Work 41 (2012) 4484-4489
DOI: 10.3233/WOR-2012-0749-4484
IOS Press

Can we make health IT safe enough for patients?

Robert L Wears, MD, MS, PhD[a,b*]
[a]*Department of Emergency Medicine, University of Florida – Jacksonville, 655 W 8th Street, Jacksonville, FL 32209, USA*
[b]*Centre for Safety and Quality Improvement, Imperial College London, QEQM Building, Praed Street, London W2 1NY, UK*

Abstract. Health information technology (HIT) is widely believed to be an essential modality for improving the efficiency, effectiveness, and safety of healthcare, and has its adoption has been vigorously promoted. However, the safety of commercially available HIT systems has never been independently and rigorously assessed. This paper discusses critical issues to be considered in the development of safe and reliable HIT, and identifies a group of structural impediments that may slow or prevent the arrival of HIT that is actually safe enough for routine clinical use. It argues that this situation is analogous to NASA's promotion of the space shuttle not as an experimental, risky technology, but rather as a routine, ready-for-ordinary-use resource.

Keywords: Health care, safety, information technology, safety-critical computing

"We mistake tools for solutions" [33]

1. Introduction

Healthcare comprises a substantial portion of the domestic economy of most advanced countries (*eg*, approximately 15% of GDP in the US). In addition, it has been associated with a considerable public health burden of mortality and morbidity, with 'defect rates' ranging on the order of 10^{-2} in multiple studies [4,9,13,36,39,45]. Thus, a "triple threat" of inadequate safety, low quality, and high cost afflicts healthcare performance to a greater or lesser degree in all advanced countries.

Health information technology (HIT) has been commonly advocated as a potentially transformative solution to this problem. HIT encompasses a suite of computer-based applications, typically including such subsystems as computerized provider order entry (CPOE), bar-coded medication administration (BCMA), electronic health records (EHR), and clinical decision support (CDS) systems, among others. These technologies, jointly or separately, are felt to be necessary to produce a transformative change in the delivery of care, and most western health systems are involved their implementation, deployment, and use, to a varying degree.

The process has been considerably accelerated in the US by the HITECH (Health Information Technology for Economic and Clinical Health) provisions contained in the 2009 American Recovery and Reinvestment Act [2]. This program provides for up to $44 billion in incentives to care delivery organizations that adopt a certain functional level of HIT (termed "meaningful use" [8]) beginning in 2011. These payments will be gradually phased out and by 2015, financial penalties will be exacted on

* Corresponding author: wears@ufl.edu, +1 904 244 4405, +1 904 244 4508 (fax)

organizations failing to achieve at least this degree of use.

However, despite the widespread high hopes that HIT is ready for widespread deployment [7], a small minority have raised significant questions about the current state of HIT safety [3,10,20,21,23,37,42,44]. This paper will not rehash those arguments, but instead will begin with the minimalist assumption that the safety of the currently available commercial HIT systems has not been objectively and independently established, and will focus on the prospects and problems of developing and / or deploying HIT systems that are safe enough for widespread use.

2. Issues for HIT safety

This section discusses a group of important issues that need to be considered (and which to a large extent have been overlooked) in the development, implementation, and maintenance of HIT that would be "safe enough for patients."

2.1. Design for safety

A fair amount has been learnt about how to design, build, implement, deploy, maintain, and decommission safety critical computing systems, largely from a quarter-century's experience with military, aerospace, and transportation systems [22,24,25,30,35]. Al-though these systems differ in important ways from those that make up HIT, there are a number of important, generalisable lessons that can be drawn from this experience [18].

First, safety must be considered from the earliest phases of system design. Designing systems to be safe is much easier, more effective, and in the long run less costly than adding safety features later [25,43]. (It should be noted here that we are speaking of total system cost; one of the impediments to be discussed later is problem of who benefits and who pays for safety).

Second, system design must take a socio-technical systems approach – that is, the probable environment of use and propensities of future users must be incorporated into the design [15]. If safety depends on users acting correctly, then any risk assessment, risk mitigation, or residual risk acceptance procedure must account for the likelihood of incorrect behaviour and its potential consequences.

2.2. Independent safety assessment

Software engineers have long understood that a system cannot be objectively evaluated by its developers [32]. Even apart from overt conflicts of interest the process of development embeds unspoken assumptions about the manner and environment of use that may be unsubstantiated and thus lead to unexpected consequences or risks. Thus, safety assessments should be independently made by a team or group separate from the developer / vendor. Typically such assessments take the form of a "safety case" argument, an organized, detailed analysis of potential risks, their mitigation, and acceptability [29].

While it is obviously not practical to expect such assessments to include all elements of specific implementation choices or environments, if does not follow that no reasonable assessment at all is possible. Currently, HIT systems (in the US) can be sold, installed, and implemented without any prior assessment at all. The International Standards Organization has developed draft standards for both the production [18] and the deployment and use [19] of HIT that are currently awaiting adoption, although the UK's National Health Service has already decided to begin to use them internally.

However, the US Food and Drug Administration, which has jurisdiction over the marketing and use of medical devices, has historically considered HIT to be a minimal risk device that does not require prior approval, a decision supported by the HIT industry as potentially speeding up innovation.

This lack of oversight does not impact only vendors, because there is similarly no requirement for deploying care delivery organizations to undertake their own safety case analysis prior to deployment or to maintain it based on information gathered during use and maintenance. Thus care delivery organisations typically do not integrate HIT oversight into their overall safety management or governance structures, leaving it as merely a technical task to be performed by technical (*eg*, IT) staff.

Although there have been a few prominent calls for either the FDA or some new regulatory body to undertake the work of ensuring safety assessment [12,16,17], the recent report of the Institute of Medicine's Committee on Patient Safety and Health Information Technology unfortunately shrank from such a recommendation [20], even though no other hazardous industry develops or deploys its information technology in this way.

2.3. Foundational work

There is a second design issue beyond designing for safety specifically, in that current HIT designs have been based on inaccurate models of clinical work. This has long been pointed out as a reason for HIT's slow acceptance by users [5,6], but has not been accepted by either HIT proponents or the industry, who prefer to view the problem of 'resistance' as manifestations of technophobia, inability to type, or old age. There are two reasons for this oversight.

First, the foundational work of understanding the environment of use – the nature of users, their goals, constraints, what conflicts, ambiguities, uncertainties, and time pressures they face – has not been done (personal communication, Matthew Weinger, Vanderbilt University). Because of the lack of attention to the sort of detailed, ethnographic, cognitive engineering foundations [27,38], HIT has been developed based on normative, idealized visions of clinical work that clash too strongly with the realities of the workplace. The result has been systems that interfere with work rather than support it, and the development of work-arounds and other methods of subversion.

The second issue is that the supraordinate goals of HIT are actually mixed; most systems are developed primarily to support administrative aspects of care delivery – billing, inventory control, compliance, management information – rather than to support the front-line worker. These goals are clearly important, and need to be met, but it is likely unwise to attempt to meet both management and front-line work goals in the same system [14,31,41]. This problem has been known as Grudin's Law, one form of which is: "When those who benefit are not those who do the work, then the technology is likely to fail, or at least, be subverted." Essentially, current HIT asks front-line workers to go on diets so managers can lose weight.

These problems are manifest in both the usability and usefulness domains, although the former has gotten a great deal more attention. The few 'official' recognitions of safety problems in HIT have tended to focus on usability, specifically, human-computer interface issues [26,34]. While these are undeniably important, I would argue that the emphasis is misplaced, and that improving usability will not go far in alleviating work-arounds and provider 'resistance' until the system is made more useful to front-line workers in helping them to do their jobs better.

3. Impediments to improvement

Given the current set of broad safety issues outlined above, what are the prospects for addressing them in a useful way? While there has been some progress in the sense of a grudging admission that new safety issues might arise, somehow, the prospects for a serious treatment of HIT safety seem remote, absent a motivating, disastrous incident. There are several structural impediments to progress.

3.1. Ground-up rebuilding

The problems in design can only be remedied in a new design, so clearly, a fundamental approach to safer HIT will involve a ground-up redesign and reinstantiation of HIT systems. This is an unlikely prospect, for two reasons: it is likely to be inordinately expensive, and the prospects for success are not great.

First, although great progress has been made in better understanding how to create reliable software, the software engineering community has still not resolved the problems that earned the label "the software crisis" in 1968 [1]. Software engineering is not yet really engineering; it is reminiscent of materials and structural engineering at the beginning of the 19th century, which was characterized by bridge and tunnel collapses, boiler explosions, and other disasters. We do not currently understand how to create software that is safe, free from defects, performs effectively, and comes in at or under budget. The failure of the National Program for Information Technology (NPfIT) in the UK, which was recently abandoned prior to ever being deployed at an estimated cost of £11 billion (roughly $17 billion), is a cautionary tale in this regard.

In general, more than 70% of large software projects fail (either outright, or by means of underperformance, cost or schedule overruns) [40]; the larger and more complex the project, the lower the probability of success, and HIT is arguably much more complex than other, simpler systems that have met with failure. New development of an EHR has been optimistically (not allowing for failures, cost overruns, schedule slips, security issues, shoddy software, *etc*) estimated to require 10 years, $320 billion in development costs and $20 billion per year

in operating costs (in 2005 dollars) [11]. Given the current US budget crisis and vendors' sunk costs in current technology, this is unlikely to occur; and the $44 billion promised (for deployment, not development) in the HITECH provisions is barely a down payment.

3.2. Mixed incentives

Although it has been previously noted that the overall costs of safe IT systems are thought to be lower, those costs and savings are differentially borne. Vendors must invest time and effort in foundational work, redesign and re-programming, but the savings accrue not to them but to their customers, the care delivery organizations. And, the broader computing industry has shown no more progress (and arguably less inclination) in resolving their quality problems than has healthcare [28].

3.3. Escalation of commitment

Finally, a fundamental rethinking of the way HIT could actually be useful in improving the safety and quality of care with a minimum of new risks entailed is problematic, because embarking on such an effort implicitly indicates that current efforts have not worked out as hoped. The HITECH provisions represent an escalation of commitment issue, a form of continuation or sunk cost bias, in which problems are addressed by greater effort and exhortation along the same paths, rather than looking for new paths to solutions. Ironically, the activity stimulated by the HITECH provisions may slow the arrival of safe and reliable HIT, for three reasons. It has stimulated sales of current systems, thus removing market pressure for improvement. Second, it has soaked up available resources. Vendor staff are so busy doing installs there is little discretionary effort available for redesign or product improvements. And finally, care delivery organizations are committing significant proportions of their operating capital to new HIT systems. This will create a pent-up demand for capital investment in those alternatives that have been deferred, rendering delivery organizations unable to invest in new versions, improvements, and maintenance.

4. Conclusion

The opening quote for this paper, from a NASA engineer, encapsulates the HIT safety problem. Policy makers have mistaken research-oriented prototypes – successful experiments, in reality – for production ready, broadly deployable tools. In so doing, they are re-enacting NASA's fundamental error in its deployment and promotion of the space shuttle [33]; rather than face the reality that HIT is still very much a technology in its infancy, a work-in-progress, they have instead promoted it as a ready-to-go "magic bullet" that can be used in a practical, everyday manner. Just as with NASA, this self-deception was practiced with the best of motivations, but it is self-deception nonetheless. We can only hope that it does not take the HIT equivalent of *Challenger* and *Columbia* to bring about a change in course.

References

1. Software Engineering: Report of a Conference Sponsored by the NATO Science Committee. In: Naur P, Randell B, eds. Garmisch, Germany; 1968:231.
2. The Recovery Act. www.recovery.gov, accessed 20 November 2011.
3. HIT Safety Hearing. In: *Office of the National Coordinator. HIT Policy Committee Adoption / Certification Workgroup*. Washington, DC: Office of the National Coordinator. HIT Policy Committee Adoption / Certification Workgroup; 2010.
4. Amalberti R. The paradoxes of almost totally safe transportation systems. *Safety Science* 2001;37(2-3):109-126.
5. Berg M. *Rationalizing Medical Work*. Cambridge, MA: MIT Press; 1997, 238 pages.
6. Berg M. *Health Information Management: Integrating Information Technology in Health Care Work*. London, UK: Routledge; 2004.
7. Blumenthal D. Final Rules to Support Meaningful Use of EHRs. http://www.hhs.gov/news/imagelibrary/video/2010-07-13_press.html, accessed 20 November 2011.
8. Blumenthal D, Tavenner M. The "Meaningful Use" Regulation for Electronic Health Records. *N Engl J Med* 2010:NEJMp1006114.
9. Brennan TA, Leape LL, Laird NM, Hebert L, Localio AR, *et al.* Incidence of adverse events and negligence in hospitalized patients. Results of the Harvard Medical Practice Study I. *N Engl J Med* 1991;324(6):370-376.
10. Campbell EM, Sittig DF, Ash JS, Guappone KP, Dykstra RH. Types of Unintended Consequences Related to Computerized Provider Order Entry. *J Am Med Inform Assoc* 2006;13:547 - 556.
11. Charette RN. Why software fails. *IEEE Spectrum* 2005;42(9):42 - 48.
12. Cook RI. Dissenting Statement: Health IT is a Class III Medical Device. In: IOM Committee on Patient Safety

and Health Information Technology, ed. *Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington, DC: National Academies Press; 2011: pp E1 - E4.
13. Forster AJ, Asmis TR, Clark HD, Al Saied G, Code CC*, et al.* Ottawa Hospital Patient Safety Study: incidence and timing of adverse events in patients admitted to a Canadian teaching hospital. *CMAJ* 2004;170(8):1235-1240.
14. Garfinkel H. "Good" organizational reasons for "bad" clinic records. In: *Studies in Ethnomethodology*. Cambridge, UK: Blackwell Publishing Ltd; 1967: pp 186 - 207.
15. Harrison MI, Koppel R, Bar-Lev S. Unintended Consequences of Information Technologies in Health Care - An Interactive Sociotechnical Analysis. *J Am Med Inform Assoc* 2007:(web publication, in press).
16. Hoffman S, Podgurski A. Finding a cure: the case for regulation and oversight of electronic health record systems. *Harvard Journal of Law & Technology* 2008;22(1):104 - 165.
17. Hoffman S, Podgurski A. Why electronic health record systems require safety regulation. *Hastings Center Bioethics Forum* 2009; 39. http://www.thehastingscenter.org/Bioethicsforum/Post.aspx?id=3284, accessed 2 April 2009.
18. International Standards Organization. *Health informatics -- application of clinical risk management to the manufacture of health software*. International Standards Organization; ISO/TS 29321:2008; 2008, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45411, 80 pages.
19. International Standards Organization. *Health informatics -- guidance on the management of clinical risk relating to the deployment and use of health software systems*. International Standards Organization; ISO/TS 29322:2008(E); 2008, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45412, 74 pages.
20. IOM Committee on Patient Safety and Health Information Technology. *Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington, DC: National Academies Press; 2011, 197 pages.
21. Jackson D, Thomas M, Millett LI, eds. *Software for Dependable Systems: Sufficient Evidence?* Washington, DC: National Academy Press; 2007, 148 pages.
22. Johnson CW. *Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting*. Glasgow, Scotland: University of Glasgow Press; 2003, 986 pages.
23. Koppel R, Metlay JP, Cohen A, Abaluck B, Localio AR*, et al.* Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors. *JAMA* 2005;293(10):1197-1203.
24. Leveson NG. Software safety: why, what, and how. *ACM Computing Surveys* 1986;18(2):125 - 163.
25. Leveson NG. *Safeware: System Safety and Computers*. Boston: Addison-Wesley; 1995, 680 pages.
26. National Institute of Standards and Technology. Usability in Health IT: Technical Strategy, Research, and Implementation. In. Gaithersburg, MD; 2010:20.
27. Nemeth CP, Cook RI, Woods DD. The messy details: insights from the study of technical work in health care. *IEEE Transactions on Systems, Man and Cybernetics: Part A* 2004;34(6):689 - 692.
28. Pogue D. The year of CEO failures explained. http://pogue.blogs.nytimes.com/2011/12/15/the-year-of-c-e-o-failures-explained/?ref=personaltechemail&nl=technology&emc=cta1, accessed 20 December 2011.
29. Reason J. *Managing the Risks of Organizational Accidents*. Aldershot, UK: Ashgate Publishing Co; 1997, 252 pages.
30. Redmill F, Rajan J. *Human Factors in Safety-Critical Systems*. Oxford, UK: Butterworth - Heineman; 1997, 354 pages.
31. Rosenbloom ST, Denny JC, Xu H, Lorenzi N, Stead WW, Johnson KB. Data from clinical notes: a perspective on the tension between structure and flexible documentation. *Journal of the American Medical Informatics Association* 2011;18(2):181-186.
32. Sommerville I. *Software Engineering*. Third ed. Reading, MA: Addison-Wesley Publishing Company; 1989, 653 pages.
33. Starbuck WH, Stephenson J. Making NASA more effective. In: Starbuck WH, Farjoun M, eds. *Organization at the Limit: Lessons from the Columbia Disaster*. Oxford, UK: Blackwell Publishing; 2005: pp 309 - 335.
34. Steering Committee on the Usability Security and Privacy of Computer Systems, ed. *Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop*. Washington, DC: National Academy Press; 2010, 70 pages.
35. Storey N. *Safety-Critical Computer Systems*. Harlow, UK: Pearson Education Limited; 1996, 453 pages.
36. Thomas EJ, Studdert DM, Burstin HR, Orav EJ, Zeena T*, et al.* Incidence and types of adverse events and negligent care in Utah and Colorado. *Med Care* 2000;38(3):261-271.
37. van Rosse F, Maat B, Rademaker CM, van Vught AJ, Egberts AC, Bollen CW. The effect of computerized physician order entry on medication prescription errors and clinical outcome in pediatric and intensive care: a systematic review. *Pediatrics* 2009;123(4):1184-1190.
38. Vicente KJ. *Cognitive Work Analysis*. Mahwah, NJ: Lawrence Erlbaum Associates; 1999, 398 pages.
39. Vincent C, Neale G, Woloshynowych M. Adverse events in British hospitals: preliminary retrospective record review. *BMJ* 2001;322(7285):517-519.
40. Wallace L, Keill M. Software project risks and their effect on outcome. *Communications of the ACM* 2004;47(4):68 - 73.
41. Wears RL. The chart is dead--long live the chart. *Ann Emerg Med* 2008;52(4):390-391.
42. Wears RL, Berg M. Computer Technology and Clinical Work: Still Waiting for Godot. *JAMA* 2005;293(10):1261-1263.
43. Wears RL, Leveson NG. "Safeware": safety-critical computing and healthcare information technology. In: K H, Battles JB, Keyes MA, Grady ML, eds. *Advances in Patient Safety: New Directions and Alternative Approaches.* AHRQ Publication No. 08-0034-4 ed. Rockville, MD: Agency for Healthcare Research and Quality; 2008: pp 1 - 10.
44. Weiner JP, Kfuri T, Chan K, Fowles JB. "e-Iatrogenesis": The Most Critical Unintended Consequence of CPOE and other HIT. *J Am Med Inform Assoc* 2007;14(3):387-388.

45. Wilson RM, Runciman WB, Gibberd RW, Harrison BT, Newby L, Hamilton JD. The Quality in Australian Health Care Study. *Med J Aust* 1995;163(9):458-471.