical, and transportation industries (Costella et al., 2009; Hollnagel, Woods, & Leveson, 2006). Compared to these domains, the system dynamics in health care can be considered to be more influenced by the intentions of social actors (Pejtersen & Rasmussen, 1997). Another difference is that preventable bad outcomes are relatively common and often undetected in health care, unlike in these other domains (Amalberti, 2006; Wears, 2012). While there is growing literature on resilience in health care (e.g., Wears, Hollnagel, & Braithwaite, 2013), including health information technology (HIT; Nemeth & Cook, 2007; Skorve, 2010), there are as yet no empirical studies of resilience in management of EHRs.

Understanding successful practices in the management of EHR-related safety is critical given the inherent safety risks associated with EHRs (Ash, Sittig, Campbell, Guappone, & Dykstra, 2007; Karsh, Weinger, Abbott, & Wears, 2010; Sittig & Singh, 2009; Skorve, 2010; Walker et al., 2008) and the rapid adoption of HIT in the United States (Coiera, Aarts, & Kulikowski, 2012). In view of the dynamic complexity of EHR-enabled health care delivery systems (Carayon et al., 2006; Kannampallil, Schauer, Cohen, & Patel, 2011; Sittig & Singh, 2010), we propose that successful safety management of EHRs entails the use of resilience-related practices. The primary goal of this study was to identify the role of resilient safety practices in the management of EHR safety. While the specific practices are situated in the domain of health care, the patterns in how the practitioners cope with complexity may reflect general strategies used in other domains that, like health care, are also trying to maintain resilience while introducing automation into complex sociotechnical systems where boundaries between safe and unsafe can often get fuzzy. Thus, a secondary goal of the study was to go beyond the specific domain and see how these practices relate to more general, domain-independent patterns of dealing with challenges in complex systems (Roth et al., 2013; Woods & Hollnagel, 2006). To collect evidence on practices to successfully manage EHRs within complex sociotechnical systems, we focused on safety practices used in large health care systems that have had many years of experience successfully managing HIT quality and safety.

## METHOD

This study was part of a larger project on EHR safety (Singh, Ash, & Sittig, 2013) that involved numerous interviews, each one focused on one of the facets of HIT identified as key risk areas (Magrabi, Ong, Runciman, & Coiera, 2012; Myers, Jones, & Sittig, 2011). These key risk areas were computerized physician order entry, clinical decision support, test results reporting, communication between providers, patient identification, EHR downtime events, EHR customization and configuration, system-system interface data transfer, and HIT safety-related human skills. Our settings were two very large private health care systems in the United States regarded as successful pioneers in EHR implementation, each with over 20 years of experience using clinical IT systems. These two systems are Partners HealthCare (Teich et al., 1999) and Geisinger Health Systems (Paulus, Davis, & Steele, 2008).

We conducted interviews with 56 key informants (36 from Partners, 20 from Geisinger). The informants were identified by leadership contacts at each facility, based on each informant's expertise in one or more of the key risk areas listed above. Thus, the interviews were broadly focused on EHR safety as it related to the expertise of the key informant rather than only on the use of resilient safety practices. Informants' roles included chief medical information officer, director of nursing informatics, director of pharmacy informatics, director of IT optimization/innovation, risk manager, and physician project specialist. The interviews were semistructured, consisting of questions pertaining to that informant's unique expertise and responsibilities, and included open-ended questions inviting the informant to raise issues of his or her own. Hence a different set of questions

**TABLE 1:** Facility and Roles of Key Informants

| Informants | Interviewed | Mentioned Resilient Practices |
|---|---|---|
| Facility | | |
| Partners | 36 | 25 |
| Geisinger | 20 | 16 |
| Role | | |
| Information technology | 14 | 11 |
| Informatics | 15 | 11 |
| Physicians | 12 | 8 |
| Other clinical operations | 8 | 5 |
| Safety, quality, and security | 7 | 6 |
| Total | 56 | 41 |

was used for each participant. All interviews were recorded and transcribed. Interview transcript lengths ranged from 2,000 words to 16,000 words, averaging approximately 6,500 words.

Conceptually, we approached the analysis of interview data using a systems resilience engineering framework (Costella et al., 2009; Hollnagel, 2009; Woods, 2006). We analyzed interview transcripts using framework analysis (Ritchie & Spencer, 2002), a qualitative methodology that allows for both a "top-down" analysis using an existing framework and a "bottom-up" analysis for emergent themes or patterns. Thus, our analysis accounted for both anticipated resilience-related concepts, such as monitoring, anticipation, and sensitivity to risks, as well as new information that did not readily fit within our framework.

Using an iterative process, the transcripts were reviewed and statements relating to safety practices and any resilience-related concepts were coded as such. Then the coded items were reviewed to more specifically identify in what ways they reflected aspects of resilient safety practices. Afterward, these codes were reviewed and used in a process of iterative categorization in which coded items were grouped according to how they reflected concepts related to resilience. As various categorizations illuminated different patterns, items were recategorized accordingly. From this process, the final set of categories emerged. Then the literature was searched to confirm that each of the category concepts had been identified independently in other research on safety in complex domains (see Discussion). The Atlas.ti software package (ATLAS.ti Scientific Software Development GmbH, Berlin, Germany) was used for coding passages of transcripts. As part of the emphasis on domain-independent patterns, the coding was performed by a research team member with a background in cognitive systems engineering rather than health care operations or health information systems. To enhance credibility of the analysis (Patton, 2002), corroboration was performed by looking for conflicts between our initial coding and categorization results versus coding on general HIT safety issues and detailed interview summaries, all generated independently by other research team members as part of the parent project (Singh et al., 2013).

## RESULTS

### Informants and Statements

From the interview transcripts, we identified 156 statements or references regarding resilient practices from 41 different informants. The informants represented a diverse range of roles and included physicians, IT personnel, and quality and safety personnel (Table 1).

### Categorization

Our analysis generated five main categories, each with two or more subcategories (Table 2). The categories reflect the resilience functions of sensitivity to risks, monitoring, control

**TABLE 2:** Levels of Resilient Practices

| Level | Summary of Practices |
|---|---|
| 1. Sensitivity to fundamental risks<br>A. Awareness of need for monitoring<br>B. Sensitivity to dynamics and interdependencies | The informants recognized the dynamic nature of the HIT systems and how they are used, and the interdependencies between parts of the HIT systems and the larger health care system and how these can affect patient safety risks. |
| 2. Basic monitoring and responding practices<br>A. Processes of testing and tracking<br>B. Processes for responding | They used a very wide range of approaches to monitor and evaluate the performance of the systems, including indicators of risk. Responses to problems involved work on software but also on other facets of the sociotechnical system (e.g., software-enhanced workarounds to mitigate risks due to poor system integration). |
| 3. Management of monitoring and responding practices<br>A. Maintaining capability for testing and tracking<br>B. Maintaining capability for responding<br>C. Enabling safety and quality control | They had practices to ensure continued capability to effectively monitor and respond to risks. They used their understanding of dynamics and interdependencies to use resources more efficiently. |
| 4. Sensitivity to risks beyond the horizon<br>A. Processes and mechanisms for being proactive<br>B. Controlling risk at governance level | Practices were in place to proactively assess for risks and to deliberately avoid installing software that would unduly increase risk. |
| 5. Reflecting on risks with the safety and quality control process itself<br>A. Limitations of monitoring methods<br>B. Sensitivity to failure in the quality control process | Many of the informants were aware of limitations with the methods used in detecting and managing risk. Furthermore, some were aware of limitations and overly narrow system boundaries in the conceptual model of the system used to guide the quality control process. |

*Note.* HIT = health information technology.

systems, responding, anticipation, and mindfulness. Examples and details for each category level and subcategory are in Table 2.

### 1. Sensitivity to Fundamental Risks

Statements in this category referred to the organization's awareness of basic threats to the safe operation of HIT systems.

> We absolutely have to test every one of them [monthly software patches from vendor]. . . . We may report an issue . . . and they [the vendor] work on it, and they have a fix for it ready. . . . They say, "OK, yeah, we have this ready. We can send you the fix." But when we do that [implement the fix], that fix also touches all these other things . . . and all those other things also had fixes. So now this one fix you want, you have to bring in 50 others.

*A. Awareness of the need for ongoing safety analysis, including review and documentation.* Informants described the need for testing and post-implementation monitoring, even when software was off-the-shelf without any add-ons ("No one ever just puts it in place and lets it go"). Informants also mentioned periodic

reviews of policies and order sets and revisiting decisions to disable particular EHR safety features. They mentioned the importance of documenting the processes by which EHR components are implemented and monitored, and documenting workflow because workflows change. Two informants expressed sensitivity to the risks faced by health care facilities that are new to EHRs: "They don't know what they don't know."

*B. Sensitivity to dynamics and interdependencies in these sociotechnical systems*. Some comments emphasized the volatility of both the EHR system and the larger context of the health care industry. Informants mentioned several factors that changed the risk profile of the system over time, including the increasing length of patient notes ("note bloat"), providers' alert fatigue, and customization of the EHR. One informant pointed out how risks related to patient identification could affect a broad range of functions, from medication administration to food delivery.

Several comments referred to the interface between the EHR and other system components. For instance, one informant recounted a problem that resulted when another application vendor made changes to its EHR software without informing the facility, which led to problems with the integration of the updated software with other software in place. Another informant described the complexity of adding a new drug into the order entry system; in order for the drug to be dispensed correctly, it also needed to be added to other parts of the system (pharmacy and bar-coding administration systems). These are examples of the informants' sensitivity to the problem of asynchronous evolution of subsystems within integrated systems, whereby changes in one subsystem lead it to become incompatible with the other subsystems that lag behind (Leveson et al., 2006).

Finally, informants were aware of how changes in government policies, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA; Department of Health and Human Services, n.d.) and "meaningful use" criteria (Blumenthal & Tavenner, 2010), affect workflow and how these changes in workflow in turn affect software configuration and use (Campbell, Guappone, Sittig, Dykstra, & Ash, 2009). The interdependency between software and workflow was also acknowledged in the inclusion of workflows into the software testing process and in a vendor-led process of requirements and specifications validation.

### 2. Basic Monitoring and Responding Practices

Statements in this category referred to ways in which facilities ensured that their EHRs continued to operate as designed and fulfill their basic functions.

> We do a tremendous amount of testing before any release upgrade. The team reads all of the release notes. We do integrative testing, unit testing. We do a dry run. We do testing where we have two weeks where almost all hands are on deck just the first two weeks that the new software is loaded into a test system to see what we're breaking.

*A. Processes of testing and tracking*. Informants used various testing practices and other strategies to assess the functioning of EHR systems. These included testing in development platforms and in the live platforms using test patients. One facility used the Leapfrog Group's safety assessment tool for computerized physician order entry systems (Classen, Avery, & Bates, 2007).

Software upgrades were often mentioned as an impetus for testing. The testing required by upgrades encompasses not only the upgrade itself but also the ancillary systems that are integrated with the upgraded software and the post-upgrade patches that are developed by the vendor as problems are discovered. System configurations were tested to ensure compatibility with clinical workflows. In addition, several informants mentioned testing the integration between components. One informant specifically described a test that included not only sending information to the pharmacy but also calling the pharmacy to ask how the information was displayed on the screen.

Informants mentioned practices designed to encourage incident reporting and regular review of IT-related safety concerns. Other sources of information about risks included announcements from the vendors and networking with other facilities that use the same EHR systems.

*B. Processes for responding as part of quality and safety control feedback.* Informants presented many different ways they continually adjusted and corrected EHR systems. There were processes and tools that facilitated rapid response to EHR issues by monitoring for acute problems and alerting staff. For problems with a vendor's software, responses could involve informing the vendor of problems discovered and sharing information about problems and solutions with other facilities that use that vendor's EHR.

Reports of problems and incidents were reviewed with a focus on identifying potential areas for improvement and proposing solutions. Responses could be quite thorough in order to maintain safety. In one case, when it was discovered that many allergies had been entered into records not as coded data but as free text, which the drug allergy checking algorithm could not detect, the facility manually recoded the allergies in all the affected records.

The types of responses mentioned also included work-arounds. For example, because a software system for managing dosing of anticoagulant medication did not integrate well with the order entry system, there was a risk that patients would be prescribed the wrong dosage. In response, the hospital developed software that prompted providers to double-check the dosages when discharging a patient on anticoagulants. A similar solution was developed to prompt providers to double-check certain high-risk medications during the medication reconciliation process performed when patients are discharged from the hospital. In addition to exploring work-arounds as possible short-term solutions for risks, facilities assessed the proposed work-arounds for any risks they might introduce if they were implemented.

### 3. Management of Monitoring and Responding Practices

Statements in this category referred to what the facilities did to ensure they were able to continue to oversee and correct HIT operations.

> One thing we try to stress, from a production support standpoint, is that when you do your project life cycles, there should be a line item there for an error [management] process.

*A. Maintaining capability for testing and tracking*. Informants stressed the importance of maintaining resources for ongoing monitoring and review. They described staffing resources made available for such functions, including people to monitor logs of errors in information transmission and people to perform various manual testing operations. Organizational structures were changed to use staffing resources more effectively and efficiently. For example, groups of informaticians and risk management specialists were moved to integrate better with front-line care staff.

Informants mentioned resources dedicated to help people report safety risks or incidents. These include incentives for physicians, systems to track the status of the facility's response to the issue, and specific tools to enable providers to easily comment on the appropriateness of decision support recommendations.

To use testing resources efficiently, they were applied based on the likelihood of uncovering something important. The degree of testing was adjusted to the estimated impact of the implementation on clinical processes. For example, informants mentioned how a forthcoming major update to the EHR was undergoing rigorous testing but that smaller changes to the system received less intensive testing. They also mentioned how most problems were usually discovered early on, in the pilot testing, which allowed for corrections to be made before the software was fully implemented.

Software tools to support monitoring were also mentioned. These included tools for automatically monitoring the interfaces between subsystems and a tool for tracking safety issues (Walker, Hassol, Bradshaw, & Rezaee, 2012). One facility replaced periodic error reports with continuous error log monitoring. Another use of technology was the automation of a multistep software testing process. Scripts were used to efficiently run a battery of standard tests. One informant mentioned testing the accuracy and potential impact of decision support algorithms in a way that did not impact providers. The algorithms were run in "stealth mode," without

showing the alert messages to clinicians but storing results in a log for review. In an additional example of the use of tools to detect problems early on, a thermal scanner was used to detect unusually hot electrical connections between devices in the data center serving the IT system.

As the use and scale of the EHR evolved, tools were created in response to the accompanying risks. One evolving risk was from bad information accidently entered into charts due to imprecise copying and pasting from older notes in the EHR, instead of clinicians manually entering in all the text documentation (Hammond, Helbig, Benson, & Brathwaite-Sketoe, 2003). One facility developed a tool to monitor the extent of copying and pasting in their charts. Another tool was developed to identify instances of potential mismapping between a patient and a record. It detected unusual modifications made to patient identification information (e.g., updating birthday or full name), as would occur when Person B's record was being altered under the false assumption that it belonged to Person A. Another example of software developed in response to a problem was a tool that automatically checked for addressing and routing problems that could prevent correct delivery of pathology reports to the ordering providers.

*B. Maintaining capability for responding*. Informants also stressed the importance of maintaining the resources necessary for responding to problems that arise. Furthermore, one mentioned the value of a process for ensuring resolution of issues by escalating unresolved ones to relevant leadership. Another informant emphasized preemptively validating particular error management processes to ensure that the team can fix any known problems with software should they occur after the software is implemented on the live platform. In other words, a team may set up an error on a test platform and see if it is possible to repair it with the constraints present on the live production platform.

Informants mentioned a few specific examples of maintaining response capabilities. As instructed by the supervisor, a junior IT person performed a maintenance operation on a live in-use (but redundant) part of the IT infrastructure in order to become more comfortable with working on live in-use IT systems should the need arise. To be available in case of problems with a significant upgrade being installed on the live system, a large IT team remained on site the entire night. In order to implement changes more rapidly, some informaticians were dedicated to and co-located with specific front-line clinical operations.

*C. Enabling safety and quality control in an effective and efficient way*. Some informants mentioned practices for securing resources for quality improvement. One informant used data from assessments and monitoring to facilitate budget negotiations for resources for safety.

Other practices mentioned were to use the resources more effectively and efficiently. One example was embedding informatics staff with clinical groups in order to speed up the cycle of problem detection and response. Many practices involved using IT tools to support the quality improvement process, such as providing information to stakeholders via databases and reporting engines. Informants mentioned specific examples of using IT to improve the process of monitoring performance and implementing adaptations. In one example concerning the tool used by clinicians to view information on patients who had been transferred into that facility, software tracked the way clinicians customized the display of information fields. That data were then used to identify which fields to prioritize in the redesigns of the patient transfer forms. Another example was a practice aimed at reducing alert fatigue. Pop-up warnings for drug-drug interactions were monitored to see which ones were overridden by providers on a consistent basis; those warnings for which the providers had found no value were removed in order to reduce alert fatigue (Phansalkar et al., 2010).

## 4. Sensitivity to Risks Beyond the Horizon

Statements in this category referred to facilities' strategies of predicting and proactively managing problems that could occur in future HIT systems and in the larger sociotechnical system beyond the HIT system itself.

> We have to be proactive here. . . . You know why? Because if you're up at 2 o'clock in the morning and trying to deal

> with a production problem where someone's life may be in danger, you want to be proactive. You want to have the work done ahead.

*A. Processes and mechanisms for being proactive.* Several informants mentioned the role of testing and evaluation to proactively identify problems. One informant stressed the close evaluation of software upgrades to facilitate responding to potential problems during the upgrade process. Another mentioned that "most of the bigger issues get found in pilot phase. . . . We can . . . make corrections before it even gets rolled out anywhere else."

Informants mentioned the use of reviews to identify potential hazards with new EHR implementations. In preparation for going live with a new inpatient system, one facility conducted a thorough prospective risk assessment, involving a wide range of clinical staff (Hundt et al., 2013). Another type of prospective risk assessment mentioned was validation sessions with the vendor of an EHR, to assess fit with workflows and identify gaps.

Additionally, one informant stressed the need for resources and processes to make sure issues were detected proactively and were acted upon. This included having effective communication channels with leadership to ensure that issues get addressed. Informants at both facilities mentioned having governance committees that reviewed proposed additions or modifications to the clinical IT systems and changes to clinical knowledge structures (e.g., decision rules, templates). These committees included people from clinical, IT, operations, and risk management. Also mentioned were efforts to ensure that representatives of various groups, including end users, were involved in HIT decisions.

Informants mentioned processes to keep leadership and other stakeholders informed about the risks in the system. This included reports to HIT and clinical steering committees, reviews of significant safety issues with the management team and the executive committee, and notifications to senior leadership (Belmont et al., 2013). Another practice was a daily teleconference involving representatives from various locations in the system, in which open issues including safety and EHR concerns were discussed.

*B. Controlling risk at governance level.* Informants also shared examples concerning how knowledge of potential risks was used in decisions about IT implementation. These examples included: deciding to not install some software because of problems detected ahead of time, disabling some EHR functionality because of the associated risks, and installing major version upgrades only after the subsequent wave of software patches from the vendor had been issued.

One facility was migrating from a custom best-of-breed system (using components from various developers) to an integrated off-the-shelf system in response to the risks posed by continued use of a "fragmented" and "siloed" system. Informants also mentioned instances where investments in new HIT-based safety projects were made only after explicit assessments of risks.

Informants mentioned using anticipated risks to inform decisions about resource investments for safety. One informant stressed how there would still be a need for resources for EHR configuration and evaluation even after the pending migration to an off-the-shelf system. Another mentioned the need to expand the current IT backup infrastructure to keep pace with the rapid growth of HIT in the facility.

Identifying future needs could also involve factors outside the immediate focus of EHR safety. One informant gave an example of this involving the meaningful-use EHR reimbursement requirement (Blumenthal & Tavenner, 2010) concerning greater use of patient portals. Because recent lab results and current medication lists were now more visible to patients, the clinicians became under pressure to make sure those parts of the record were accurate and up-to-date. However, due to workforce distributions and rules regarding scopes of practice, nonphysicians were unable to offload the extra work now required of the primary care physicians.

### 5. Reflecting on Risks With the Safety and Quality Control Process Itself

Statements in this category referred to methods by which the facilities recognized and addressed ways the safety and quality control process itself could fail.

> What the [information systems] leader thinks is happening, in fact, isn't necessarily what's happening.

*A. Limitations of monitoring methods*. Informants emphasized the importance of the quality and accuracy of the information in the system, one stating that "the flow of information about potential errors needs to be very high quality." The limitations of incident reports and verbal feedback were mentioned by two informants, who described them as incomplete sources of information.

Informants mentioned the limitations of testing and how problems have been encountered in live EHR systems despite thorough prior testing. They suggested many reasons. Problems related to specific and infrequently encountered interactions or other circumstances would be more likely to appear only during widespread regular use, not during limited, pre-live testing. Automated testing tools would not necessarily work for a facility's particular customizations, nor would testing environments necessarily capture all the relevant aspects of the real world system. Testing may not have encompassed the range of upstream and downstream components that could be involved in a safety issue.

Informants referred to alternative methods used to mitigate the limitations of current monitoring methods. Focus groups and surveys with end users were used to solicit feedback on patient transfer and handoff tools. After scripts and configurations of IT products were set up, a second IT person would review them before they were implemented.

The way users performed tasks with the software was monitored to see if they had to perform work-arounds due to shortcomings with the software and its fit with the users' workflows. Developers used a similar approach to evaluate a handoff tool designed to provide all the necessary information for clinical staff taking over responsibility of patients. Clinicians were asked if any information was missing and also what problems arose or additional tasks were required as a result of information not being available.

*B. Sensitivity to failure in the quality control process.* One informant mentioned some limitations with the quality control process itself related to software and workflow validation. One aspect of this was how the introduction of new software functionality almost always occurred in the context of other concurrent changes, meaning that confounding factors made it difficult to establish the particular role of the EHR intervention in affecting outcomes. To improve the quality control process itself, facilities monitored the implementation of EHR interventions more closely and implemented tools to support collaboration across departments.

Some informants raised questions about the underlying assumptions regarding the functioning and scope of the EHR system. One pointed out that many patients move about the country but still need continuity of care, thus requiring EHRs to support real-time health information exchange over a much wider geographic range of clinical partners than currently supported. Addressing the need for continuity and coordination of care across different facilities, another informant suggested that EHRs could and should do more to support coordination beyond the current function of simply exchanging minimal clinical data.

One informant mentioned an effort illustrating how IT managers were willing to acknowledge the risk of problematic inaccuracies in their own interpretations of the current state of the EHR. Work on mitigating these limitations included plans for software to automatically capture additional data on the current state of the EHR.

## Credibility Assessment

Our findings were evaluated against the independently generated codes on HIT safety in general and the independently authored detailed summaries of the interviews for each of the facilities, all generated as part of the parent project (Singh et al., 2013). There were no conflicts between our findings and those coding results and detailed summaries.

To confirm that the categories reflect practices at both facilities, we assessed the distribution of the topics of the comments within and across the two facilities. A chi-square test of the number of comments from Partners and Geisinger for each of the five levels indicates no significant difference in proportions across facilities and category levels ($p = .310$).

## DISCUSSION

### Categorization of Statements About Resilient Safety Practices

We conducted interviews with 56 key informants from two large health care systems recognized as leaders in use of HIT and EHRs. The interviews focused on HIT and EHR safety issues related to the various roles of the informants, which included IT, informatics, clinical providers, and safety and quality managers. Forty-one participants mentioned practices that reflected some element of the resilience approach to safety. Overall, there were 156 references to resilient practices. The practices covered a wide range of activities related to resilience in health care systems. For instance, almost all of Carthey et al.'s (2001) 20 indicators of institutional resilience in health care systems are reflected in the set of practices. The results also show how these facilities engaged in practices that support different levels of HIT safety: the functioning of the HIT systems themselves, the co-evolution of workflow and HIT systems to enhance performance, and the application of IT to new ways for facilitating safety (Sittig & Singh, 2012).

Our analysis generated a categorization of five levels, each with two or more subcategories. The levels reflect some primary resilience functions: sensitivity to risks (Costella et al., 2009; Nemeth, 2008; Woods et al., 2010), monitoring risks (Hollnagel, 2009; Wreathall, 2011), using control systems to track and modify performance of safety-related operations (Hollnagel, 2008b; Leveson, 2012), maintaining the capability to respond (Hollnagel, 2009; Pariès, 2011), anticipating changes and being proactive (Hollnagel, 2009; Klein, Snowden, & Pin, 2010; Woods, 2011), and mindfulness and reflection on the risks related to the safety management process itself (Reason, 2008; Woods, 2006; Woods et al., 2010; Woods, Schenk, & Allen, 2009).

The practices that reflect resilience are certainly not the only practices important for HIT safety. The importance of best practices in software design, usability testing, and implementation have been stressed (Middleton et al., 2013; Office of the National Coordinator, 2012). Other developments in systems safety, such as high reliability theory (Roberts, 1990), can also offer some contributions. However, the results here emphasize the need for facilities to practice active monitoring and management beyond the initial development and implementation stages. They include practices regarding managing resource constraints and other trade-offs, which is not addressed by high reliability theory.

### Generic Patterns That Facilitate Resilience

Because we interviewed informants who were engaged in the real-world work of managing HIT systems in large health care systems, we have made certain that our findings are ecologically valid and grounded in real-world practice. In accordance with the research agenda of cognitive systems engineering (Woods & Hollnagel, 2006), it is important to complement this focus on a specific context by addressing generic, domain-independent patterns in how work is accomplished in complex systems (i.e., macrocognitive functions; Cacciabue & Hollnagel, 1995). We look beyond the specific categories by exploring the commonalities among them, establishing an interpretation of the findings in terms of underlying functions that facilitate resilience.

*Reflection.* The relationship between the five category levels can be seen in terms of how a critical and reflective view of one level is necessary for the implementation of the subsequent level.

- Level 1 (sensitivity to fundamental risks) is the critical recognition of dynamic risks to which the system is vulnerable.
- Even though the risks are ensconced in uncertainty, in Level 2 (basic monitoring and responding practices), the risks are seen as subject to prediction and management via systematic measurement and intervention.
- In Level 3 (management of monitoring and responding practices), these systematic measurements and interventions are acknowledged as operations that require resources and oversight.
- This ongoing need—for resources and oversight to manage risk—presents pressures for efficiency and effectiveness. Thus in Level 4 (sensitivity to risks beyond the horizon), there is the recognition

of the need for planning, anticipation of future demands, and proactive management.
- Because of the anticipation of future demands and planning for them, there is in Level 5 (reflecting on risks with the safety and quality control process itself) recognition of the potential problems owing to the limits of the current safety management approach itself.

Reflection is related to a basic pattern in how cognitive systems manage complex work. The capacity to shift and contrast perspectives is essential in exploring complex situations, generating alternate courses of action, and coordinating work with others (Woods et al., 2010; Woods & Hollnagel, 2006;). The presence of multiple potential points of view encourages reflection and critical evaluation of a given point of view (Hoffman & Woods, 2011). Reflection is also related to one of the basic functions required for resilience: learning (Hollnagel, 2009, 2011). As part of organizational learning (Argyris & Schön, 1996), reflective practice (Schön, 1983) involves being able to detect problems with and make corrections for one's current conceptual model or perspective. This practice is called "double-loop" learning, as it serves as an overarching control loop for improving one's performance at one's normal control loop tasks (Argyris, 1977).

*Transcending boundaries.* In all of the category levels, there are examples of organizational or technical boundaries being crossed as part of efforts to support resilience. The boundaries of the IT system, as implied by standard HIT use cases (e.g., Cusack et al., 2009), are crossed in the work of HIT systems safety. The informants were sensitive to interactions and risks from various sources, not just IT. They considered impacts to safety from diverse influences, such as external regulations (HIPAA and meaningful use, and also scope of practice) and the effect of patients' direct access to their records. As a means of learning about risks and responding to them, it was a regular practice to communicate about problems with both the vendor and other health care facilities external to their own health care system. Furthermore, as presented in Level 5, Part B (sensitivity to failure in quality control process), a few informants explicitly questioned the scope of the HIT system itself.

One definition of resilience is "stretching at and beyond boundaries" (Woods, Chan, & Wreathall, 2013). This definition emphasizes how fixation (De Keyser & Woods, 1990) on predefined boundaries or scopes of influence can hamper safety management (Reiman & Rollenhagen, 2011). Important risks and opportunities may be overlooked if there is too narrow a view taken on the scope of activities to be monitored or leverage points to be utilized (Woods et al., 2010). In contrast, the function of "seeing the bigger picture" can facilitate resilience.

*Sharp-end stakeholders.* Across the category levels, there are examples of sharp-end practitioners (e.g., physicians, nurses) serving as active stakeholders in the safety management process, serving to establish a degree of distributed control of the operations of the HIT systems. This role is in contrast to the idea that sharp-end practitioners under automated supervisory control can respond to the technology only through compliance or resistance (see Greenhalgh et al., 2009). Resilience is enhanced by facilitating influence up the chain of command (Carthey et al., 2001) and by sharing some control with sharp-end practitioners (Woods, 2006; Woods & Branlat, 2010). Thus, the function of distributing and coordinating the control of safety across the blunt-end/sharp-end spectrum may facilitate resilience.

These two health care systems established and maintained practices and tools for the purpose of obtaining input from the front-line providers. Informatics and risk management staff were moved to front-line clinical organizations to facilitate problem detection and solving. Tools were developed for end users to report issues and track the organization's response. Evaluations of the IT system included identifying which parts were helpful and not helpful for end users (e.g., drug-drug interaction alerts, fields in patient transfer templates). Of course, these practices constitute only a small range of the possible ways control of the HIT system can be distributed. However, they do show the value of involving sharp-end practitioners as a part of ongoing system management, versus only during an initial requirements elicitation or usability evaluation phase.

## Recommendations and Future Work

The U.S. health care system is undergoing a significant transformation as more and more health care facilities, including smaller clinics and private practices, adopt EHRs and other HIT. Proposals for enhancing EHR safety have emphasized user-centered design approaches and usability testing, and the use of incident reporting, collection, and analysis systems at a large scale (Middleton et al., 2013; Office of the National Coordinator, 2012). Although these are valuable and necessary methods for improving safety, the results of this study suggest that EHR safety also depends on persistent testing and monitoring (Sittig & Classen, 2010; Walker et al., 2008), especially in terms of ongoing appraisal of sociotechnical factors that affect the use and maintenance of the EHR.

Although smaller clinics and private practices have less overall complexity than large health care systems, they are still subject to dynamics and interdependencies that affect risk. Vast numbers of the facilities now adopting HIT lack experience with and/or resources for safety assessment and management of HIT systems (Walker et al., 2008). There is a high demand for workers with HIT operation skills (Furukawa, Vibbert, & Swain, 2012; Hersh & Wright, 2008). These conditions will exacerbate the risks related to dynamics and interdependencies.

By identifying the resilient practices used in a domain, requirements for training and tools to support those practices can be developed (Hale, Guldenmund, & Goossens, 2006; Smith, Davis Giardina, Murphy, Laxmisan, & Singh, 2013). The training for HIT workforce development should address post-implementation quality and safety control, including practices for resilience in complex sociotechnical systems.

The tools available for IT system administrators are poor at supporting the tasks involved in ongoing supervision and management of IT systems (Barrett et al., 2004). Such deficiencies are exacerbated in complex sociotechnical systems, like health care. However, by designing the tools and processes to support collaboration and sensemaking (e.g., Watts-Perotti & Woods, 2009), they will better support safety management. Resilience will be further enhanced by incorporating ways for sharp-end practitioners to participate in safety and quality control of IT systems.

Because of the large numbers of new EHR adopters lacking in relevant skills and resources, it is more critical to develop techniques to support awareness of the risks (Level 1) and their monitoring and management (Level 2). One method to support awareness of risks is to identify risk indicators that are easily detectable (Reason, 2008; Sittig & Singh, 2013). Ways to facilitate monitoring include the development of easy-to-use measures (Sittig, Campbell, Guappone, Dykstra, & Ash, 2007) and safety audit tools (Singh et al., 2013).

The utility of the information collected via monitoring can be enhanced through cognitive engineering approaches aimed at facilitating interpretation of and responses to the information (Endsley, 1988; Militello & Klein, 2013; Vicente, 1999). This approach includes designing the display of and interaction with the information such that it does not induce cognitive fixation on system boundaries and instead helps the practitioners understand and manage the safety issues as they manifest across system boundaries.

There are also techniques to support the macrocognitive function of reflection, identified as a facilitator of resilient practices across the categorization levels. Methods include doing "premortem" analyses of proposals (Klein, 2007) and generating scenarios to explore new potential risks (Carroll, 2000). Another method is to make explicit the trade-off decisions between goals that organizations face (e.g., being both efficient and thorough), thereby encouraging stakeholders to reflect on how safety is being managed (Branlat & Woods, 2011; Hoffman & Woods, 2011).

## Limitations

In this study, we collected data from only two health care systems. However, because both are leaders in the strategic application of HIT, and the focus of the study is on the practices used by health care systems with the greatest experience and success in HIT use, this limitation should not be seen as a threat to appropriate generalizability (Lipshitz, 2010). The two facilities are different: Partners HealthCare is a loosely connected system of hospitals and clinics in a dense

metropolitan area, using various EHR tools, many developed internally, whereas Geisinger Health Systems is a tightly integrated system in a nonmetropolitan area, using a leading commercial EHR. This difference in conjunction with the overlap of resilient practices across the two different facilities strengthens the generalizability.

This study did not include analysis of contrasting cases to check if facilities with less experience or success in HIT management also showed evidence of these practices. However, we suspect those with less success are not likely to use the same practices, as there are some indications that differences in HIT safety outcomes are related to HIT implementation practices and management. For example, Han et al. (2005) reported on the unexpected increase in mortality at one facility following implementation of a commercially sold computerized order entry system, whereas Longhurst et al. (2010) found a decrease in their facility's mortality rate following implementation of the same vendor's EHR but with the use of much improved processes and management techniques (Sittig, Ash, Zhang, Osheroff, & Shabot, 2006).

Another limitation is that the information about the practices came from interviews. We did not perform observations or otherwise evaluate for independent evidence of the practices. However, almost all of the practices were mentioned by more than one informant. Some of these facilities' practices have been the subject of scientific publications (Hundt et al., 2013; Paulus et al., 2008; Phansalkar et al., 2010; Teich et al., 1999; Walker et al., 2012). Furthermore, these resilient practices were volunteered during interviews about HIT safety in general (as pertaining to the informant's role); the interviews were not conducted as cognitive task analysis interviews designed to elicit specific types of strategies. This suggests that these practices were strongly associated with general HIT safety in the minds of the informants. A methodology focused on eliciting resilience-specific practices might have uncovered additional ones.

## CONCLUSIONS

Our study of quality and safety control processes used for HIT by two leading health care systems shows that resilient safety practices are an important part of safety in complex sociotechnical systems. The practices mentioned were categorized into five areas: (a) awareness of dynamics and interdependencies affecting risk, (b) established monitoring and responding practices, (c) management of resources and methods, (d) anticipating risks, and (e) reflecting on limitations of the safety management process itself. These practices were facilitated by the functions of reflective learning, the capability to revise system boundaries, and systematic sharing of control with sharp-end practitioners.

## ACKNOWLEDGMENTS

The SAFER project is supported through a subcontract from Westat (HHSP-23320095655WC0095655; Anticipating the Unintended Consequences of Health IT) funded by the Office of the National Coordinator for Health Information Technology (ONC) (HHSP23337003T; to Drs. Sittig, Ash, and Singh) and the VA HSR&D Center for Innovations in Quality, Effectiveness and Safety (#CIN 13-413) at the Michael E. DeBakey VA Medical Center, Houston, Texas (to Dr. Singh). The funders had no role in the design and conduct of the study; collection, management, analysis, and interpretation of the data; preparation, review, or approval of the manuscript; and decision to submit the manuscript for publication. Andrea Bradford, PhD, provided medical editing services on behalf of the authors. The views expressed in this article are those of the authors and do not necessarily represent the views of the Department of Veterans Affairs or the Office of the National Coordinator for Health Information Technology.

## REFERENCES

Aarts, J. (2011). Towards safe information technology in health care. *Information, Knowledge, Systems Management*, *10*, 335–344.

Amalberti, R. (2006). Optimum system safety and optimum system resilience: Agonistic or antagonistic concepts. In E. Hollnagel, D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 253–274). Farnham, UK: Ashgate.

Argyris, C. (1977). Organizational learning and management information systems. *Accounting, Organizations and Society*, *2*, 113–123.

Argyris, C., & Schön, D. A. (1996). *Organizational learning 2*. Boston, MA: Addison-Wesley.

Ash, J. S., Sittig, D. F., Campbell, E. M., Guappone, K. P., & Dykstra, R. H. (2007). Some unintended consequences of clinical decision support systems. In *AMIA 2007 Annual Symposium*

*Proceedings* (pp. 26–30). Retrieved from http://www.ncbi.nlm.nih.gov/pmc/issues/177326/

Bainbridge, L. (1983). Ironies of automation. *Automatica*, *19*, 775–780.

Barrett, R., Kandogan, E., Maglio, P. P., Haber, E. M., Takayama, L. A., & Prabaker, M. (2004). Field studies of computer system administrators: Analysis of system management tools and practices. In *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work* (pp. 388–395). New York, NY: ACM.

Belmont, E., Chao, S., Chestler, A., Fox, S., Lamar, M., Rosati, K., . . . Valenti, A. (2013). *Minimizing EHR-related serious safety events*. Washington, DC: American Health Lawyers Association. Retrieved from http://www.healthlawyers.org/hlresources/PI/InfoSeries/Documents/For%20the%20Healthcare%20Executive/Minimizing%20EHRSSE.pdf

Blumenthal, D., & Tavenner, M. (2010). The "meaningful use" regulation for electronic health records. *New England Journal of Medicine*, *363*, 501–504.

Branlat, M., & Woods, D. (2011, June). *How human adaptive systems balance fundamental trade-offs: Implications for polycentric governance architectures*. Paper presented at the 4th Resilience Engineering International Symposium, Sophia Antipolis, France.

Cacciabue, P. C., & Hollnagel, E. (1995). Simulation of cognition: Applications. In J. M. Hoc, P. C. Cacciabue, & E. Hollnagel (Eds.), *Expertise and technology: Cognition and human-computer cooperation* (pp. 55–73). Hillsdale, NJ: Lawrence Erlbaum.

Campbell, E. M., Guappone, K. P., Sittig, D. F., Dykstra, R. H., & Ash, J. S. (2009). Computerized provider order entry adoption: Implications for clinical workflow. *Journal of General Internal Medicine*, *24*, 21–26.

Carayon, P., Schoofs Hundt, A., Karsh, B. T., Gurses, A. P., Alvarado, C. J., Smith, M., & Flatley Brennan, P. (2006). Work system design for patient safety: The SEIPS model. *Quality & Safety in Health Care*, *15*(Suppl. 1), i50–i58.

Carroll, J. M. (2000). Five reasons for scenario-based design. *Interacting With Computers*, *13*, 43–60. doi:10.1016/S0953-5438(00)00023-0

Carthey, J., De Leval, M. R., & Reason, J. T. (2001). Institutional resilience in healthcare systems. *Quality in Health Care*, *10*, 29–32.

Classen, D. C., Avery, A. J., & Bates, D. W. (2007). Evaluation and certification of computerized provider order entry systems. *Journal of the American Medical Informatics Association*, *14*, 48–55. doi:10.1197/jamia.M2248

Coiera, E., Aarts, J., & Kulikowski, C. (2012). The dangerous decade. *Journal of the American Medical Informatics Association*, *19*, 2–5.

Committee on Data Standards for Patient Safety. (2003). *Key capabilities of an electronic health record system: Letter report*. Washington, DC: National Academies Press. Retrieved from http://www.nap.edu/openbook.php?record_id=10781

Cook, R., & Rasmussen, J. (2005). "Going solid": A model of system dynamics and consequences for patient safety. *Quality and Safety in Health Care*, *14*, 130–134. doi:10.1136/qshc.2003.009530

Cook, R. I., & Wood, D. D. (1994). Operating at the Sharp End: The Complexity of Human Error. In M. S. Bogner (Ed.), *Human Error in Medicine* (pp. 255–310). Erlbaum.

Cook, R.I., & Nemeth, C. (2006). Taking things in one's stride: Cognitive features of two resilient performances. In E. Hollnagel, D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 205–221). Farnham, UK: Ashgate.

Costella, M., Saurin, T., & de Macedo Guimarães, L. (2009). A method for assessing health and safety management systems from the resilience engineering perspective. *Safety Science*, *47*, 1056–1067.

Cusack, C., Byrne, C., Hook, J., McGowan, J., Poon, E., & Zafar, A. (2009). *Health information technology evaluation toolkit: 2009 update* (No. AHRQ Publication No. 09-0083- EF). Washington, DC: Agency for Healthcare Research and Quality. Retrieved from http://healthit.ahrq.gov/sites/default/files/docs/page/Evaluation%20Toolkit%20Revised%20Version.pdf

De Keyser, V., & Woods, D. D. (1990). Fixation errors: Failures to revise situation assessment in dynamic and risky systems. In A. G. Colombo & A. Saiz de Bustamante (Eds.), *Systems reliability assessment* (pp. 231–251). Dordrecht, Netherlands: Springer.

Dekker, S. (2006). *The field guide to understanding human error* (1st ed.). Farnham, UK: Ashgate.

Department of Health and Human Services. (n.d.). *Summary of the HIPAA Security Rule*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors and Ergonomics Society 32nd Annual Meeting* (pp. 97–101). Santa Monica: CA: Sage.

Furukawa, M., Vibbert, D., & Swain, M. (2012). *Hitech and Health IT jobs: Evidence from online job postings* (No. ONC Data Brief No. 2). Washington, DC: Office of the National Coordinator for Health Information Technology. Retrieved from http://www.healthit.gov/sites/default/files/pdf/0512_ONC-DataBrief2_JobPostings.pdf

Greenhalgh, T., Potts, H., Wong, G., Bark, P., & Swinglehurst, D. (2009). Tensions and paradoxes in electronic patient record research: A systematic literature review using the meta-narrative method. *Milbank Quarterly*, *87*, 729–788.

Grol, R., & Grimshaw, J. (2003). From best evidence to best practice: Effective implementation of change in patients' care. *The Lancet*, *362*, 1225–1230.

Hale, A., Guldenmund, F., & Goossens, L. (2006). Auditing resilience in risk control and safety management systems. In E. Hollnagel, D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 289–314). Farnham, UK: Ashgate.

Hale, A. R., Heming, B. H. J., Carthey, J., & Kirwan, B. (1997). Modelling of safety management systems. *Safety Science*, *26*, 121–140.

Hammond, K., Helbig, S., Benson, C., & Brathwaite-Sketoe, B. (2003). Are electronic medical records trustworthy? Observations on copying, pasting and duplication. In *AMIA 2003 Annual Symposium Proceedings* (pp. 269–273). Retrieved from http://www.ncbi.nlm.nih.gov/pmc/issues/131751/

Han, Y., Carcillo, J., Venkataraman, S., Clark, R., Watson, S., Nguyen, T., . . . Orr, R. (2005). Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. *Pediatrics*, *116*, 1506–1512.

Hersh, W., & Wright, A. (2008). What workforce is needed to implement the health information technology agenda? Analysis from the HIMSS Analytics™ database. In *AMIA 2008 Annual Symposium Proceedings* (pp. 303–307). Retrieved from http://www.ncbi.nlm.nih.gov/pmc/issues/177327/

Hoffman, R. R., & Woods, D. D. (2011, May/June). *Simon's slice: Five fundamental tradeoffs that bound the performance of human work systems*. Paper presented at the 10th International Conference on Naturalistic Decision Making, Orlando, FL.

Hollnagel, E. (2008a). The changing nature of risk. *Ergonomics Australia Journal*, *22*, 33–46.

Hollnagel, E. (2008b). Safety management: Looking back or looking forward. In E. Hollnagel, C. Nemeth, & S. Dekker (Eds.), *Resilience engineering perspectives* (Vol. 1, pp. 63–77). Farnham, UK: Ashgate.

Hollnagel, E. (2009). The four cornerstones of resilience engineering. In C. Nemeth, E. Hollnagel, & S. Dekker (Eds.), *Resilience engineering perspectives* (Vol. 2, pp. 117–134). Farnham, UK: Ashgate.

Hollnagel, E. (2011). To learn or not to learn, that is the question. In E. Hollnagel, J. Pariès, D. Woods, & J. Wreathall (Eds.), *Resilience engineering in practice* (pp. 193–198). Farnham, UK: Ashgate.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Farnham, UK: Ashgate.

Hsieh, T. C., Kuperman, G. J., Jaggi, T., Hojnowski-Diaz, P., Fiskio, J., Williams, D. H., . . . Gandhi, T. K. (2004). Characteristics and consequences of drug allergy alert overrides in a computerized physician order entry system. *Journal of the American Medical Informatics Association*, *11*, 482–491.

Hundt, A. S., Adams, J. A., Schmid, J. A., Musser, L. M., Walker, J. M., Wetterneck, T. B., . . . Carayon, P. (2013). Conducting an efficient proactive risk assessment prior to CPOE implementation in an intensive care unit. *International Journal of Medical Informatics*, *82*, 25–38. doi:10.1016/j.ijmedinf.2012.04.005

Hunte, G. S., Wears, R. L., & Schubert, C. C. (2013, June). *Structure, agency, and resilience*. Paper presented at the 5th Resilience Engineering International Symposium, Soesterberg, Netherlands.

Institute of Medicine. (2012). *Health IT and patient safety: Building safer systems for better care*. Washington, DC: National Academies Press. Retrieved from http://www.nap.edu/openbook.php?record_id=13269

Jha, A. K., & Classen, D. C. (2011). Getting moving on patient safety: Harnessing electronic data for safer care. *New England Journal of Medicine*, *365*, 1756–1758.

Kannampallil, T., Schauer, G., Cohen, T., & Patel, V. (2011). Considering complexity in healthcare systems. *Journal of Biomedical Informatics*, *44*, 943–947.

Karsh, B. T., Weinger, M., Abbott, P., & Wears, R. (2010). Health information technology: Fallacies and sober realities. *Journal of the American Medical Informatics Association*, *17*, 617–623.

Klein, G. (2007). Performing a project premortem. *Harvard Business Review*, *85*(9), 18–19.

Klein, G., Snowden, D., & Pin, C. L. (2010). Anticipatory thinking. In K. Mosier & U. Fischer (Eds.) *Informed by knowledge: Expert performance in complex situations* (pp. 235–246). New York, NY: Psychology Press.

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science*, *42*, 237–270.

Leveson, N., Dulac, N., Zipkin, D., Cutcher-Gershenfeld, J., Carroll, J., & Barrett, B. (2006). Engineering resilience into safety-critical systems. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 95–123). Farnham, UK: Ashgate.

Leveson, N. G. (2012). *Engineering a safer world: Systems thinking applied to safety*. Cambridge, MA: MIT Press.

Lipshitz, R. (2010). Rigor and relevance in NDM: How to study decision making rigorously with small *n*s and without controls and (inferential) statistics. *Journal of Cognitive Engineering and Decision Making*, *4*, 99–112.

Longhurst, C. A., Parast, L., Sandborg, C. I., Widen, E., Sullivan, J., Hahn, J. S., . . . Sharek, P. J. (2010). Decrease in hospital-wide mortality rate after implementation of a commercially sold computerized physician order entry system. *Pediatrics*, *126*, 14–21.

Magrabi, F., Ong, M.-S., Runciman, W., & Coiera, E. (2012). Using FDA reports to inform a classification for health information technology safety problems. *Journal of the American Medical Informatics Association*, *19*, 45–53.

Middleton, B., Bloomrosen, M., Dente, M. A., Hashmat, B., Koppel, R., Overhage, J. M., . . . Zhang, J. (2013). Enhancing patient safety and quality of care by improving the usability of electronic health record systems: Recommendations from AMIA. *Journal of the American Medical Informatics Association*, *20*(e1), e2–e8.

Militello, L. G., & Klein, G. (2013). Decision-centered design. In J. Lee & A. Kirlik (Eds.), *The Oxford handbook of cognitive engineering* (pp. 261–271). Oxford, UK: Oxford University Press.

Myers, R. B., Jones, S. L., & Sittig, D. F. (2011). Review of reported clinical information system adverse events in US Food and Drug Administration databases. *Applied Clinical Informatics*, *2*, 63.

Nemeth, C. (2008). Resilience engineering: The birth of a notion. In E. Hollnagel, C. Nemeth, & S. Dekker (Eds.), *Resilience engineering perspectives* (Vol. 1, pp. 3–9). Farnham, UK: Ashgate.

Nemeth, C., & Cook, R. (2007). Healthcare IT as a source of resilience. In *IEEE International Conference on Systems, Man and Cybernetics* (pp. 3408–3412). doi:10.1109/ICSMC.2007.4413721

Office of the National Coordinator. (2012). *Health information technology patient safety action & surveillance plan for public comment*. Retrieved from http://www.healthit.gov/sites/default/files/safetyplanhhspubliccomment.pdf

Pariès, J. (2011). Resilience and the ability to respond. In E. Hollnagel, J. Pariès, D. Woods, & J. Wreathall (Eds.), *Resilience engineering in practice* (pp. 3–8). Farnham, UK: Ashgate.

Patton, M. (2002). *Qualitative research and evaluation methods*. Thousand Oaks, CA: Sage.

Paulus, R. A., Davis, K., & Steele, G. D. (2008). Continuous innovation in health care: Implications of the Geisinger experience. *Health Affairs*, *27*, 1235–1245.

Pejtersen, A. M., & Rasmussen, J. (1997). Ecological information systems and support of learning: Coupling work domain information to user characteristics. In M. G. Helander, T. K. Landauer, & P. V. Prabhu (Eds.), *Handbook of human-computer interaction* (pp. 315–346). Amsterdam: Elsevier.

Phansalkar, S., Edworthy, J., Hellier, E., Seger, D., Schedlbauer, A., Avery, A., & Bates, D. (2010). A review of human factors principles for the design and implementation of medication safety alerts in clinical information systems. *Journal of the American Medical Informatics Association: JAMIA*, *17*, 493–501.

Qureshi, Z. H., Ashraf, M. A., & Amer, Y. (2007). *Modeling industrial safety: A sociotechnical systems perspective*. In 2007 IEEE International Conference on Industrial Engineering and Engineering Management (pp. 1883–1887). New York, NY: IEEE.

Rankin, A., Lundberg, J., Woltjer, R., Rollenhagen, C., & Hollnagel, E. (2013). Resilience in everyday operations a framework for analyzing adaptations in high-risk work. *Journal of Cognitive Engineering and Decision Making*. Advance online publication. doi:10.1177/1555343413498753

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, *27*, 183–213.

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

Reason, J. T. (2008). *The human contribution: Unsafe acts, accidents and heroic recoveries*. Farnham, UK: Ashgate.

Reiman, T. (2011). Understanding maintenance work in safety-critical organisations: Managing the performance variability. *Theoretical Issues in Ergonomics Science*, *12*, 339–366. doi:10.1080/14639221003725449

Reiman, T., & Rollenhagen, C. (2011). Human and organizational biases affecting the management of safety. *Reliability Engineering & System Safety*, *96*, 1263–1274.

Ritchie, J., & Spencer, L. (2002). Qualitative data analysis for applied policy research. In M. Huberman & M. Miles (Eds.), *The qualitative researcher's companion* (pp. 305–329). Thousand Oaks, CA: Sage.

Roberts, K. H. (1990). Some characteristics of one type of high reliability organization. *Organization Science*, *1*, 160–176.

Roth, E., Kilgore, R., Burns, C., Wears, R., Lee, J. D., Jamieson, G., & Bisantz, A. (2013). Cognitive engineering across domains: What the wide-angle view can provide. In *Proceedings of the Human Factors and Ergonomics Society 57th Annual Meeting* (pp. 139–143). Santa Monica, CA: Human Factors and Ergonomics Society.

Saleh, J. H., Marais, K. B., Bakolas, E., & Cowlagi, R. V. (2010). Highlights from the literature on accident causation and system safety: Review of major ideas, recent contributions, and challenges. *Reliability Engineering & System Safety*, *95*, 1105–1116.

Schön, D. A. (1983). *The reflective practitioner: How professionals think in action*. New York, NY: Basic Books.

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

Sittig, D. F., Ash, J. S., Zhang, J., Osheroff, J. A., & Shabot, M. M. (2006). Lessons from "Unexpected Increased Mortality After Implementation of a Commercially Sold Computerized Physician Order Entry System." *Pediatrics*, *118*, 797–801.

Sittig, D. F., Campbell, E., Guappone, K., Dykstra, R., & Ash, J. S. (2007). Recommendations for monitoring and evaluation of in-patient computer-based provider order entry systems: Results of a Delphi survey. In *AMIA 2007 Annual Symposium Proceedings* (p. 671). Bethesda, MD: American Medical Informatics Association.

Sittig, D. F., & Classen, D. C. (2010). Safe electronic health record use requires a comprehensive monitoring and evaluation framework. *JAMA: The Journal of the American Medical Association*, *303*, 450-451.

Sittig, D. F., & Singh, H. (2009). Eight rights of safe electronic health record use. *JAMA*, *302*, 1111–1113. doi:10.1001/jama.2009.1311

Sittig, D. F., & Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *Quality and Safety in Health Care*, *19*(Suppl. 3), i68–i74.

Sittig, D. F., & Singh, H. (2012). Electronic health records and national patient-safety goals. *New England Journal of Medicine*, *367*, 1854–1860.

Sittig, D. F., & Singh, H. (2013). A red-flag-based approach to risk management of EHR-related safety concerns. *Journal of Healthcare Risk Management*, *33*(2), 21–26.

Skorve, E. (2010). Patient safety, resilience and ICT. A reason for concern? *Studies in Health Technology and Informatics*, *157*, 199–205.

Smith, M., Davis Giardina, T., Murphy, D., Laxmisan, A., & Singh, H. (2013). Resilient actions in the diagnostic process and system performance. *BMJ Quality & Safety*, *22*, 1006–1013. doi:10.1136/bmjqs-2012-001661

Teich, J. M., Glaser, J. P., Beckley, R. F., Aranow, M., Bates, D. W., Kuperman, G. J., . . . Spurr, C. D. (1999). The Brigham Integrated Computing System (BICS): Advanced clinical systems in an academic hospital environment. *International Journal of Medical Informatics*, *54*, 197–208.

Teich, J. M., Merchia, P. R., Schmiz, J. L., Kuperman, G. J., Spurr, C. D., & Bates, D. W. (2000). Effects of computerized physician order entry on prescribing practices. *Archives of Internal Medicine*, *160*, 2741.

Vicente, K. (1999). *Cognitive work analysis: Toward safe, productive, and healthy computer-based work*. Boca Raton, FL: CRC Press.

Vicente, K. J. (2002). From patients to politicians: A cognitive engineering view of patient safety. *Quality and Safety in Health Care*, *11*, 302–304.

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. *Journal of the American Medical Informatics Association*, *15*, 272–277.

Walker, J. M., Hassol, A., Bradshaw, B., & Rezaee, M. (2012). *Health IT hazard manager beta-test: Final report* (No. AHRQ Publication No. 12-0058-EF). Washington, DC: Agency for Health Care Research and Quality.

Watts-Perotti, J., & Woods, D. (2009). Cooperative advocacy: An approach for integrating diverse perspectives in anomaly response. *Computer Supported Cooperative Work (CSCW)*, *18*, 175–198.

Wears, R. L. (2012). Rethinking healthcare as a safety-critical industry. *Work: A Journal of Prevention, Assessment and Rehabilitation*, *41*, 4560–4563. doi:10.3233/WOR-2012-0037-4560

Wears, R. L., Hollnagel, E., & Braithwaite, J. (2013). *Resilient Health Care*. Ashgate Publishing.

Woods, D. (2011). Resilience and the ability to anticipate. In E. Hollnagel, J. Pariès, D. Woods, & J. Wreathall (Eds.), *Resilience engineering in practice* (pp. 121–126). Farnham, UK: Ashgate Publishing.

Woods, D. D. (2006). Essential characteristics of resilience. In E. Hollnagel, D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 21–34). Farnham, UK: Ashgate.

Woods, D. D., & Branlat, M. (2010). Hollnagel's test: Being "in control" of highly interdependent multi-layered networked systems. *Cognition, Technology & Work*, *12*, 95–101.

Woods, D. D., Chan, Y. J., & Wreathall, J. (2013, June). *The stress-strain model of resilience operationalizes the four cornerstones of resilience engineering*. Paper presented at the 5th Resilience Engineering International Symposium, Soesterberg, Netherlands.

Woods, D. D., Dekker, S., Cook, R., Johannesen, L., & Sarter, N. (2010). *Behind human error*. Farnham, UK: Ashgate.

Woods, D. D., & Hollnagel, E. (2006). *Joint cognitive systems: Patterns in cognitive systems engineering*. Boca Raton, FL: CRC Press.

Woods, D. D., Schenk, J., & Allen, T. (2009). An initial comparison of selected models of system resilience. In C. Nemeth, E. Hollnagel, & S. Dekker (Eds.), *Resilience engineering perspectives* (Vol. 2, pp. 73–94). Farnham, UK: Ashgate.

Woods, D. D., & Wreathall, J. (2008). Stress-strain plots as a basis for assessing system resilience. In E. Hollnagel, C. Nemeth, & S. Dekker (Eds.), *Resilience engineering perspectives* (Vol. 1, pp. 143–158). Farnham, UK: Ashgate.

Wreathall, J. (2011). Monitoring: A critical ability in resilience engineering. In E. Hollnagel, J. Pariés, D. Woods, & J. Wreathall (Eds.), *Resilience engineering in practice* (pp. 61–68). Farnham, UK: Ashgate.

Wright, A., Henkin, S., Feblowitz, J., McCoy, A. B., Bates, D. W., & Sittig, D. F. (2013). Early results of the meaningful use program for electronic health records. *New England Journal of Medicine*, *368*, 779–780.

Michael W. Smith, PhD, is a health science specialist and human factors engineer at the Center for Innovations in Quality, Effectiveness and Safety, Michael E. DeBakey VA Medical Center, and an instructor in the Department of Medicine, Section of Health Services Research, Baylor College of Medicine. He received his MS in ergonomics from University of Miami in 1997 and his PhD in cognitive systems engineering from Ohio State University in 2010.

Joan S. Ash, PhD, MLS, MS, MBA, is a professor and vice chair in the Department of Medical Informatics and Clinical Epidemiology, School of Medicine, Oregon Health and Science University. She holds master's degrees in library science (Columbia), health science (California State–Northridge), and business administration (Portland State). Her doctorate is in systems science: business administration (Portland State). She has served on the boards of directors of the American Medical Informatics Association and the Medical Library Association.

Dean F. Sittig, PhD, is a professor in the School of Biomedical Informatics at University of Texas, Health Sciences Center–Houston and member of the UT–Memorial Hermann Center for Healthcare Quality and Safety. He was awarded a master's degree in biomedical engineering from Pennsylvania State University in 1984 and a PhD in medical informatics from the University of Utah in 1988. In 1992, he was elected as a Fellow in the American College of Medical Informatics.

Hardeep Singh, MD, MPH, is chief of the Health Policy, Quality, and Informatics Program at the Center for Innovations in Quality, Effectiveness, and Safety, Michael E. DeBakey VA Medical Center. He is also an associate professor in the Department of Medicine, Baylor College of Medicine. He directs the VA Center of Inquiry to Improve Outpatient Safety Through Effective Electronic Communication, a multidisciplinary center focused on improving electronic health record–related patient safety and reducing diagnostic errors.