Current challenges in health information technology–related patient safety

Dean F Sittig
The University of Texas Health Science Center at Houston (UTHealth), USA

Adam Wright
Harvard Medical School, USA

Enrico Coiera and Farah Magrabi
Macquarie University, Australia

Raj Ratwani
National Center for Human Factors in Healthcare, MedStar Health, USA

David W Bates
Harvard Medical School, USA; Harvard T.H. Chan School of Public Health, USA

Hardeep Singh
Center for Innovations in Quality, Effectiveness and Safety, Michael E DeBakey Veterans Affairs Medical Center and Baylor College of Medicine, Houston, Texas, USA

Abstract
We identify and describe nine key, short-term, challenges to help healthcare organizations, health information technology developers, researchers, policymakers, and funders focus their efforts on health information technology–related patient safety. Categorized according to the stage of the health information technology lifecycle where they appear, these challenges relate to (1) developing models, methods, and tools to enable risk assessment; (2) developing standard user interface design features and functions; (3) ensuring the safety of software in an interfaced, network-enabled clinical environment; (4) implementing a method for unambiguous patient identification (1–4 Design and Development stage); (5) developing and

Corresponding author:
Dean F Sittig, Memorial Hermann Center for Healthcare Quality and Safety and School of Biomedical Informatics, The University of Texas Health Science Center at Houston (UTHealth), 6410 Fannin Street, Houston, TX 77030, USA.
Email: dean.f.sittig@uth.tmc.edu
implementing decision support which improves safety; (6) identifying practices to safely manage information technology system transitions (5 and 6 Implementation and Use stage); (7) developing real-time methods to enable automated surveillance and monitoring of system performance and safety; (8) establishing the cultural and legal framework/safe harbor to allow sharing information about hazards and adverse events; and (9) developing models and methods for consumers/patients to improve health information technology safety (7–9 Monitoring, Evaluation, and Optimization stage). These challenges represent key “to-do’s” that must be completed before we can expect to have safe, reliable, and efficient health information technology–based systems required to care for patients.

**Keywords**
electronic health records, healthcare policy, information and knowledge management, information technology design and development methodologies, organizational change and information technology

**Introduction**

Introducing health information technology (IT) within a complex adaptive health system has potential to improve care but also introduces unintended consequences and new challenges.\textsuperscript{1–3} Ensuring the safety of health IT and its use in the clinical setting has emerged as a key challenge. The scientific community is attempting to better understand the complex interactions between people, processes, environment, and technologies as they endeavor to safely develop, implement, and maintain the new digital infrastructure. While recent evidence from in-patient settings shows that health IT can make care safer,\textsuperscript{4,5} it can also create new safety issues, some manifesting long after technology has been implemented.\textsuperscript{6,7}

Looking at this issue more deeply, it is clear that safe and effective design, development, implementation, and use of various forms of health IT require shared responsibility\textsuperscript{8} and a socio-technical approach (i.e. focus on the people, processes, environment, and technology involved).\textsuperscript{9} In a stepwise progression, health IT must be designed and developed in such a way that it supports user goals and workflows, and organizations must configure health IT correctly if they adopted commercially available products, and then organizations must implement health IT that is safe (i.e. health IT should work as designed and be available when and where it is needed \(24 \times 7\)).\textsuperscript{10} Second, this technology must be used correctly and completely by all healthcare providers as they care for their patients. In the event that correct use of the application does not support users’ goals or existing workflows, then both the software and the workflows need to be reviewed and potentially modified to facilitate safe and effective care. Third, healthcare organizations must work in conjunction with their electronic health record (EHR) vendors to monitor and optimize this technology to enable it to help them identify, measure, and improve the quality and safety of the care provided. Thus, safe technology, safe use of technology, and use of technology to improve safety are all critically important for improving healthcare.\textsuperscript{11}

More broadly, improving the overall safety of our evolving healthcare system represents a monumental sociotechnical challenge.\textsuperscript{12} The goal of this article is to identify and briefly describe nine key, short-term (i.e. addressable within 3–5 years) challenges, identified through an iterative process by the authors, so that healthcare organizations, health IT developers, researchers, policymakers, and funders can focus their efforts where they are needed the most. We categorized these challenges according to the stage of the health IT lifecycle where they appear: (1) Design and Development, (2) Implementation and Use, and (3) Monitoring, Evaluation, and Optimization (see Table 1).
Table 1. Overview of the identified challenges in health information technology (IT)-related patient safety categorized according to the stage of the health IT lifecycle where they appear.

<table>
<thead>
<tr>
<th>Design and Development challenges</th>
<th>Implementation and Use challenges</th>
<th>Monitoring, Evaluation, and Optimization challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Developing models, methods, and tools to enable risk assessment</td>
<td>5. Developing and implementing decision support which improves safety</td>
<td>7. Developing real-time methods to enable automated surveillance and monitoring of system performance and safety</td>
</tr>
<tr>
<td>2. Developing standard user interface design features and functions</td>
<td>6. Identifying practices to safely manage IT system transitions</td>
<td>8. Establishing the cultural and legal framework/safe harbor to allow sharing information about hazards and adverse events</td>
</tr>
<tr>
<td>3. Ensuring the safety of software in an interfaced, network-enabled clinical environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Implementing a method for unambiguous patient identification</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Developing models and methods for consumers/patients to improve Health IT safety</td>
</tr>
</tbody>
</table>

**Design and Development challenges**

Developing proactive models, methods, and tools to enable risk assessment. The use of any features and functions of a complex health IT–based clinical application can create risks to patients, or even the developers of these systems. We should be able to derive an overall proactive risk for an error class (e.g. patient gets the wrong medication due to selection of the wrong item from a drop-down list\(^{13}\) or a patient’s diagnosis and treatment are delayed due to failure to follow-up on an abnormal laboratory test result\(^{14}\)) when severity and likelihood estimates of a potential error are combined. However, current estimates of severity and likelihood are most often based on retrospective incident reports generated by clinical staff or expert opinion. There are well-known biases and under-reporting in such incident data, making them an unreliable basis for frequency estimation.\(^{15}\) We thus need new proactive, data-driven models, methods, and tools for estimating both the severity and frequency of these events to enable us to understand the potential risk. In addition, we need to ensure that both employees of healthcare organizations and health IT manufacturers “have the knowledge, experience and competencies appropriate to undertaking the clinical risk management tasks assigned to them.”\(^{16}\) This will help prioritize efforts to develop compensating controls to prevent or at least reduce the likelihood of these errors from occurring. As some error classes can be detected automatically within digital systems such as the EHR, more reliable frequency estimates should be possible for many issues.\(^{17,18}\)

Developing standard user interface design features and functions. Poor user interface design leads to errors in data input and comprehension.\(^{19}\) For example, most EHRs, intensive care units (ICUs) or vital signs monitors, and infusion devices may have a different method of presenting the patient’s identifying information,\(^{20}\) requiring users to acknowledge their acceptance of entered data in different ways (Ok, Save, Commit, etc.), and providing selection options for data input choices. This inconsistency and lack of accepted and implemented standards force the provider to constantly switch mental models regarding how each interface functions, which increases the likelihood for error.\(^{21}\) We need better and more standardized ways of allowing users to enter data, as well as automatically checking that the entered data are correct for a particular patient.\(^{22}\) Finally, the industry must follow well-established standards for design, development, and testing of safety-critical
software. These standards may be developed by national or international standards bodies and endorsed by governments or other authorities.

**Ensuring the safety of software in an interfaced, networked clinical environment.** Regardless of the comprehensiveness of the product offerings from a single health IT vendor, there will always be new health IT functionality along with stand-alone applications (e.g. apps that run on handheld smartphones or as a web application) developed that must be interfaced to the existing system(s). The entire process of developing, implementing, patching, and updating should be error free. Currently, the health IT industry has not developed fail-safe software design, development, or testing methodologies for isolated, self-contained systems, let alone the massively interconnected systems that will be required to enable seamless sharing of patient data across EHRs, organizations, communities, and eventually nations. At least, we should begin to recognize healthcare as a safety-critical industry and begin to treat the IT components used by it with the same importance as that of the aerospace, nuclear, or defense industries. Some of the Scandinavian countries and the United Kingdom, for example, have taken steps toward developing guidelines and even mandating some processes for the oversight of health IT, while other countries such as the United States have not yet recommended a stringent, industry or government-led, regulatory environment for health IT. Nevertheless, the US Food and Drug Administration’s recent announcement of a software developer “pre-certification” program that will certify software developers rather than individual projects is a step in the right direction that attempts to balance safety and innovation.

**Implementing a method for unambiguous patient identification.** One of the greatest patient safety risks involves accurate patient matching within and across EHRs, organizations, communities, and nations. Although some nations have adopted unique patient identifiers (e.g. Ireland, the Nordic countries, Australia, New Zealand, and the United Kingdom), many have not (e.g. United States, Germany, Italy and Canada), and the most current patient matching technology uses either an exact or a probabilistic patient match that relies on ambiguous (i.e. first name variants), non-unique (i.e. date of birth, gender), temporary (i.e. address), changeable (i.e. last name), identifying characteristics. We need method(s) of accurately linking patients across organizations, locations, and time. Failure to recognize the same patient’s data in two different locations is potentially as important as incorrectly matching two different patients’ data. Potential options to choose from include the following:

(a) Where it has not already been done so, for national organizations to assign each individual a unique number, and then requiring its use;
(b) In those nations where a unique number is politically unacceptable, utilizing one or more biometric identifiers (e.g. fingerprint, palm vein, iris, retina scan, or DNA);
(c) Establishing a common set of identifying characteristics and probabilistic methods to combine them (e.g. last name, first name, date of birth, gender/sex, postal code, and full street address).

**Implementation and Use challenges**

**Developing and implementing decision support which improves safety.** Busy clinical application users will continue to make errors and mistakes (e.g. inappropriate dosing of medications, forgetting to order routine yearly screening exams, failure to order evidence-based treatments). Health IT should act as a cockpit and also as a “safety net” both to make it easier to do the right thing, as
well as catch errors. Current computer-based clinical decision support systems rely mainly on “alerts” and “reminders” to clinicians which are often ignored.\textsuperscript{40} In some instances, the computer even recommends something that the clinician inappropriately follows leading to yet another kind of error.\textsuperscript{41} How should useful clinical decision support be developed, implemented, and potentially regulated to have the biggest impact?\textsuperscript{42,43} Providing the appropriate amount and ensuring the safety and reliability of artificial intelligence (AI)-driven automation while also ensuring that the human is aware of what is happening and is “in the loop” are critical to successful health IT.\textsuperscript{44} How does the computer know when it is appropriate to interrupt a human? How do humans know when it is appropriate to overrule the computer? Current interruptive alerts pop up and require a response from a user before users can continue with their work. These alerts can often be clinically irrelevant due to limitations in capturing accurate and timely patient data, reliance on incomplete clinical knowledge represented in the computer, and incomplete understanding of the specific clinical context and clinician’s thought processes. All of these issues need exploration.

Identifying and implementing practices to safely manage IT system transitions. De novo system implementation, transitions from an in-house developed EHR to a commercial off-the-shelf EHR or from one commercial EHR to another, and even major upgrades of an existing EHR introduce safety risks.\textsuperscript{45} What are the best practices to manage the different types of system transitions including partial implementation (hybrid record system), record migration, software updates, and downtime?\textsuperscript{46} What sort of anomaly detection should be in place?\textsuperscript{47} What is the role of going through and responding to user-reported issues?\textsuperscript{48} How do we prepare staff for downtimes when most healthcare systems are completely reliant on their health IT systems and the new generation of staff have never worked without health IT?\textsuperscript{49} We have learned from decades of health services research that even when guidelines and best practices are clear and available, implementing them itself remains a grand challenge.

Monitoring, Evaluation, and Optimization challenges

Developing real-time methods to enable automated surveillance and monitoring of system performance and safety. Organizations today do not have rigorous, real-time, or even close-to-real-time, approaches to routinely assess the safety of their health IT systems and identify safety hazards. Measurement of these issues has been conceptually challenging and this makes it very hard to ask questions like “Is care getting safer?” or “Am I safer getting my care at one organization rather than another?” or even “Have any aspects of my EHR stopped working or malfunctioned recently?” In 2016, a US National Quality Forum Committee identified nine high-priority measurement areas for health IT–related safety.\textsuperscript{50} To advance the scientific path to measure health IT safety, they recommended measuring concepts (e.g. Retract-and-reorder tool),\textsuperscript{51} possible data sources (e.g. order entry logs), data collection strategies for each measurement topic (e.g. retrospective analysis of order entry logs), and entities that were accountable for performance (e.g. health IT vendors, healthcare organizations, and clinicians). While this lays groundwork for future efforts, researchers would need to work closely with computer scientists,\textsuperscript{52} health IT vendors,\textsuperscript{53} and healthcare organizations\textsuperscript{49} to develop additional scientific knowledge, methods, and tools to advance real-time measurement, make surveillance more automated,\textsuperscript{54} and initiate safety improvement efforts.

Establishing the cultural and legal framework/safe harbor to allow sharing information about hazards and adverse events. The vast majority of EHR–related patient safety concerns, “broadly defined
as adverse events that reached the patient, near misses that did not reach the patient, or unsafe conditions that increase the likelihood of a safety event” are not identified, let alone reported.\(^5\) This must change if we are to gather enough data to identify common modes of failure and estimate the likelihood of similar future events. We propose the creation of a mandatory, blame-free, national or international health IT reporting system that gathers and investigates serious patient safety issues with the help of dedicated experts. Such a system could be modeled after the airline industry’s existing near-miss reporting system that has created a list of “near-misses” (e.g. smoke in the cabin, aircraft goes off the end of the runway, aborted landing attempt) that must be reported and include additional information on events.\(^5\) In addition, we must begin exploring methods to bring together information from existing registries for equipment failure and hazards,\(^5\) medical record review,\(^1\) user complaints,\(^5\) and medico-legal investigations,\(^6\) for example, to help us form a more comprehensive understanding about the nature, causes, consequences, and outcomes of IT problems in healthcare.\(^6\) We have already seen benefits of analyzing large databases of patient safety event reports to identify health IT safety hazards.\(^19,62,63\)

**Developing models and methods for consumers/patients to improve health IT safety.** As consumers and their caregivers start to play a bigger role in managing their health information, what is their role in detecting and mitigating IT-related errors? For example, patients can report diagnostic errors to their clinicians\(^4\) or medication order errors they experience at the pharmacy. Will they be expected to play different roles and take on more responsibility for their healthcare, especially with the advent of activity tracking and personal/shared health records?\(^6\) Accessibility of progress notes and other clinical data introduces a new level of transparency and will require a cultural shift, which is a substantial “non-technical” barrier to overcome itself.\(^6\)

**Conclusion**

Safety of health IT needs to be improved substantially. Although scientific knowledge has improved, a great deal still needs to be learned and much remains to be done. These challenges, taken together, represent a necessary, but not complete set of key “to-do’s” of all the work that must be done before we can expect to have safe, reliable, and efficient health IT–based systems required to care for patients. While we are seeing rapid adoption of health IT globally, it is not yet clear how much of this technology is actually improving safety. If we are to realize the potential returns on this investment, addressing the nine challenges we describe must be a high priority for organizations that use these systems, health IT vendors that develop them, and government organizations that help fund and establish policies for their oversight.

**Declaration of Conflicting Interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding**

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Dr H Singh was supported by the VA Health Services Research and Development Service (CRE12-033; Presidential Early Career Award for Scientists and Engineers USA 14-274), the VA National Center for Patient Safety, the Agency for Health Care Research and Quality (R01HS022087), the Gordon and Betty Moore Foundation, and the Houston VA HSR&D Center for Innovations in Quality, Effectiveness and Safety (CIN 13–413). Drs DF Sittig and A Wright were supported by the National Library of Medicine of the National Institutes of Health under Award No. R01LM011966. DF Sittig was also supported by the Agency
for Health Care Research and Quality (P30HS024459). Dr R Ratwani was supported by the Agency for Healthcare Research and Quality (R01HS02370104). The content is solely the responsibility of the authors and does not necessarily represent the official views of the National Institutes of Health, the VA, or AHRQ.

References
8. Sittig DF, Belmont E and Singh H. Improving the safety of health information technology requires shared responsibility: it is time we all step up. *Healthc* 2018; 6(1): 7–12.


