Reducing Risks by Engineering Resilience into HIT for EDs

Principal Investigator: Robert L. Wears, MD, MS, PhD

Team Members:

John Wreathall

Rollin (Terry) Fairbanks, MD, MS

Ann M. Bisantz, PhD

Shawna J Perry, MD

Chris Johnson, PhD

Erik Hollnagel, PhD

Ross Koppel, PhD

L. Kendall Webb, MD

Primary Organization: University of Florida

Project Period: 30 Sep 2008 – 31 Mar 2012

Federal Project Officer: Denise Burgess

Grant Number: 1R18 HS017902-01

Abstract

Purpose: To develop guidance for care delivery organizations for safely and resiliently operating and maintaining their safety-critical HIT systems.

Scope:

Methods: Review of technical standards and documents related to safety-critical computing in other domains, reducing and distilling them to a simple, web-based format, and eliciting feedback and potential modifications from users based on their experience. Interviews with key organizational personal in the management of care delivery organizations; in HIT management; and in IT management in non-healthcare, safety-critical industries (*eg*, commercial aviation). Essentially, qualitative methods were used in review and summarization; thematic saturation was used to limit data collection.

Results: In total, 45 documents were identified for initial review: 11 general standards documents, 11 US government civilian guidance or standards documents, four military standards, and 19 scientific books or papers relevant to safety critical computing. These were supplemented as additional materials came to light over the course of the project. The data were summarized into seven modules (IT safety management systems, risk assessment, change management, anomaly response, usability issues, legal and contracting issues, and adequacy of feedback. These modules (and associated introduction, bibliography, and glossary) were instantiated in a wiki, at http://www.complex-work.org/hit. The site has shown steady growth since it was first opened to the public, with roughly 120 unique visitors from 10 countries; each visitor views an average of five pages, for about 3 minutes each.

Key Words: health information technology; patient safety; safety-critical computing

1. Purpose

Though the safety and quality benefits of introducing information technology into healthcare seem readily apparent [1-7], the difficulties associate with health information technology (HIT) are also daunting [8-14], and HIT-related risks are just beginning to become apparent [15-19]. System maintenance has lead to missing [20] or false laboratory information [21] and incorrect guidance in decision support [22]; computerized provider order entry, the 'Holy Grail' of safety efforts, has led to new forms of failure [15,16,23,24]. To date, these risks have largely been related to problems with the human-computer interface [15,23] or to unintended interaction with existing work practices [16]. The idea that the technology itself might be inherently unsafe – that it might lead to adverse outcomes due to internal faults or unexpected interactions with users or external devices, *even when the system is operating as intended by its designers and in the absence of human factors or work practices problems* – has barely been recognized in these discussions. This problem leads to the two, broad, long-term objectives for this project:

1. To mitigate the hazards identified in the previously conducted proactive risk assessment (PRA) with respect to HIT-related hazards in the emergency department (ED) setting.
2. To improve the resilience of HIT by enhancing the ability of HIT systems, and the larger sociotechnical systems in which they are embedded, to survive and return to normal operations despite challenges, expected or unexpected, with a minimum of adverse effects on patients.

We approached these objectives by developing a toolkit to enable care delivery organizations to identify and rank the safety criticality of their information systems and components on a continuing basis, to assess their ability to manage maintenance (upgrades, patches) and anomalies (faults or error reports), and to identify potential usability issues.

2. Scope

Background and Context. Because the safety of HIT has seldom been studied, we used guidance documents from other safety-critical computing endeavors in other industries as sources for the guidance to be developed. We chose to use a resilience approach in the project. That is, rather than focusing on striving for systems that can never fail, we focused instead on enhancing the ability of organizations to rapidly recover from inevitable failures and to minimize their adverse consequences.

In addition, we focused most of our attention on the maintenance and operations phases of the system life cycle [25-28], for two reasons. First, a good deal of guidance is

available for the acquisition and implementation phases of HIT systems; second, these are the longest-lasting phases, and the majority of failures occur in them [25].

The original proposal envisioned alpha- and beta-testing of the guidance developed at the participating sites, but this plan was seriously challenged by the somewhat chaotic organizational changes in the information technology strategy at Shands and UF, intended to take advantage of ARRA and the HITECH Act funding opportunities. As previously reported, this seriously impacted these efforts in several ways: a loss of local IT leadership; competition for IT professionals time, effort, and interest; and paradoxically, by a marginalization of IT safety interests, because they were interpreted as opposition to the new IT strategic plan.

As a result, we shifted to a more diffused mode of evaluation, by realizing the guidance being developed in a wiki form (http://www.complex-work.org/hit), to allow for continuing development and modification via 'crowd-sourcing' as experience is gained and captured feedback assessments via personal reports from key organization members as well as a web-based survey tool (based on the Technology Acceptance Model) attached to the wiki.

Settings and Participants. The primary site for the project was the University of Florida's second largest hospital, Shands Jacksonville, in Jacksonville, FL. Shands is a large, 450-bed, urban teaching hospital serving primarily an inner city, indigent population. The second site was Strong Memorial Hospital in Rochester, NY; Strong is a large academic medical center that is the primary teaching hospital for the University of Rochester. The two centers had markedly different IT systems at the beginning of the project but have converged remarkably as a result of the changes occasioned by the HITECH Act.

Interview subjects included two IT managers, two IT technical experts charged with system safety and integrity, one CIO, two clinical department managers, one CMO, and one COO. The research team included clinicians, IT professionals, and safety engineers.

3 Methods

Data sources. Because little study has been made of the safety of HIT, we sought to summarize, compile, and translate to relevant language, standards, and guidance for safe computing from other safety critical industries, such as aviation, the military, nuclear power, *etc*. We supplemented these data with guidance from scientific papers and books relevant to safety-critical computing. During the project, we repeatedly scanned the horizon for new materials potentially relevant to the work. We supplemented this archival review material with interviews of key personnel from

three stakeholder groups: clinical managers; high-level hospital managers; and IT technical and management leaders.

Development methods. Because of the disparate nature of the source materials, qualitative methods were used to summarize, compile, and translate for a clinical audience the various document and standards that had been identified. Each document was reviewed and summarized by two or more members of the research team and jointly in discussions at team meetings and Skype sessions.

A specific decision was made to use an informal rather than an academic style in producing the guidance, as it seemed that this would be more accessible to the target audience. Finally, the guidance was instantiated as a wiki and loaded onto a website. The wiki modality gives several advantages. First, it greatly enabled cooperation and joint editing and development within the project team, because edits in place could be readily viewed by the entire group without having the overhead of scheduling required by synchronous work. Second, the format is familiar to users in terms of both navigation and modification. Finally, and more importantly, it supports continuing development and extension of the guidance based on the experience of users who choose to contribute by adding to or modifying its pages. Though this 'crowd-sourcing' process brings some potential risks (and a requirement for supervision), it in principle will be self-correcting and ultimately will allow the guidance to be a compendium of users' experiences, and thus become a living, continuing resource.

Evaluation. As it became progressively clear that none of the project organizations would be in a position to fully implement the guidance, we obtained targeted feedback from key personnel within the organization and at one external organization to help shape the development of the guidance. This led to considerable revision in shortening and simplifying the materials selected for final inclusion.

In order to supplement the direct feedback obtained from participants, the Technology Acceptance Model instruments previously developed in paper form were translated to a web-based survey format and attached to each of the seven modules to capture users' assessments going forward in time.

5. Results

Forty-five documents were identified for initial review: 11 general standards documents, 11 US government civilian guidance or standards documents, four military standards, and 19 scientific books or papers relevant to safety critical computing. These were supplemented as additional materials came to light over the course of the project; in the end, 81 documents were reviewed.

The data were summarized into seven modules (IT safety management systems, risk assessment, change management, anomaly response, usability issues, legal and contracting issues, and adequacy of feedback). These modules (and associated introduction, bibliography, and glossary) were instantiated in a wiki, entitled *Managing HIT Safely and Resiliently*, available at:

http://www.complex-work.org/hit

The site has shown steady growth since it was first opened to the public, with roughly 120 unique visitors from 10 countries; each visitor views an average of five pages, for about 3 minutes each.

Because the wiki site suffered initially from some nonmalicious vandalism, its security was tightened to allow only registered users to make changes. (Registration requires only a name and a valid email address, but at this writing we have only 10 registered users). In addition, the team is notified anytime a page is modified and the wiki software records all change so that they can be rolled back by an administrator if necessary. We believe that this issue is sufficiently controlled, so we can begin to publicize the wiki to attract broader participation in its growth and development.

Feedback from users has been mixed. Although the consensus of both IT and management personnel when queried directly has been favorable in terms of both usefulness and usability, and although the guidance has been modified based on their suggestions, there has been considerable concern expressed that their organizations would not be willing to commit the time and effort required to fully implement these procedures. In addition, feedback from users suggested that many potential users would have difficulty in responding to some of the self-assessment items initially, as they would raise issues that had not been previously considered. From a safety point of view, that would be considered a good thing, but, in order to reduce frustration and increase acceptance, we modified the introductory section to point out that such an eventuality was actually a form of progress and encouraged future feedback and modification of the wiki-based guidance with users' additional experiences. Taken as a whole, these results suggest that care delivery organizations need assistance in attending to the deeper safety issue raised by HIT and perhaps even need either some sort of regulatory floor (beyond HIPAA) or at least a much broader awareness of the risks of current HIT.

6. List of Publications and Products

The following publications, presentations, and other products have resulted in whole or in part from this project.

Journal Articles.

Fairbanks RJ, Wears RL. Hazards With Medical Devices: The Role of Design. *Ann Emerg Med* 2008;52(5):519-521.

Guerrera TK, Fairbanks RJ, Karn KS, Caplan SH, Shah MN, Wears RL. Usability evaluation of an emergency department information system. *Academic Emergency Medicine* 2008;15(5):S27 - S28.

Karsh B-T, Weinger MB, Abbott PA, Wears RL. Health information technology: fallacies and sober realities. *Journal of the American Medical Informatics Association* 2010;17(6):617 - 623.

Patterson ES, Rogers ML, Tomolo AM, Wears RL, Tsevat J. Comparison of extent of use, information accuracy, and functions for manual and electronic patient status boards. *International Journal of Medical Informatics* 2010;79(12):817-823.

Pennathur P, Cao D, Bisantz A, Lin L, Fairbanks R, *et al.* Emergency Department Patient Tracking System Evaluation. *International Journal of Industrial Ergonomics* 2011;41(4):360 - 369.

Handel DA, Wears RL, Nathanson LA, Pines JM. Using Information Technology to Improve the Quality and Safety of Emergency Care. *Academic Emergency Medicine* 2011;18(6):e45-e51.

Conference Proceedings.

Johnson CW. Politics and patient safety don't mix: understanding the failure of large-scale software procurement for healthcare systems. *Proceedings of the Fourth IET System Safety Conference* London, UK: IET Conference Publications; 2009 http://www.dcs.gla.ac.uk/~johnson/papers/politics_hit.pdf.

Gilardi S, Guglielmetti C, Perry SJ, Pravettoni G, Wilson S, Wears RL. People, technology and complex work in health care. *Proceedings of the 9th International Naturalistic Decision-Making Conference*: p. 316 - 318. Covent Garden, London, UK; 2009.

Patterson ES, Wears RL, Militello LG, Anders S, Karsh B-T. Medical informatics: what contributions can human factors make? *Proceedings of the 53rd Human Factors and Ergonomics Society* in press. San Antonio, TX; 2009.

Perry SJ, Wears RL, Chozos N. "It came from within": clinical impact of latent IT failures on patient safety. *Proceedings of the 2008 International Conference on Healthcare Ergonomics and Patient Safety* Strasbourg, FR; 25 - 27 June 2008.

Perry SJ, Wears RL, Spillane J. When worlds collide: two medication systems in one emergency department. In: Hollnagel E, Pieri F, Rigaud E, eds. *3nd International Symposium on Resilience Engineering*. 28 - 30 October 2008 ed. Juan-les-Pins, France: Mines ParisTech; 2008:219 - 226.

Bisantz AM, Karsh B-T, Wears RL, Lewis VR, Ancker JS, Fairbanks RJ. Health information technology: can there be meaningful use without meaningful design? *Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting*: p 808 - 812. Las Vegas, NV;19 - 23 September 2011.

Wears RL, Webb LK. Fundamental on situational surprise: a case study with implications for resilience. *Proceedings of the 4th International Conference on Resilience Engineering*: p 270 -276. Sophia Antipolis, France;6 - 8 June 2011.

Wears RL. Can we make health IT safe enough for patients? *Proceedings of the International Ergonomics Association*: p in press. Recife, Brazil;12 - 16 February 2012.

Wears RL. I'm from the EHR and I'm here to help you. *Proceedings of the Human Factors and Ergonomics Society Medical Symposium* Baltimore, MD;12 - 13 March 2012.

Reports

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.

Electronic Resources

Wears RL. Health information technology risks. *The Risks Digest* 2010; 26. *http://catless.ncl.ac.uk/Risks/26.25.html#subj1*, accessed 14 December 2010.

Wears RL. Re: Health information technology risks (Kenzo, RISKS-26.30). *The Risks Digest* 2010; 26. *http://catless.ncl.ac.uk/Risks/26.31.html#subj15*, accessed 24 January 2011.

Safe HIT Working Group. Managing Health Information Technology Safely and Resiliently. *http://www.complex-work.org/hit,* accessed 29 June 2012.

Book Sections

Koppel R, Davidson S, Wears RL, Sinsky CA. Health care information technology to the rescue. In: Koppel R, Gordon S, eds. *First Do Less Harm: Confronting the Inconvenient Problems of Patient Safety*. Ithaca, NY: Cornell University Press; 2012: pp 62 - 89.

References

1. Bates DW, Cohen M, Leape LL, Overhage JM, Shabot MM, Sheridan T. Reducing the frequency of errors in medicine using information technology. *J Am Med Inform Assoc* 2001;8(4):299-308.
2. Bobb A, Gleason K, Husch M, Feinglass J, Yarnold PR, Noskin GA. The epidemiology of prescribing errors: the potential impact of computerized prescriber order entry. *Arch Intern Med* 2004;164(7):785-792.
3. Executive Order: Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Programs. *http://www.whitehouse.gov/news/releases/2006/08/print/20060822-2.html*, accessed 29 August 2007.
4. Rosenfeld S, Bernasek C, Mendelson D. Medicare's next voyage: encouraging physicians to adopt health information technology. *Health Aff (Millwood)* 2005;24(5):1138-1146.
5. Taylor R, Bower A, Girosi F, Bigelow J, Fonkych K, Hillestad R. Promoting health information technology: is there a case for more-aggressive government action? *Health Aff (Millwood)* 2005;24(5):1234-1245.
6. Leapfrog Group. Leapfrog initiatives to drive great leaps in patient safety. *http://www.leapfroggroup.org/safety1.htm*, accessed 17 October 2000.
7. Leapfrog Group. The Leapfrog Group Fact Sheet. *http://www.leapfroggroup.org/media/file/leapfrog_factsheet.pdf*, accessed 29 August 2007.
8. Jha AK, Poon EG, Bates DW, Blumenthal D, Middleton B, *et al.* Defining the priorities and challenges for the adoption of Information Technology in HealthCare: opinions from an expert panel. *AMIA Annu Symp Proc* 2003:881.
9. Kaushal R, Blumenthal D, Poon EG, Jha AK, Franz C, *et al.* The costs of a national health information network. *Ann Intern Med* 2005;143(3):165-173.
10. Ash JS, Stavri PZ, Kuperman GJ. A consensus statement on considerations for a successful CPOE implementation. *J Am Med Inform Assoc* 2003;10(3):229-234.
11. Ash JS, Berg M, Coiera E. Some Unintended Consequences of Information Technology in Health Care: The Nature of Patient Care Information System-related Errors. *J Am Med Inform Assoc* 2004;11(2):104-112.
12. Ash JS, Sittig DF, Dykstra RH, Guappone K, Carpenter JD, Seshadri V. Categorizing the unintended sociotechnical consequences of computerized provider order entry. *International Journal of Medical Informatics* 2007;76(Supplement 1):S21-S27.
13. Berg M. *Health Information Management: Integrating Information Technology in Health Care Work*. London, UK: Routledge; 2004.

14. Wears RL, Berg M. Computer Technology and Clinical Work: Still Waiting for Godot. *JAMA* 2005;293(10):1261-1263.
15. 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.
16. Han YY, Carcillo JA, Venkataraman ST, Clark RSB, Watson RS, *et al.* Unexpected Increased Mortality After Implementation of a Commercially Sold Computerized Physician Order Entry System. *Pediatrics* 2005;116(6):1506-1512.
17. Perry SJ, Wears RL, Cook RI. The role of automation in complex system failures. *Journal of Patient Safety* 2005;1(1):56-61.
18. Wears RL, Cook RI, Perry SJ. Automation, interaction, complexity, and failure: a case study. *Reliability Engineering and System Safety* 2006;91(12):1494-1501.
19. McDonald CJ. Computerization can create safety hazards: a bar-coding near miss. *Ann Intern Med* 2006;144(7):510-516.
20. Wears RL. More on computer glitches and laboratory result reporting. *http://catless.ncl.ac.uk/Risks/23.64.html#subj4*, accessed 29 December 2004.
21. Burstein D. Canadian medical tests give reversed results. *http://catless.ncl.ac.uk/Risks/23.19.html#subj2*, accessed 19 February 2004.
22. Northern General Hospital NHS Trust. Report of the Inquiry Committee into the Computer Software Error in Downs Syndrome Screening. *http://kingsfund.koha-ptfs.eu/cgi-bin/koha/opac-detail.pl?biblionumber=30167*, accessed 13 March 2005.
23. Horsky J, Kuperman GJ, Patel VL. Comprehensive analysis of a medication dosing error related to CPOE. *J Am Med Inform Assoc* 2005;12(4):377-382.
24. Baldwin FD. Physician resistance arrests CPR system. In: *Healthcare Informatics*; 2003:34 - 36.
25. Sommerville I. *Software Engineering*. Third ed. Reading, MA: Addison-Wesley Publishing Company; 1989, 653 pages.
26. Storey N. *Safety-Critical Computer Systems*. Harlow, UK: Pearson Education Limited; 1996, 453 pages.
27. Leveson N. A new accident model for engineering safer systems. *Safety Science* 2004;42(4):237 - 270.
28. US Food and Drug Administration. General Principles of Software Validation; Final Guidance for Industry and FDA Staff. *http://www.fda.gov/cdrh/comp/guidance/938.pdf*, accessed 14 April 2008.
29. Perry SJ, Wears RL, Chozos P, Johnson CW, Smith KF. Consequential analysis of information system criticality in a healthcare organization. *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting*: p 1466-1468. San Francisco, CA: Human Factors and Ergonomics Society.

30. Wears RL, Perry SJ, Chozos N, Johnson CW. Plausibly correct, but wrong: a failure phenotype in health IT. *Proceedings of the 2nd Annual Patient Safety & Health IT Conference* Washington, DC; 5 June 2006: AHRQ.