The health information technology safety framework: building great structures on vast voids

Ross Koppel

Correspondence to
Dr Ross Koppel, Room 113, McNeil Bldg, Locust Walk, University of Pennsylvania, Philadelphia, PA 19094, USA; rkoppel@sas.upenn.edu

Accepted 21 October 2015
Published Online First 19 November 2015

With their health information technology (HIT) safety framework, Drs Hardeep Singh and Dean Sittig offer many admirable suggestions to improve the safety of computerised provider order entry and electronic health records (EHRs).[1] As I shall try to explain, however, I find their proposed framework less than the sum of its parts because: (1) some of its parts, in my opinion, are misdirected; (2) they make errors in their assumptions about what we can know about errors and HIT and (3) their key recommendations lack regulatory or legal teeth. Despite the authors' fine intentions and several excellent insights and recommendations, I fear their proposal will function more as a distraction than as a useful plan for improving HIT safety—something to make us feel useful while we do not address the underlying problems.

THE GOOD

- Acknowledging that we often do not know about the errors associated with the use of HIT, the authors write: '…[C]ausal 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'. (As discussed below, however, the authors often ignore this insight.)
- They wisely call for us to 'develop valid, feasible strategies to measure safety concerns at the intersection of health IT and patient safety'.
- They thoughtfully point out that previous efforts are 'notable [for the fact] that none of these data [on errors] have been collected from vendors'.
- They recommend needed steps when they write that we must: (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 and (3) develop an environment that is conducive to detecting, fixing and learning from system vulnerabilities.
- Their presentation and recommendations on socio-technical dimensions and steps to improve HIT (their table 1) succinctly summarise critical needs. Both the theory and practice reflected in the table are excellent.
- They highlight a neglected focus on patient safety, one of the original motivations for HIT. In their words, 'Over the past few years, institutions have focused their electronic health record (EHR)-related activities on achieving meaningful use requirements, and less attention has been devoted to measuring patient safety concerns'.
- Their emphasis on the need for good data on HIT is likewise a valuable contribution (highlighted as the first domain in their table 2).

THE MISSING

(1) To my mind, Drs Singh and Sittig fail to acknowledge the extent of our ignorance about errors, especially the most common errors involved with EHRs: medication prescribing errors and diagnostic errors. Because so much of their plan revolves around the idea that we can learn from better error reporting—even though so many errors are unknown—they build a framework on a vast void. Thus, theirs is a structure with many fine elements, but too much of it rests on what may not only be unknown but usually unknowable.

Why unknown and unknowable? As I have argued in the past,[2] many hospitalised patients are old and sick, have several comorbidities and are taking many other medications. Key organs, like the liver, kidney and heart, are

Linked

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

CrossMark

To cite: Koppel R. *BMJ Qual Saf* 2016;**25**:218–220.

compromised. Bad things can happen to these patients even when we do everything right; conversely, good things can happen even when we do much wrong. We usually miss the results of, say, a wrongly prescribed medication. (Note: these types of 'missed' errors contrast to leaving a pair of haemostats in the thoracic cavity or to wrong-site surgery—where most errors soon become obvious).

How do these errors relate to HIT? Answer: they are intimately related because the isolated and fragmented data—needed for patient care—are defeated by:

- dreadful presentations of patients' data and general poor usability
- drop-down lists that continue to several screens (with the existence of the extended often hidden from the clinician)
- pop-ups that hide medication or problem lists
- medication lists and problem lists that can't be seen when ordering medications
- lab reports presented in erratic or absurd formats and sequences
- herds of decision support alerts that obscure the screen
- data that should be contiguous separated by three screens and multiple clicks
- critical information on the patient is lost because of proprietary EHR software, idiosyncratic device data formats, and refusal to accept data standards, and
- lack of true interoperability.

In essence, I suggest that these two eminent colleagues tell us to look under the lamppost even though, as the old saying goes, the keys were dropped 70 feet away from the lamppost in the dark. Both Singh and Sittig, of course, are fully aware of the errors listed above,[3 4] but (1) they expect that we can detect and understand these problems with error reporting, although many potentially serious errors go undetected (thus, unreported), and when detected, the poor design features that contributed to the error may not be readily apparent. (2) Singh and Sittig tend to attribute those sorts of problems to poor implementation, user errors or lack of access to the technology. They do not seriously question if the software is fit for its purpose.

(2) And, this brings us to the second problem with their proposed framework: skirting poor design and poor usability. For example, in their table 2, the second 'domain' reflects their apparent reluctance to address this issue: on the one hand, they say, we should have (a) 'Health IT features and functionality [that] are implemented and used as intended', but on the other hand, in that same 'domain', they say we must ensure that (b) '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 minimize the potential for harm'.

While those two sentences seem at first blush to be aligned, they actually expose a contradiction. An analogy may be helpful here: will a poorly designed car, even used as intended by its engineers, provide a safe or efficient vehicle? Thus, we ask: what if: (a) 'the HIT is implemented and used as intended', but (b) HIT's design and implementation are incompatible with effective and satisfactory use? In other words, is HIT that is designed poorly with the wrong purpose likely to facilitate safe medical practice, even if implemented and used as intended? This contradiction negates, or at least weakens, much of their proposal.

In fact, their assumption that HIT software is well designed runs throughout their work. They write about: *misused* software, *unavailable* software, *poorly implemented* software and *malfunctioning* software (emphasis added), but what of badly designed software—neither user friendly nor interoperable with systems holding needed patient data? That failure is not in their purview. They don't challenge HIT vendors who design the software, or the regulators, who so often serve primarily as HIT industry promoters. Here's what they write we need to address (my italics): '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) ….'

Earlier, I praised their comment about 'institutions [that] have focused their electronic health record (EHR)-related activities on achieving meaningful use requirements, and less attention has been devoted to measuring patient safety concerns'. But revisiting their sentence about 'less attention to patient safety' also reminds us that there are two aspects of safety here: their emphasis on '*Measuring patient safety concerns*', and the *design* of the HIT systems. I suggest that most clinicians are already concerned about patient safety but are so often frustrated by HIT that presents impediments to achieving it (although offering many advantages to paper).[5]

(3) I note that much of the literature on HIT and errors is absent from the list of references supporting their proposed framework. Powerful work by Karsh, Winger, Abbott[6] the National Institute for Standards and Technology (NIST),[7] Wears, Braithwaite, Hollnagel, Fairbanks, Woods, Cook,[8–11] Borycki, Kushniruk, Nohr[12] and many, many others does not appear among the 49 references.

TO CONCLUDE

In a sense, this dispute with my colleagues (and friends), Drs Singh and Sittig, resembles an old married couple fighting the same fight. We have had this debate before. They show great faith in the value of investigating errors, often, for example, with teams like those used by the National Transportation Safety Board. In contrast, I've repeatedly noted that when

there is a plane or train crash we can examine a smoldering ruin; but when there is a medication prescribing error we seldom notice the sick patiient who continues to be sick. To their faith in reporting errors as a solution, I argue that most errors are hard to know, harder to report, and the regulatory environment adds additional barriers to addressing these errors even if one knows about and wants to report them. Added to these difficulties, vendors nether disclose their bug lists nor allow sharing of screen shots that would display HIT-related iatrogenic interfaces and functions. These industry practices, although condemed by the IOM and AMIA's task force on vendor-provider relations,[13 14] are not addressed by regulators. Providers and researchers are likewise obliged to forgo opportunities to improve patient safety via these data.

The mechanisms that would facilitate instant reporting of hazards have been sidestepped—at least in the USA—by the vendors and by the Office of the National Coordinator (ONC) for HIT. Instead, we are offered clunky websites that require clinicians to leave their work, log on to other reporting systems, report the problems, log out and then return to their work. This is a distraction to make us feel good about patient safety, not a viable solution. Healthcare Information and Management Systems Society (HIMSS) and its association of large EHR vendors (EHRA) created such a site a few years ago, and of course it had very few users (thus ironically 'proving' that EHRs were perfectly safe). Worse, recently the vendors and ONC insisted that EHRs were 'low or no risk' and thus the US Food and Drug Administration (FDA) should continue its non-oversight of EHR products. The FDA, denied resources to act on HIT, went along. This is regulatory capture at its most naked.

I reiterate that Singh and Sittig make many useful recommendations in their article.[1] Their framework is innovative and absolutely well-intended. We should ask, however, if their reliance on finding and reporting errors is insufficient for the reasons I've enumerated above, and only provide a false sense of security, making us feel like we are addressing a problem when we have not.

We know that HIT systems are fragmented, usability is often primitive, and interoperability is promised on a ten year plan when it should have been a requirement a decade ago. We need to fix the software and interoperability to reduce errors. Reporting errors is essential, but so many errors are unknown, are attributed to poor implementation or user incompetence, and are made difficult to report by clunky mechanisms, legal concerns, and normative pressures. Waiting for error reports from existing HIT systems may well be a distraction. We should first address the very design and data fluidity problems that contribute to errors and also undermine efforts to report those errors.

Competing interests None declared.

Provenance and peer review Commissioned; internally peer reviewed.

REFERENCES

1 Singh H, Sittig D. Measuring and Improving Patient Safety through Health Information Technology: The Health IT Safety Framework. *BMJ Qual Saf* 2016;25:226–32.
2 Koppel R. "Great promises of Healthcare Information technology deliver less" Chapter in Healthcare Information Management Systems: Cases, Strategies, and Solutions. In: Weaver CA, Ball MJ, Kim GR, eds. Berlin: Springer-Verlag, 2015.
3 Sittig DF, Singh H. Defining health information technology-related errors: new developments since to err is human. *Arch Intern Med* 2011;171:1281–4.
4 Sittig DF, Classen DC, Singh H. Patient safety goals for the proposed Federal Health Information Technology Safety Center. *J Am Med Inform Assoc* 2015;22:472–8.
5 Koppel R. Is Healthcare Information Technology Based on Evidence? Keynote Chapter. Intl Med Informatics Assoc Yearbook 2013: Evidence-based Health Informatics.
6 Karsh B-T, Weinger MB, Abbott PA, *et al*. Health information technology: fallacies and sober realities. *J Am Med Inform Assoc* 2010;17:617–23.
7 Lowery SZ, *et al*. Technical Evaluation, Testing, and Validation of the Usability of Electronic Health Records: Empirically Based Use Cases for Validating Safety Enhanced Usability and Guidelines for Standardization NISTIR 7804-1. Washington, DC NIST.
8 Wears RL. Improvement and evaluation. *BMJ Qual Saf* 2015;24:92–4.
9 Wears RL. Health information technology and victory. *Ann Emerg Med* 2015;65:143–5.
10 Fairbanks RJ, Wears RL, Woods DD, *et al*. Resilience and resilience engineering in health care. *Jt Comm J Qual Patient Saf* 2014;40:376–83.
11 Braithwaite J, Wears RL, Hollnagel E. Resilient health care: turning patient safety on its head. *Int J Qual Health Care* 2015;27:418–20.
12 Borycki E, Kushniruk A, Nohr C, *et al*. Usability Methods for Ensuring Health Information Technology Safety: Evidence-Based Approaches. Contribution of the IMIA Working Group Health Informatics for Patient Safety. Yearbook of Medical Informatics 2013;8:20–7.
13 Sinsky CA, Hess J, Karsh B, *et al*. Comparative user experiences of health IT products: how user experiences would be reported and used [Internet]. Washington (DC): Institute of Medicine; 2012 Sep [cited 2012 Nov 26]. http://www.iom.edu/Global/Perspectives/2012/~/media/Files/Perspectives-Files/2012/Discussion- Papers/comparative-userexperiences. Pdf
14 Goodman K, Berner E, M Dent, *et al*. Challenges in ethics, safety, best practices and oversight regarding HIT vendors, their customers, and patients: a report of an AMIA special task force. *J Am Medical Informatics Assoc* 2011:18:77e81.