Measuring and improving patient safety through health information technology: The Health IT Safety Framework

Hardeep Singh,1 Dean F Sittig2

1Houston Veterans Affairs Center for Innovations in Quality, Effectiveness and Safety, Michael E. DeBakey Veterans Affairs Medical Center and Baylor College of Medicine, Houston, Texas, USA, Houston, Texas, USA
2UTHealth – Memorial Hermann Center for Healthcare Quality and Safety, School of Biomedical Informatics, University of Texas Health Science Center, Houston, Texas, USA

Correspondence to Dr Hardeep Singh, 2002 Holcombe Blvd, 152, Houston, TX 77030, USA; hardeeps@bcm.edu

Received 14 June 2015
Revised 5 August 2015
Accepted 20 August 2015
Published Online First 14 September 2015

▸http://dx.doi.org/10.1136/bmjqs-2015-004486

ABSTRACT
Health information technology (health IT) has potential to improve patient safety but its implementation and use has led to unintended consequences and new safety concerns. A key challenge to improving safety in health IT-enabled healthcare systems is to develop valid, feasible strategies to measure safety concerns at the intersection of health IT and patient safety. In response to the fundamental conceptual and methodological gaps related to both defining and measuring health IT-related patient safety, we propose a new framework, the Health IT Safety (HITS) measurement framework, to provide a conceptual foundation for health IT-related patient safety measurement, monitoring, and improvement. The HITS framework follows both Continuous Quality Improvement (CQI) and sociotechnical approaches and calls for new measures and measurement activities to address safety concerns in three related domains: 1) concerns that are unique and specific to technology (e.g., to address unsafe health IT related to unavailable or malfunctioning hardware or software); 2) concerns created by the failure to use health IT appropriately or by misuse of health IT (e.g., to reduce nuisance alerts in the electronic health record (EHR)), and 3) the use of health IT to monitor risks, health care processes and outcomes and identify potential safety concerns before they can harm patients (e.g., use EHR-based algorithms to identify patients at risk for medication errors or care delays). The framework proposes to integrate both retrospective and prospective measurement of HIT safety with an organization’s existing clinical risk management and safety programs. It aims to facilitate organizational learning, comprehensive 360 degree assessment of HIT safety that includes vendor involvement, refinement of measurement tools and strategies, and shared responsibility to identify problems and implement solutions. A long term framework goal is to enable rigorous measurement that helps achieve the safety benefits of health IT in real-world clinical settings.

INTRODUCTION
Health information technology (health IT) has potential to improve patient safety but its implementation and use has met with unintended consequences and new safety concerns.1–5 A key challenge to improving patient safety in IT-enabled healthcare systems is to develop valid, feasible strategies to measure safety concerns at the intersection of health IT and patient safety.6 7 For example, health IT-related adverse events, near misses and unsafe conditions are difficult to define and detect for several reasons. Because health IT is integrated with all aspects of care delivery, a wide variety of heterogeneous safety concerns can occur, often in temporally or physically separated circumstances. Moreover, causal attributions for health IT-related risks and adverse events are also difficult to identify, as they generally involve interactions of technical and non-technical factors, which are notoriously difficult to separate.8

For example, an error in the system-to-system interface between a medication order-entry module and the pharmacy inventory management system could cause a different medication to be dispensed than what was prescribed. The ordering physician may not have any indication that something is wrong, and unless the pharmacist accesses and reviews the patient’s medical record and finds that the new medication was clearly not indicated for the patient, he/she has...
no idea either. At present, few strategies exist to systematically detect and correct such health IT-related safety issues, and frontline clinicians and healthcare organisations (HCOs) are often unaware of recommended practices for safe health IT implementation and use. Addressing health IT-related patient safety has yet to find its place in mainstream patient safety measurement, which itself is still evolving 15 years after the landmark Institute of Medicine report on patient safety.9 Despite recent efforts to define the nature and scope of health IT-related safety concerns,10–12 the ‘basic science’ of measuring health IT-related patient safety remains in its infancy.

In response to the fundamental conceptual and methodological gaps related to both defining and measuring health IT-related patient safety, we developed a new framework, the health IT safety (HITS) framework, to provide a conceptual foundation for health IT-related patient safety measurement, monitoring, and improvement (figure 1).

**FRAMEWORK RATIONALE**

Current patient safety-oriented organisational activities do not facilitate or focus on measurement of health IT-related patient safety. Over the past few years, institutions have focused their electronic health record (EHR)-related activities on achieving meaningful use requirements,13 and less attention has been devoted to measuring patient safety concerns. However, emerging evidence suggests the need to refocus efforts.10–12

Health IT is commonly deployed on a large scale, often across multiple, geographically distributed facilities, and thus the consequences of health IT-related safety concerns can rapidly affect not only a single department or institution but possibly an entire healthcare system.17 As IT-enabled patient care is rapidly becoming the norm, it is essential to (1) refine the science of measuring health IT-related patient safety (2) make health IT-related patient safety an organisational priority by securing commitment from organisational leadership and refocusing the organisation’s clinical governance structure to facilitate measurement and monitoring (3) develop an environment that is conducive to detecting, fixing and learning from system vulnerabilities. We envision that the conceptual scientific foundation laid out by this framework can help overcome HITS measurement challenges, as well as position HITS at the centre of an organisation’s existing patient safety-oriented activities. A long-term framework goal is to enable rigorous measurement that helps achieve the safety benefits of health IT in real-world clinical settings.

**OVERVIEW OF THE HITS FRAMEWORK**

The framework follows the principles of Continuous Quality Improvement, which has been defined as “a philosophy that encourages all healthcare team members to continuously ask the questions, ‘How are we doing?’ and ‘Can we do it better?’.”18 It also addresses a third element ‘how can we do better’. We describe each component of the HITS framework below.

**Sociotechnical work system**

The HITS framework posits that safety events must be understood within the full context of the
‘sociotechnical work system’,19 which refers to the many interacting technical (hardware, software, networking infrastructure) and non-technical (clinical workflow, internal organisational policies, people, physical environment and external policies) variables that affect health IT-related patient safety (table 1).

External factors that can affect measurement include clinical productivity and legal pressures, including privacy, confidentiality and accreditation requirements; reimbursement issues, administrative demands and other confounding factors related to ongoing mandatory quality measurements. The HITS framework is set within this complex adaptive sociotechnical system.19

Measurement of three overlapping domains of HITS

The intersection of health IT and patient safety is one that involves three overlapping domains covering the lifecycle of health IT implementation and use.21 The first domain, safe health IT, pertains to addressing safety concerns that are unique and specific to technology (ie, making health IT hardware and software safe and free from malfunctions). The second domain, safe use of health IT, includes safe and appropriate use of technology by clinicians, staff and patients, as well as identifying and mitigating unsafe changes in workflows that emerge due to technology use. The third domain, using health IT to improve safety, includes use of technology to identify and monitor patient safety events, risks and hazards and to intervene before actual harm occurs. These domains account for the range of risks and opportunities for health IT to influence patient safety in both new and established health IT-based work systems.22 Each domain is supported by principles adapted from those used in the development of the SAFER (Safety Assurance Factors for EHR Resilience) guides (table 2).22

Measurement in all three domains must involve retrospective data collection methods as well as more proactive measurement and monitoring of HITS because many errors are unknown and reporting is underutilized.23 Additional measurement methods, such as use of triggers for automated detection of health IT-related concerns and prospective methods such as proactive risk assessments could provide a more comprehensive picture of the extent and seriousness of current risks.24 Good measures should meet the criteria of being impactful (ie, important to measure and report), scientifically acceptable (reliable, valid), feasible (clinically, technically and financially), usable (easily extracted from existing EHRs) and transparent (reviewable by all stakeholders).25

Expected measurement impact

The complex and multifaceted nature of health IT-related safety risks necessitates the co-operation of multiple stakeholders, including healthcare providers, patient safety professionals and EHR vendors, to collaboratively address safety concerns and develop tools and strategies to optimise the safety of health IT. However, health IT-related safety is not currently integrated with most HCOs’ patient safety programmes.8 26 Improved measurement is needed to create feedback for organisational learning,27 28 which in turn should lead to development of more refined measurement tools, clear definitions and rigorous assessments of the types of safety concerns the organisation should focus on. It would also lead to prioritising and implementing best practices related to HITS, enacting plans to maintain safety practices already in place and dedicating the required financial and human resources to make necessary improvements.

Measurement is critically dependent on a heterogeneous group of people, including those who are more technically oriented (eg, EHR designers, database administrators, hardware and networking infrastructure-related personnel) as well as those focused on healthcare delivery systems (eg, clinical medicine, quality improvement, organisational change, risk management and patient safety). Creating an environment in which these individuals with widely varying backgrounds can work together on measurement and learning in a collegial manner is no small task. The framework thus posits that all of these people share responsibility for improvement, which

---

**Table 1** Sociotechnical dimensions19

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware and software</td>
<td>Computing infrastructure used to support and operate clinical applications and devices</td>
</tr>
<tr>
<td>Clinical content</td>
<td>The text, numeric data and images that constitute the ‘language’ of clinical applications, including clinical decision support</td>
</tr>
<tr>
<td>Human–computer interface</td>
<td>All aspects of technology that users can see, touch or hear as they interact with it</td>
</tr>
<tr>
<td>People</td>
<td>Everyone who is involved with patient care and/or interacts in some way with healthcare delivery (including technology). This would include patients, clinicians and other healthcare personnel, IT developers and other IT personnel, informaticians</td>
</tr>
<tr>
<td>Workflow and communication</td>
<td>Processes to ensure that patient care is carried out effectively, efficiently and safely</td>
</tr>
<tr>
<td>Internal organisational features</td>
<td>Policies, procedures, the physical work environment and the organisational culture that govern how the system is configured, who uses it and where and how it is used</td>
</tr>
<tr>
<td>External rules and regulations</td>
<td>Federal or state rules (eg, CMS’s Physician Quality Reporting Initiative,20 HIPAA and Meaningful Use programme) and billing requirements that facilitate or constrain the other dimensions</td>
</tr>
<tr>
<td>Measurement and monitoring</td>
<td>Evaluating both intended and unintended consequences through a variety of prospective and retrospective, quantitative and qualitative methods</td>
</tr>
</tbody>
</table>

HIPAA, Health Insurance Portability and Accountability Act of 1996; IT, information technology.
Table 2  Health IT safety domains (Adapted from reference 39)

<table>
<thead>
<tr>
<th>Level</th>
<th>Principles adapted from those used in the development of the SAFER guides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain 1 Safe health IT: address concerns unique to technology</td>
<td>▶ Data availability—Health IT is accessible and usable upon demand by authorised individuals.</td>
</tr>
<tr>
<td></td>
<td>▶ Data integrity—Health IT data or information is accurate and created appropriately and has not been altered or destroyed in an unauthorised manner.</td>
</tr>
<tr>
<td></td>
<td>▶ Data confidentiality—Health IT data or information is only available or disclosed to authorised persons or processes.</td>
</tr>
<tr>
<td>Domain 2 Using health IT safely: optimise the safe use of technology</td>
<td>▶ Complete/correct health IT use—Health IT features and functionality are implemented and used as intended.</td>
</tr>
<tr>
<td></td>
<td>▶ Health IT system usability—Health IT features and functionality are designed and implemented so that they can be used effectively, efficiently and to the satisfaction of the intended users to minimise the potential for harm.</td>
</tr>
<tr>
<td>Domain 3 Monitoring safety: use technology to monitor and improve patient safety</td>
<td>▶ Surveillance and optimisation—As part of ongoing quality assurance and performance improvement, mechanisms are in place to monitor, detect and report on the safety and safe use of health IT, and leverage health IT to reduce patient harm and improve safety.</td>
</tr>
</tbody>
</table>

IT, information technology; SAFER, Safety Assurance Factors for EHR Resilience.

means the HCO and its various internal and external IT partners, including EHR vendors, must share the responsibility of safety. For example, many EHRs now calculate and display a ‘falls risk assessment score’ for patients based on age, medications, clinical condition and recent procedures. If there is an error in this calculation or erroneous data creeps into the patient’s EHR, this score will be incorrect. As a result, the nursing staff, increasingly dependent on these computer-based reminders, might not take appropriate fall prevention precautions leading to a preventable adverse event. The EHR and those responsible for its content also have a role in addressing this problem. Organisational learning would be fostered by sharing responsibility for safety with the EHR vendors and ensuring that different external stakeholders, such as EHR vendors, clinical knowledge suppliers or IT infrastructure providers, achieve a shared understanding of safe practices.

While recent analyses of retrospective reports confirm safety problems, they tend to provide a narrow and technical view of the picture, rather than one through a sociotechnical lens. Moreover, it is notable that none of these data have been collected from vendors. To advance the ‘basic science’ of health IT-related safety, the HITS framework suggests a 360-degree approach that includes both sociotechnical thinking and vendor involvement to enable system-wide learning. It is unclear how EHR vendors are obtaining and using feedback about the effects of their systems on patient safety. Given the increasing number of EHR vendors, ensuring they are included in health IT-related patient safety initiatives is critical.

Recent efforts have been made to facilitate the reporting of health IT-related incidents, but little is known about how to analyse this data to generate actionable findings. Closely integrating HITS with an organisation’s existing clinical risk management and patient safety programmes could help achieve that. These programmes could ensure that data from existing safety events are aggregated and used to identify common health IT-related unsafe conditions, provide recommendations to mitigate risks and follow-up with responsible stakeholders to ensure that recommendations are actually implemented.

All of these measurement impacts would help create a culture of health IT-related patient safety and inform safer IT-enabled healthcare.

USE OF THE FRAMEWORK TO OVERCOME CHALLENGES OF REAL-WORLD MEASUREMENT

In this section, we discuss how various components of the HITS framework can work together and help overcome key challenges in advancing measurement of health IT-related safety. We also outline some key necessities and assumptions for the framework to function for this purpose.

Uncover hidden HIT safety risks

Health IT operations are not visible to EHR users and without a basic HITS measurement system in place, it is unlikely that health IT-related concerns will be captured easily. The HITS framework presupposes that HCOs will need to obtain authority and resources from organisational leadership and their firm commitment to measurement and reporting in all three domains of HITS. This new approach is needed because users are often unaware of the origins of safety concerns or how health IT was involved. ‘Hidden’ safety issues carry the potential to affect many patients. For example, in one study, several systematic errors resulted in missed follow-up of abnormal laboratory test results, including problems with the test ordering and reporting workflow and problems with the configuration of the system that should have automatically notified the appropriate provider of the abnormal result. As a result, several providers did not receive timely notification of their patients’ abnormal test results. This error remained unknown for several months and affected a large number of tests.
HITS framework also assumes that HCOs will modify their existing patient safety structures and processes to incorporate the unique skill mix needed for comprehensive, three-domain HITS measurement. For example, HCOs might need to use informaticians or clinicians trained in the newly created subspecialty of clinical informatics or a multidisciplinary oversight committee to help identify risks, prioritise interventions and review IT-related solutions.34 35 They might also create multidisciplinary EHR safety teams with human factors and informatics expertise to investigate safety events with potential ‘health IT involvement’. These teams could work within the protections of patient safety organisations during investigations and solution development and be integrated with an HCO’s existing risk management infrastructure.36

Facilitate organisational preparedness
HCOs using health IT would first need to rigorously assess their measurement readiness in all three domains of HITS and consider how HITS is integrated within their existing patient safety infrastructure.37 This would require determining how health IT/EHRs are involved in safety events and what types of changes have been made based on this data. Risk managers and other quality personnel would need to become aware of red flags for health IT-related safety issues.38 They could also consider conducting or participating in proactive risk assessments using SAFER guides22 39 and integrate these activities within their existing patient safety programmes.

ADVANCE CURRENT MEASUREMENT METHODS
Although it is well established that health IT can introduce new types of errors,2 14 15 40–42 comprehensive data on IT-related safety events are lacking11 14 and most current data comes from reporting of safety events. Voluntary reporting alone detects only a small proportion of problems and often neglects latent errors and near-misses that could point to important safety issues.11 43 Moreover, few organisations are reporting health IT or EHR-related safety issues. Thus, alternative approaches to data collection need to be used to capture and respond appropriately to the full scope of health IT-related safety risks. HCOs will also need to consider additional methods of measurement beyond reporting, such as the use of automated triggers to detect wrong patient orders,24 helpdesk logs,10 triggers for ordering recovery medications (naloxone outside the operating room),14 provocative testing45 or real-time observations46 47 and feedback from users. They will also need measures to address certain framework components, such as what type of turn-around time exists for resolving vendor-reported EHR safety concerns (for shared responsibility). Better measurement will also promote the development of a comprehensive taxonomy of HITS concerns.10 14 16 48

Identify top priorities for measure development
Beyond HCO-level use, HITS framework could provide a conceptual foundation for initiatives currently underway to advance measurement of HITS. For example, the National Quality Forum is currently developing a comprehensive approach to assess HITS measurement and conducting a measure gap analysis. The framework could help identify priorities for measure development in each of the HITS domains and their respective principles outlined in table 2. Measurement was also emphasised recently by the Roadmap for the Federal Health IT Safety Center in the USA,12 49 which is expected to be operationalised within the authorities of the Office of the National Coordinator for Health Information Technology and the Agency for Healthcare Research and Quality.

In conclusion, the HITS framework helps conceptualise patient safety related to health IT, both in terms of risks emanating from health IT and its uses and how health IT might be harnessed to enhance patient safety. A key risk in any new measurement initiative, which this framework could help overcome, is leaving out one or more essential concepts that are fundamental to improvement initiatives, which could lead the initiative to fail. Although careful definition and eventual operationalisation of the many concepts necessary to provide a full picture of health IT-related patient safety will be challenging, the HITS framework can be used to provide a foundation for efforts to advance measurement and help identify priorities for measure development. The framework proposes to integrate both retrospective and prospective measurement of HITS within an organisation’s existing clinical risk management and safety programme and aims to facilitate organisational learning, comprehensive 360-degree assessment of HITS, refinement of measurement tools and strategies and shared responsibility to identify problems and implement solutions. This approach would enable us to achieve the safety benefits of health IT in real-world clinical settings.
REFERENCES


36. Howard J, Levy F, Mareiniss DP, et al. New legal protections for reporting patient errors under the Patient Safety and


