Healthcare xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Healthcare

journal homepage: www.elsevier.com/locate/healthcare

Opinion paper

Improving the safety of health information technology requires shared responsibility: It is time we all step up☆

Dean F. Sittig[a,*], Elisabeth Belmont[b], Hardeep Singh[c]

[a] University of Texas – Memorial Hermann Center for Healthcare Quality & Safety, School of Biomedical Informatics, University of Texas Health Science Center at Houston, TX, United States

[b] MaineHealth, Portland, ME, United States

[c] Center for Innovations in Quality, Effectiveness and Safety, Michael E. DeBakey Veterans Affairs Medical Center and Baylor College of Medicine, Houston, TX, United States

ABSTRACT

In 2011, an Institute of Medicine report on health information technology (IT) and patient safety highlighted that building health-IT for safer use is a shared responsibility between key stakeholders including: "vendors, care providers, healthcare organizations, health-IT departments, and public and private agencies". Use of electronic health records (EHRs) involves all these stakeholders, but they often have conflicting priorities and requirements. Since 2011, the concept of shared responsibility has gained little traction and EHR developers and users continue to attribute the substantial, long list of problems to each other. In this article, we discuss how these key stakeholders have complementary roles in improving EHR safety and must share responsibility to improve the current state of EHR use. We use real-world safety examples and outline a comprehensive shared responsibility approach to help guide development of future rules, regulations, and standards for EHR usability, interoperability and security as outlined in the 21st Century Cures Act. This approach clearly defines the responsibilities of each party and helps create appropriate measures for success. National and international policymakers must facilitate the local organizational and socio-political climate to stimulate the adoption of shared responsibility principles. When all major stakeholders are sharing responsibility, we will be more likely to usher in a new age of progress and innovation related to health IT.

1. Introduction

Over the past 10 years, many countries have enacted policies calling for health systems to implement an enormously complex set of interconnected, often externally developed, software applications that together create an electronic health record (EHR).[1] Use of EHRs involves a wide variety of stakeholders often with conflicting priorities and requirements. These conflicts are exemplified by the following scenario. Most physicians would ideally like to dictate, write or type a concise, highly technical description of the patient's problem(s) and their treatment plans for their progress note and orders and then have someone else responsible for entering the information into the coded fields required for real-time clinical decision support, quality reporting, and billing.[2] Patients want an easy to understand explanation of their underlying medical problems and a clear explanation of what they should do.[3] The finance department wants a concise, structured note that can generate a defensible bill.[4] The pharmacy wants an unambiguous order for medications that coincide with their current inventory.[5] Researchers want a highly structured note, or one without "typing errors, inconsistency, redundancy and spelling variants" that would allow them to use high-powered data mining algorithms to discover new knowledge.[6] Payer-sponsored quality-based incentive programs want clear evidence that key performance metrics (or reasons for exclusion) have been met.[7] Taken together, these disparate "requirements" make current EHRs overly complex, difficult and time-consuming to use, and error prone.[8,9]

Emerging research on evaluating EHR-related patient safety suggests the need to address both technical and non-technical contextual factors involved (e.g., people, workflow and organizational issues) to overcome safety concerns.[10] Addressing these 'socio-technical' issues

☆ Dr. Sittig is supported in part by a grant from the Agency for Health Care Research and Quality (P30HS024459). Dr. Singh is supported by the VA Health Services Research and Development Service (CRE 12-033; 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 and R21HS023602), and the Houston VA HSR & D Center for Innovations in Quality, Effectiveness and Safety (CIN 13-413).

* Correspondence to: University of Texas – Memorial Hermann Center for Healthcare Quality, 6410 Fannin St. UTPB 1100.43, Houston, TX 77030, United States.
E-mail address: dean.f.sittig@uth.tmc.edu (D.F. Sittig).

http://dx.doi.org/10.1016/j.hjdsi.2017.06.004
Received 16 January 2017; Received in revised form 19 June 2017; Accepted 21 June 2017

Table 1
Overview of five ways that EHRs can fail within an EHR-enabled healthcare system along with potential effects on patient outcomes. (Adapted from J Am Med Inform Assoc. 2015 Mar;22(2):472-8.).

EHR failure mode	Example Problem	Potential Patient Outcome
HIT fails during use or is otherwise not working as designed.[17]	Network problem prevented remote allergy checking from working correctly.[18]	Patient suffers an allergic reaction to medication and spends additional days in the hospital.
HIT is working as designed, but the design does not meet the user's needs or expectations (i.e., bad design).[19]	A weight-based dosing algorithm coupled with a "mode" error causes clinician to enter order for 39-fold overdose of medication.[20]	Patient is given 38 Septra pills, suffers grand mal seizure and has respiratory failure.
HIT is well-designed and working correctly, but was not configured, implemented, or used in a way anticipated or planned for by system designers and developers.	Barcode scanner attached to mobile computer cart does not fit into patient room forcing RN to scan medication before entering room. Wrong patient warning cannot be seen by RN in the room following patient scan.[21]	A patient is given medication prescribed for a different patient; for an antihypertensive their blood pressure drops to dangerously low level; for an antibiotic, infection goes additional 8 h without any treatment.
HIT is working as designed, and was configured and used correctly, but interacts with external systems (e.g., via hardware or software interfaces) so that data is lost or incorrectly transmitted or displayed.[22,23]	Alert for monitoring thyroid function in patients receiving amiodarone stopped working for 3 years when an internal identifier for amiodarone was changed in an external system.[24]	Alert recommending thyroid function testing fired 9774 times less than expected over the 3 year period. Many patients did not receive appropriate thyroid function monitoring.
Specific HIT safety features or functions were not implemented or not available.[25]	Hospitals without an up-to-date, comprehensive back-up of their data and system configuration suffer "ransomware" attack.[26]	At many hospitals "elective operations were canceled, ambulances were diverted away from stricken hospitals, and patients were urged to stay away".[27]

and multiple ways in which EHRs can fail (see Table 1) requires confronting issues related to the design, development, implementation, and use of EHRs. Ensuring EHR safety requires shared responsibility between several entities, including EHR developers and those within the local health care organization who are responsible for configuring, implementing, and using them along with government regulators who create the policies that govern their design, development, and use. But this collaborative spirit has been severely tested. EHR users have blamed developers for poor usability,[11] government officials have blamed developers for lack of interoperability that prevents sharing patient information between different health care delivery systems using different EHR vendors,[12] and EHR developers have even blamed their users for how the EHR is configured by local organizations (e.g., decisions on viewing nursing notes on the main screen)[13] and also the government for not establishing the groundwork for widespread interoperability.[14] These situations have led to potentially devastating errors.[15] The 21st Century Cures Act promises to address many of these concerns through the promulgation of new rules and regulations governing EHR interoperability, usability and security.[16]

In 2011, the Institute of Medicine (IOM) report "Health IT and Patient Safety: Building Safer Systems for Better Care" highlighted that building HIT for safer use is a shared responsibility between "vendors [EHR and clinical content developers], care providers, provider organizations and their HIT departments, and public and private agencies".[28] However, six years later, this concept has gained little traction and EHR developers and users continue to attribute the substantial, long list of problems to each other. A recent IOM report "Improving Diagnosis in Health Care" again emphasizes "collaboration is needed among the HIT vendor community, ONC [Office of the National Coordinator for HIT], and users" to ensure that HIT supports patients and health care professionals in diagnosis; a key to patient safety.[29,30] To chart the path forward, it is imperative that we operationalize the concept of 'shared responsibility' and assign accountabilities to major stakeholders involved.

2. Shared responsibility – an example from the aviation industry

The concept of shared responsibility for passenger safety has been successfully applied within the air transportation industry in which pilots, aircraft manufacturers, and government regulators work together to establish safety standards, report problems, investigate accidents, and disseminate their findings.[31] They have also taken a sociotechnical approach that includes addressing the technical aspects of the aircraft and its manufacturing and maintenance requirements as well as the social components of the policies and procedures that govern issues all the way from crew training and health to assigning the roles and responsibilities of maintenance crews and government inspectors. This type of multi-stakeholder, dynamic collaboration has been tremendously successful not only in building trust between the stakeholders but also reducing the number of accidents. While not always easy to achieve, a focus on ensuring flight safety and accident prevention has helped them overcome their differences.[32] This type of approach is essential to usher in a new age of progress and innovation related to HIT.

3. Why share responsibility for EHR safety?

Poor safety of an EHR being used in a specific health care delivery system (health system) might depend on several factors including: (1) poor design, development, and configuration of the EHR leading to errors in its software; (2) incorrect or incomplete use of EHR technology within the health system; and (3) lack of processes to monitor and improve the EHR and associated health outcomes within the health system.[33] Assigning responsibility to address safety concerns to only the developer responsible for some but not all issues, or only to the health system that has no control over how the system was designed and built, will not be successful because overall safety is based on their combined actions.[34] In this case, shared responsibility requires that the party most in control over the concern being discussed is in the best position to address poor performance.[35] This does not imply that responsibility or actions have to be shared equally for every situation. For example, a poorly designed EHR screen needs to be brought to the attention of those responsible for its development (the EHR developer), who then needs to address the issue. Conversely, an inappropriate drug-drug interaction alert nearly always needs to be brought to the attention of the health system, who should then address it.[36] Finally, the health system needs to thoroughly test and then implement the updated version of the software.[37] Thus, all parties "share" responsibility to take actions required to make the EHR safer to use. In the sections below, we use three challenges currently faced by EHR-enabled health systems as examples that impede safe patient care: interoperability, usability, and security and discuss what it means to share responsibility to address these challenges (see Table 2).[38]