Abha Agrawal
Editor

Safety of Health IT

Clinical Case Studies

Springer

Safety of Health IT

Abha Agrawal
Editor

Safety of Health IT

Clinical Case Studies

Springer

Editor
Abha Agrawal, MD, FACP, FACHE
Norwegian American Hospital
Chicago, IL, USA

Northwestern Feinberg School of Medicine
Chicago, IL, USA

ISBN 978-3-319-31121-0 ISBN 978-3-319-31123-4 (eBook)
DOI 10.1007/978-3-319-31123-4

Library of Congress Control Number: 2016944808

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

To
Mummy, Papa, and Kanha

Acknowledgements

The idea for this book emerged from my numerous conversations with physicians, nurses, and other health care providers expressing their dissatisfaction with and concerns about the current state of health information technology such as electronic health records. I am thankful to all of them for sharing their concerns and constructive solutions so generously and for being dedicated to their profession and their patients in spite of all the challenges.

I am immensely grateful to all the contributing authors. This book would not have been possible without their generous commitment to share their expertise and insights. They passionately believe that technology plays a vital role in improving patient safety and hence a clinical case-based discussion of emerging risks of technology and constructive solutions is imperative for ensuring safe care.

All patients with whom I have interacted with directly in patient care or indirectly in my administrative role bear my deepest gratitude. By allowing the clinical teams to peek inside their body and mind so that we can care for them, they are our greatest source of inspiration and motivation.

Lastly, I am eternally grateful for my son Kanha's unadulterated enthusiasm for life, sense of curiosity, boundless energy, and infectious laughter. He makes life worthwhile and beautiful.

Chicago, IL, USA Abha Agrawal MD, FACP, FACHE

Contents

Contributors

Julia Adler-Milstein, Ph.D. School of Information and School of Public Health, University of Michigan, Ann Arbor, MI, USA

Abha Agrawal, M.D., F.A.C.P., F.A.C.H.E Norwegian American Hospital, Chicago, IL, USA

Northwestern Feinberg School of Medicine, Chicago, IL, USA

Jonathan S. Bagby, M.S.N., M.B.A., R.N-.B.C. United States Department of Veterans Affairs, Roanoke, VA, USA

Elizabeth M. Borycki, R.N., Ph.D. School of Health Information Science, University of Victoria, Victoria, BC, Canada

Michelle A. Chui, Pharm.D., Ph.D. Social and Administrative Sciences Division, University of Wisconsin-Madison School of Pharmacy, Madison, PA, USA

Enrico Coiera, M.B.B.S., Ph.D., F.A.C.M.I. Centre for Health Informatics, Australia Institute of Health Innovation, Faculty of Medicine and Health Sciences, Macquarie University, Sydney, NSW, Australia

Peter A. Doyle, Ph.D. Clinical Engineering Services, The Johns Hopkins Hospital, Baltimore, MD, USA

Eric C. Ford, Ph.D. Radiation Oncology, University of Washington, Seattle, WA, USA

Richard M. Frankel, Ph.D. Indiana University School of Medicine, Center for Excellence in Healthcare Communication, Cleveland Clinic, Indianapolis, IN, USA

Center for Healthcare Information and Communication (CHIC), Richard L. Roudebush Veterans Administration Medical Center, Indianapolis, IN, USA

Anupam Goel, M.D., M.B.A. Clinical Information, Advocate Health Care, Clinical Transformation, Downers Grove, IL, USA

Lucinda Roper, Medical Student (4th Year) UNSW Medicine, University of NSW, Sydney, NSW, Australia

Michael G. Herman, Ph.D. Radiation Oncology, Medical Physics, Mayo Clinic, Rochester, NY, USA

Jan Horsky, Ph.D. Division of General Internal Medicine and Primary Care, Brigham & Women's Hospital, Boston, MA, USA

Daniel Hyman, M.D., M.M.M. Quality & Patient Safety, Children's Hospital Colorado, Aurora, CO, USA

Christine Jorm, M.B.B.S. (Hons.), M.D., Ph.D., F.A.N.Z.C.A. Sydney Medical School, Sydney University, Sydney, NSW, Australia

Andre Kushniruk, M.Sc., Ph.D. School of Health Information Science, University of Victoria, Victoria, BC, Canada

Marilyn Lamar, B.S., J.D. Liss & Lamar, P.C., Oak Brook, IL, USA

Farah Magrabi, B.E., Ph.D. Centre for Health Informatics, Australia Institute of Health Innovation, Faculty of Medicine and Health Sciences, Macquarie University, Sydney, NSW, Australia

Sandeep S. Mangalmurti, M.D., J.D. Section of Cardiology, Bassett Heart Care Institute, Cooperstown, NY, USA

Olufunmilola Abraham, Ph.D., M.S., B.Pharm. Department of Pharmacy and Therapeutics, University of Pittsburgh School of Pharmacy, Pittsburgh, PA, USA

Mei-sing Ong, B.E., Ph.D. Centre for Health Informatics, Australia Institute of Health Innovation, Faculty of Medicine and Health Sciences, Macquarie University, Sydney, NSW, Australia

Carol J. Parker, M.P.H. College of Human Medicine, Michigan State University, East Lansing, MI, USA

JoAnne Phillips, D.N.P., R.N., C.P.P.S. Penn Care at Home, Bala Cynwyd, PA, USA

Eric Rose, M.D., F.A.A.F.P. Departments of Family Medicine and Biomedical Informatics and Medical Education, University of Washington, Seattle, WA, USA

Loren J. Schleiden, B.S. Department of Pharmacy and Therapeutics, University of Pittsburgh School of Pharmacy, Pittsburgh, PA, USA

Heleen van der Sijs, Pharm.D., Ph.D. Department of Hospital Pharmacy, Erasmus University Medical Centre, Rotterdam, The Netherlands

S. Andrew Spooner, M.D., M.S. Department of Pediatrics, Cincinnati Children's Hospital Medical Center, University of Cincinnati College of Medicine, Cincinnati, OH, USA

Lynn Voss, B.S., Six Sigma Black Belt Quality & Patient Safety, Children's Hospital Colorado, Aurora, CO, USA

Chapter 1
First Do No Harm: An Overview of HIT and Patient Safety

Abha Agrawal

A 44-year-old patient with pneumonia is ordered an antibiotic at 9 AM to be administered twice a day using the hospital's newly implemented computerized physician order entry system. The software automatically calculates the antibiotic administration time to 8 AM and 8 PM. The patient doesn't receive the first dose till 8 PM–11 h later—because the order was written after 8 AM and computer system knows to trigger only default administration times on the nursing medication administration screen. Neither the physicians nor the nurses had a clear mechanism of knowing this gap in the technology system.

******

A nurse is using the bar-coded medication administration system, touted as a safety technology, with a modern wireless scanner and medication cart. While administering and documenting medications on a complex patient who is on nine medications, she hits a "cold spot" in the hospital's wireless network. She has to spend over 15 min to redo the entire work delaying medication administration for other patients and causing her anxiety and frustration.

****

Due to high noise levels and "noise fatigue" among staff and patients, an ICU nurse silences the alarm system on a cardiac monitor on an ICU patient. She thought this was a temporary change but the system took it to be a permanent change. Later in the evening, the patient is found deceased in his room. The monitor tracings show that he had a fatal arrhythmia that would have normally alerted the staff for prompt life-saving measures had the alarm not been "silenced."

A. Agrawal, M.D., F.A.C.P., F.A.C.H.E. (✉)
Norwegian American Hospital, Chicago, IL, USA

Northwestern Feinberg School of Medicine, Chicago, IL, USA
e-mail: agrawal.abha@gmail.com

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_1

******

A 66-year-old woman, mother of three and grandmother of five, visits her primary care physician with chest symptoms. The physician orders a chest X-ray and CT scan; both reveal a small lung nodule. However, due to integration issues between the radiology system and the electronic health record, the report does not get "filed" into the patient's chart. She is finally diagnosed with advanced untreatable lung cancer 1 year later. The radiologist who interpreted the initial studies said he tried to call the ordering physician but the contact information in the system was not up-to-date and therefore he couldn't reach the referring physician.

*****

During a busy holiday weekend, with several physicians covering on a medical floor, a patient with low potassium was given potassium both intravenously (IV) and orally (PO) resulting in an overdose. The patient suffered cardiac arrhythmia and expired. The analysis identified that IV and PO orders are available on separate ordering screens, neither of which displays the total potassium dose being administered. Despite months of negotiations, the software vendor hasn't been able to fix the system. In the absence of a technology fix, training has been instituted to alert users to double-check both the IV and PO orders and add up the total dose themselves. This adds to yet another source of frustration and time-crunch for medical staff and residents.

Introduction

Growing concerns about the cost, efficiency, and safety of our health care system [1, 2] have turned national attention on health care information technologies (HIT) such as electronic health records (EHRs) as important foundational solutions to enable the transformation of health care delivery [3]. Over the last several years, a number of countries have made multibillion dollar investments in EHRs to improve quality, safety and efficiency and reduce costs. In the USA, the 2009 American Recovery and Reinvestment bill (ARRA), popularly known as the "stimulus plan" provided for approximately $36 billion in incentive payments to hospitals and office practices for demonstrating "meaningful use" of certified EHRs [4].

As a result, there has been an accelerated adoption of EHRs around the world. In the USA, over 90 % of office practices and hospitals currently use certified EHRs [5]. As of August 2015, almost 545,000 physician practices and hospitals have received approximately $31 billion in incentive payments [6]. In the UK, Australia, the Netherlands, and Germany, close to 90 % of physician practices are reported using EHR technology [7]. As the eminent researcher and policy expert, David Blumenthal, noted, "Information is the lifeblood of modern medicine. Health information technology (HIT) is destined to be its circulatory system [4]."

The EHR can play a transformative role in health care by improving medication safety, making patient health information available at the point of care, facilitating care coordination, optimizing efficiency, and engaging patients and caregivers. A review of the recent literature concluded that 92 % of the published articles on HIT demonstrated net benefit in improving quality and outcomes [8]. HIT demonstrated positive results for efficiency of care, effectiveness of care, patient and provider satisfaction, care process, preventive care, and access to care.

Unintended Consequences and Safety Risks of Health Information Technology

As Everett Rogers might have predicted, this transformative technology also has unintended consequences:

> *No innovation comes without strings attached. The more technologically advanced an innovation, the more likely its introduction will produce many consequences, both anticipated and latent* [9].

In fact, a growing number of research and review articles are raising concerns that poor implementation, workflow integration or design of EHR systems can paradoxically facilitate medication errors [10], increase mortality [11], lead to physician dissatisfaction [12], and adversely impact physician–patient relationship [13]. A number of news stories in print and online media have also reported incidents of HIT leading to serious injuries and death [14].

In 2007, noted informatics researcher Weiner coined the term "e-iatrogenesis" to denote patient harm resulting at least in part from HIT [15]. In his 2010 testimony to Institute of Medicine Committee on Patient Safety and Health Information Technology Public Meeting, Jeffrey Shuren, the Director of Food and Drug Administration (FDA)'s Center for Devices and Radiological Health noted, *"In the past 2 years, we have received 260 reports of HIT-related malfunctions with the potential for patient harm—including 44 reported injuries and 6 reported deaths. Because these reports are purely voluntary, they may represent only the tip of the iceberg in terms of the HIT-related problems that exist."* [16] Further, the ECRI Institute, a widely recognized nonprofit organization has been listing various HIT products among their top 10 technology hazards annually since 2011 [17].

Recognizing the mounting risks of HIT and EHR systems, in 2008, The Joint Commission released a sentinel events alert #42 titled "Safely Implementing Health Information and Converging Technologies" focusing on technology-related adverse events and encouraging health care providers to be alert to the associated safety risks [18]. Of note, a new sentinel events alert #54 was issued in March 2015 which yet again highlights that the HIT-associated risks require our ongoing attention for ensuring patient safety [19].

Besides potential direct safety risks to patients, a number of reports are citing EHRs as contributing to the growing problem of professional dissatisfaction and burnout among physicians. In a joint 2013 report by the American Medical Association and RAND Corporation [12], physicians approved of EHRs in concept and appreciated having better ability to remotely access patient information and improvements in quality of care. However, for many physicians, the current state of EHR technology significantly worsened professional satisfaction in multiple ways. Aspects of current EHRs that were particularly common sources of dissatisfaction included poor usability, time-consuming data entry, interference with face-to-face patient care, inefficient and less fulfilling work content, inability to exchange health information, and degradation of clinical documentation. In a more recent 2015 Medscape Physician Lifestyle report, 46 % of all physicians said that they are burned out [20]. The "increased computerization of the practice" was cited as the fourth most significant contributor to physician burnout in the 2015 report, moving up from the ninth place in the 2013 study. Seventy percent of physicians said that EHR technology decreased their face-to-face time with patients, and 57 % noted that it detracted from their ability to see patients. Furthermore, according to a 2014 Physicians Foundation survey, although 85 % of physicians have now implemented an EHR, only 32 % say the technology has improved the practice, and 46 % say the software has detracted from efficiency [21]. It is not only the physicians; patients are also reporting the negative consequences of the intrusion of the computer and EHRs in the exam rooms on physician–patient relationship. In a 2012 article in the Journal of the American Medical Association titled, "Cost of Technology," the physician author shared a story and a drawing by his 7-year-old patient depicting her view of the exam room. The artist, the young patient, is sitting on the exam table with her family around her. The doctor is sitting staring at the computer, his back to the patient—and everyone else [22].

In addition to the unintended consequences in regards to safety risks, questions are also being raised about the promised value of HIT in curbing the cost of health care. A 2005 report by RAND Corporation had projected that the rapid adoption of HIT could save the US health care system $81 billion annually [23]. However, a new analysis 7 years later demonstrated that the conversion to EHRs has failed so far to produce the hoped-for savings in health care costs and has had mixed results, at best, in improving efficiency and patient care. The study found that the results are primarily attributable to the lack of integration between various systems and the poor usability of EHRs [24].

Because of the central role of HIT in the reengineering of the health care delivery system and because so many hospitals and physician offices are rapidly adopting EHRs, it is essential and urgent that we understand HIT's unintended and adverse consequences and their root causes, and implement risk mitigation strategies to ensure that this largely beneficial technology can continue to improve the health of our patients.

The Sociotechnical Context of Health Information Technology

The foundational insight from recent literature is that the EHR is not a technology but rather a system that operates in a larger sociotechnical context [25]. Therefore, the benefits and risks are dependent not only on the software but on the other elements of the sociotechnical system such as clinical workflow and processes, users, hardware, and organizational policies. We can apply the model of sharp-end errors and latent errors to HIT as well [26]. For HIT-related events, let us consider EHR to be at the sharp end of the error; for HIT-related safety risks to take place, there are a host of "latent" sociotechnical factors that are aligned in a Swiss Cheese model [27] to cause an adverse event. We must address the entire system for us to mitigate HIT-related safety risks and to realize the promised benefits of HIT.

Additionally, how users interact with the technology and the usability of the technology itself is a major determinant of the willingness/satisfaction of the users of technology as well as the outcomes. The diametrically opposite worlds of technology and humanity come together every day in countless hospitals and practices: technology—rigid, certain, inflexible, preprogrammed, without emotions or fatigue, oblivious to environment; humanity—emotional, variable, compassionate, subjected to conditions around us. In the words of the New York Times columnist, David Brooks, this is "the bloody cross-roads where technology meets humanity" [28]. This bloody cross-roads is where patients get harmed. The safety of our patients depends on how well we manage this cross-roads and what kind of traffic signals we put there. Unfortunately, much of the current design, development and implementation of HIT have taken place with little regard to these complex human factors.

It is also important to understand that the safety risks posed by HIT are unique as compared to the other types of errors in health care. First, they are opaque to users; it can be very challenging to understand how a particular failure occurred and could potentially be forestalled. Second, HIT systems tend to have a "magnifying" property, wherein, one exchanges a large number of small failures in a paper-based system for a small number of large, potentially catastrophic failures in an electronic system. For example, in a non-electronic system, one pharmacist can make a single transcription error that affects one patient, where a medication dispensing robot with a software glitch can produce hundreds of errors in an hour. Moreover, as different HIT systems get coupled (e.g., when a CPOE system is directly linked to a pharmacy information system and an electronic medication administration record), errors early in the medication process can quickly pass unscrutinized to the patient. Hence, for HIT implementations to be successful, it is essential that we understand not only the technology but also the workflow and the health care workers.

Another important consideration is that currently there is a lack of clarity regarding shared accountability between the vendors (developers of HIT) and users (hospitals, physicians, other clinicians etc.). The users are quick to blame EHRs for inefficient practices and workflows that existed long before the introduction of EHRs. The vendors are reticent to take responsibility for the product due to contractual languages and fear of bad press and litigation; they often point the blame at how

EHRs are implemented or customized by the user or integrated into workflow. To improve safety of EHRs, we need to ensure that there is shared responsibility and transparency in accountability between the developers, implementers and uses of EHRs [29].

Why This Book?

Even though there is incontrovertible evidence of unintended consequences of HIT, many HIT vendors, hospital leaders and IT departments underestimate the potential safety risks of HIT. Worse, when clinicians bring them to the attention of IT department or administrators, they are often disparagingly labeled as "neo-Luddites" or "not with the program" and are admonished to "try harder."

Much of the conversation around unintended consequences of HIT and the need to ensure its safety has been taking place in academic, policy or technology circles. In spite of emerging literature, most front-line clinicians remain unaware of these risks and specific strategies to ensure patient safety in the world of technology-enabled health care. Since the realm of HIT has moved from the world of technology to the world of clinicians, this book is written from the clinical viewpoint. Through the lens of a variety of case studies, this reference book illustrates that HIT/EHR usage is not without risks and provides practical clinically acceptable risk mitigation strategies. The book aims to take the discourse about HIT and patient safety from the policy/research or technology-centric discussion to patient-centric discussion. The unique strength of the book is that these are clinical case scenarios of post-implementation HIT-in-use (in vivo) from the field as opposed to hypothetical "use cases" designed by the developers of systems in early stages of technology development (in vitro).

One of the key recommendations in the Institute of Medicine's landmark report titled *Health IT and Patient Safety: Building Safer Systems for Better Care* is that mechanisms for reporting HIT deaths, serious injuries or unsafe conditions must be established and efforts should be developed to remove barriers to reporting [14]. It is widely acknowledged that adverse event reporting for all patient safety concerns (not just HIT-related) is critical to promoting safer systems. Still studies find that the reporting of events remains low [30]. This is even more applicable to HIT-related events due to a lack of regulatory requirements and reporting mechanisms for such events. By increasing awareness through case studies, and by fostering a dialog among users, this book should facilitate reporting of HIT-related events as reporting mechanisms get clarified.

The book builds the case that these safety risks from HIT are often as a result of usability, work flow integration, information exchange issue and other variables and that it is unproductive to blame the technology itself or the users (mostly clinicians) for those risks or unintended consequences. Since little is available in the literature regarding what actions institutions can take when they encounter HIT-related

adverse events (or adverse events in which HIT plays an important contributory role), the book aims to provide examples of practical solutions that have been used by other organization as risk reduction strategies. A greater understanding of EHR-induced risks and vulnerabilities will help address and mitigate potential safety risks before patient harm occurs. The ultimate goal of the book is to save patients' lives through safer use of health IT.

The Road Ahead

It is worth reiterating that HIT is an essential technology for modern health care; no one can or should argue going back to the world of paper. A recent joint report from the Canadian Patient Safety Institute and Canada Health Infoway "Electronic Health Records and Patient Safety: Future Directions for Canada," expresses this well [31]:

> *"I think if you went back to the early nineteen hundreds and did a controlled clinical trial—or, not clinical but a controlled trial—on the horse versus the car, in the very early days of the car, the horse probably would have won. And if you took a snapshot of those early days and based your future projections on it, you'd say, "Well, let's throw out the car and go with the horse. They're obviously much more reliable." And so on and so forth. But cars got better and people had the vision to realize that and stay with them and improve them to the point where they soon outdistanced the horse."*

The health care reform law of 2010 holds the potential to "bend the cost curve" by implementing innovative programs such as the value-based purchasing, accountable care organizations and patient-centered medical homes. None of these can be accomplished without HIT providing the necessary enabling infrastructure. Given billions of dollars of investments and rapidly accelerating adoption of HIT, there is a tremendous interest among clinicians, policy makers, EHR vendors, researchers, and hospital administrators alike in the evaluation and understanding of its potential benefits and risks. It is my sincere hope and belief that this book will add to the dialog by providing a clinical and patient-centric viewpoint.

References

1. Kohn LT, Corrigan JM, and Donaldson MS Editors. To err is human: building a safer health system (Vol. 6). National Academies Press; Washington, DC. 2000.
2. Smith M, Saunders R, Stuckhardt L, and McGinnis JM Editors. Best care at lower cost: the path to continuously learning health care in America. National Academies Press; Washington, DC. 2013.
3. Committee on Quality of Health Care in America, Institute of Medicine. Crossing the quality chasm: a new health system for the 21st century; 2001.
4. Blumenthal D. Launching HITECH. N Engl J Med. 2010;362(5):382–5.
5. Adoption of Electronic Health Record Systems among U.S. Non-federal Acute Care Hospitals. ONC Data Brief. No. 23. April 2015. Available at https://www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf. Accessed 11 Oct 2015.

6. EHR Incentive program. Aug. 2015 update. Available at https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/August2015_SummaryReport.pdf.
7. Porter M. Adoption of electronic health record in the United States. Kaiser Permanente International. 2013. Available at https://xnet.kp.org/kpinternational/docs/Adoption%20of%20Electronic%20Health%20Records%20in%20the%20United%20States.pdf. Accessed 11 Oct 2015.
8. Buntin M, Burke MF, Hoaglin MC, et al. The benefits of health information technology: a review of the recent literature shows predominantly positive results. Health Aff. 2011;30(3):464–71.
9. Rogers EM. Diffusion of innovations. Simon and Schuster;2003.
10. Koppel R, Metlay JP, Cohen A, et al. Role of computerized physician order entry systems in facilitating medication errors. JAMA. 2005;293(10):1197–203.
11. Han YY, Carcillo JA, Venkataraman ST, et al. Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. Pediatrics. 2005;116(6):1506–12.
12. Friedberg MW, Chen PG, Van Busum KR et al. Factors affecting physician professional satisfaction and their implications for patient care, health systems, and health policy. RAND Corporation; Santa Monica, CA. 2013.
13. Verghese A. Culture Shock — Patient as Icon, Icon as Patient. N Engl J Med. 2008;359(26):2748–51.
14. Health IT and patient safety. Building better systems for safer care. The Institute of Medicine; 2011.
15. Weiner JP, Kfuri T, Chan K, et al. "e-Iatrogenesis": the most critical unintended consequence of CPOE and other HIT. J Am Med Inform Assoc. 2007;14(3):387–8.
16. Health IT Policy Committee. Adoption/Certification Workgroup February 25, 2010. Testimony of Jeffrey Shuren. Available at http://www.cchfreedom.org/files/files/Health%20IT%20Deaths%20-%20FDA%20jeffrey%20Shuren.pdf. Accessed 11 Oct 2015.
17. The ECRI Institute. Available at https://www.ecri.org/Pages/2015-Hazards.aspx. Accessed 20 Sept 2015.
18. Joint Commission Sentinel Events Alert #42. Available at http://www.jointcommission.org/sentinel_event_alert_issue_42_safely_implementing_health_information_and_converging_technologies/. Accessed 20 Sept 2015.
19. Joint Commission Sentinel Events Alert #54. Available at http://www.jointcommission.org/assets/1/18/SEA_54.pdf. Accessed 20 Sept 2015.
20. Burnout and happiness in physicians. Available at http://www.medscape.com/viewarticle/838437. Accessed 21 Sept 2015.
21. Physicians Foundation Survey 2014. http://www.physiciansfoundation.org/uploads/default/2014_Physicians_Foundation_Biennial_Physician_Survey_Report.pdf. Accessed 20 Sept 2015.
22. Toll E. The cost of technology. JAMA. 2012;307(23):2497–8.
23. Bigelow J et al. Analysis of healthcare interventions that change patient trajectories. Santa Monica, CA: RAND Corporation; 2005. http://www.rand.org/pubs/monographs/MG408. Accessed 20 Sept 2015.
24. Kellermann AL, Jones SS. What it will take to achieve the as-yet-unfulfilled promises of health information technology. Health Aff. 2013;32(1):63–8.
25. Sittig DF, Singh H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. Qual Saf Health Care. 2010;19 Suppl 3:i68–74.
26. Reason J. Human error: models and management. BMJ. 2000;320(7237):768–70.
27. Agrawal A, editor. Patient safety: a case-based comprehensive guide. New York, NY: Springer; 2013.
28. Brooks D. Drilling for certainty. New York Times. 27 May 2010.

29. Sittig DF, Singh H. Legal, ethical, and financial dilemmas in electronic health record adoption and use. Pediatrics. 2011;127(4):e1042–7.
30. Department of Health and Human Services. Office of the Inspector General. Hospital incident reporting systems do not capture most patient harm. January 2012.
31. Electronic Health Records and Patient Safety: Future Directions for Canada;2007.

Chapter 2
An Overview of HIT-Related Errors

Farah Magrabi, Mei-sing Ong, and Enrico Coiera

Introduction

Owing to the pervasive use of information technology (IT) in almost every aspect of modern life, computer system failures are an everyday occurrence. They manifest in a myriad of ways from a minor software glitch that freezes a Web browser to a major network outage that shuts down a stock exchange for several hours. Problems with IT also stem from our use of software systems such as making a wrong selection when shopping online or sending an email to the wrong recipient when distracted by another task. The effects of IT failures can vary from being a personal inconvenience to causing widespread disruption of services in banking and telecommunications. In safety-critical industries such as aviation, rail and nuclear power, IT failures also pose risks to humans. Health care is no exception; alongside all its benefits the widespread adoption of IT is coupled with emerging risks to patient safety [1].

In this chapter we focus on failures involving IT systems in health care or health IT (HIT) which is collectively used to describe computer software and hardware systems that support care delivery. The chapter begins by examining how problems with HIT can lead to clinical errors. We then review the current evidence about patient harms associated with such errors. The next section discusses the underlying causes of errors associated with HIT and the final section looks at systems for classification of these errors. By understanding how HIT failures can give rise to clinical errors and having knowledge about their underlying causes, we can be better equipped to design, implement, and use safer systems and to mitigate the risks of harm to patients.

F. Magrabi, B.E., Ph.D. (✉) • M.-s. Ong, B.E., Ph.D.
E. Coiera, M.B.B.S., Ph.D., F.A.C.M.I.
Centre for Health Informatics, Australia Institute of Health Innovation, Faculty of Medicine and Health Sciences, Macquarie University, Sydney, NSW 2109, Australia
e-mail: farah.magrabi@mq.edu.au; mei-sing.ong@mq.edu.au; enrico.coiera@mq.edu.au

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_2

HIT Generates Errors That Can Harm Patients

The accuracy of clinical information is fundamental to the safe delivery of care. We know that errors in clinical information can lead to patient harm. For instance, wrong information about the dose of a prescribed medication can lead to a patient being overdosed. When patient records are maintained electronically, problems with HIT systems can generate errors in clinical data. These errors are caused by HIT systems themselves [2]. Take the case of a prescribing decision support system that fails to display an alert about a potential drug interaction due to a flaw in its drug database and as a result the patient suffers from an allergic reaction. The use of HIT by clinicians also creates opportunities for error [3]. For example, a physician finds the font on the computer screen hard to read and accidentally orders laboratory tests for the wrong patient.

There are four possible ways in which problems with HIT systems themselves or their use can impact clinical data and lead to errors posing risks to patients (Table 2.1). For example, in a medication ordering system, errors would occur when:

1. *Data are wrong*: If a clinician orders the antibiotic *floxacillin* for a patient but the antimetabolite *methotrexate* appears in the pharmacy system, then an error has occurred somewhere in the process between clinical order and pharmacy receipt of the order.

Table 2.1 HIT errors can lead to adverse events and patient harm

Data are wrong
• A primary care physician mistakenly selected methadone concentrate 10 mg/ml, the first option in an alphabetically arranged list, instead of 1 mg/ml. The patient was admitted to an emergency department with respiratory arrest but made a full recovery
• A patient who was seen with another patient's records in primary care was prescribed that patient's medication and died later the same day from taking it
Data are missing
• A full-body X-ray was repeated exposing a child to high levels of radiation because images randomly went missing when they were digitized for entry into the PACS system
• A hospitalized patient did not receive her insulin for 2 days because the medication was mistakenly omitted from the list sent by her primary care clinic
Data are partial
• Patients received medications at the wrong frequency when orders communicated to the pharmacy system arrived without the time of administration
• The time and date of images was not displayed by a Picture Archiving and Communication System (PACS) leading to an incorrect diagnosis
Data are delayed
• Surgery was canceled and an anesthetized patient had to be woken up due to a network problem with a PACS system that delayed retrieval of images from a long-term storage facility
• Prescription orders that did not appear in the physicians work folder led to a 3-day delay in the administration of medications leading to an ulcer requiring an emergency procedure

2. *Data are missing*: If a patient's medication record does not display that the patient has a penicillin allergy, which has been documented, then this missing information error creates a hazard that may lead to harm.
3. *Data are partial*: If a patient's discharge medication list includes a medication's name but not its dose, this creates a hazardous situation in which another physician may reorder the medication at the wrong dose.
4. *Data are delayed*: Should a hospital physician order a new medication urgently, but the medication fails to immediately appear on the patient's medication list, it may not be dispensed and given to the patient in a timely fashion.

Errors associated with HIT or *HIT errors* are recognized as an unintended consequence of using technology to support care delivery [3]. The impact of such errors on patient safety can be understood by examining HIT in context of the wider *sociotechnical system* that includes technology, people, processes, organization and the external environment [4]. As in other domains of patient safety, HIT errors interact with other contributing factors to produce an adverse event [5]. For instance, problems with the usability of an order entry system are exacerbated by a physician's lack of familiarity with the system and lead to a patient being overdosed. By the same token, defenses in the wider sociotechnical system help to mitigate the effects of HIT errors. For example, many prescribing errors are detected when medication orders entered by physicians are checked by the pharmacy prior to dispensing medications. Thus the vast majority of HIT errors are detected by the wider system in which systems operate and do not lead to patient harm. The term *e-iatrogenesis* is also used to describe adverse events and patient harm associated with HIT [6].

In addition to adverse events, HIT errors have also been shown to impact care delivery by causing delays [7]. For instance, treatment for several patients including a major trauma is delayed because in a computerized system admissions cannot be processed, tests cannot be ordered and results cannot be accessed in an emergency department unless the patient is first registered in the system. In another situation, the follow-up of abnormal test results is delayed due to a power failure of the laboratory information system. Such treatment delays can increase risks to patients. Rework is another consequence of HIT errors [7]. For example, a physician needs to reorder laboratory tests that were lost from the system during a computer downtime. Task duplication has the potential to create new opportunities for error.

Evidence About Patient Harms Associated with HIT Is Mounting

The extent of patient harm associated with the uptake of HIT is hard to quantify, due to the lack of empirical data [1]. The "hold harmless" clauses that protect software vendors from lawsuits effectively limit the freedom to publicly raise questions about software errors [8]. Thus, many problems related to HIT remain hidden, and unresolved. Based on error rates in other industries, a recent report to the Agency for Healthcare Research and Quality estimated that if electronic health records (EHRs) are fully adopted, they could be linked to at least 60,000 adverse events a year [9].

Table 2.2 FDA, Obama digital medical records team at odds over safety oversight. Huffington Post, April 8, 2010

Computers at a major Midwest hospital chain went awry on June 29, posting some doctors' orders to the wrong medical charts in a few cases and possibly putting patients in harm's way.
The digital records system "would switch to another patient record without the user directing it to do so," said Stephen Shivinsky, vice-president for corporate communications at Trinity Health System. Trinity operates 46 hospitals, most in Michigan, Iowa, and Ohio.
Less than 2 weeks later, an unrelated glitch caused Trinity to shut down its $400 million system for 4 h at 10 hospitals in the network because electronic pharmacy orders weren't being delivered to nurses for dispensing to patients.

While we cannot ascertain the actual rate of adverse events associated with HIT, a growing body of evidence elucidates the pervasiveness of HIT-related problems (Table 2.2). The largest source of evidence came from incident reports voluntarily submitted by software vendors and clinicians to governing bodies, both at the national and local levels [7, 10–12]. The FDA maintains a medical device incident reporting system, known as the Manufacturer and User Facility Device Experience (MAUDE) database. In 2010, 260 HIT-related incident reports were submitted to the database, 44 of which were linked to patient injuries, and 6 deaths were reported [10]. The Australian Incident Management System (AIMS) is yet another initiative in the surveillance of patient safety issues. Between 2003 and 2005, 99 HIT-related incidents were submitted to AIMS [7]. While no deaths were reported, 38 % of the incidents were associated with adverse consequences caused by delay in treatment and care. Since neither system was designed specifically for the surveillance of HIT-related adverse events, it is very likely that HIT-related incidents were under-reported.

At the local level, the Pennsylvania Patient Safety Authority received 3099 reports from Pennsylvania hospitals on EHR-related problems, between the years 2004 and 2012 [13]. More than 2700 incidents were near miss events and 15 involved harm to patients. The report showed a stark rise in the number of HIT-related incidents over the years. Of the 3099 incidents reported over an 8-year period, 1142 were filed in 2011, more than double the number in 2010. With the increased adoption of HIT incentivized by the 2009 HITECH Act in the USA, the problem will only worsen [14].

Flaws in software design and system glitches accounted for many of the reported incidents [10]. For example, poorly designed user interface obscured clinical data, causing clinicians to prescribe the wrong medications, and to send the wrong patients for a procedure; computer-network delays resulted in delay in treatment; dangerous doses of medications were given to patients due to ambiguous drop-down menus; orientation markers on CT images were reversed, causing a surgeon to operate on the wrong side of patient's head. These seemingly simple errors, when occurred in a health care setting, could potentially cascade into serious life-threatening events (Table 2.3).

The transition between paper-based and EHR records represents a risky period, as physicians often use both systems in tandem [13]. At Children's Hospital of

Table 2.3 Baby's death spotlights safety risks linked to computerized systems. Chicago Tribune, June 27, 2011

The medical error that killed Genesis Burkett began with the kind of mistake people often make when filling out electronic forms: a pharmacy technician unwittingly typed the wrong information into a field on a screen.
Because of the mix-up, an automated machine at Advocate Lutheran General Hospital prepared an intravenous solution containing a massive overdose of sodium chloride—more than 60 times the amount ordered by a physician.
When the nutritional fluids were administered to Genesis, a tiny baby born 16 weeks prematurely, the infant's heart stopped, and he died, leaving behind parents stunned by grief.

Pittsburgh, EHR implementation was found to be associated with an increased risk of mortality [15]. The mortality rate increased to 6.6 % in the 5 months after the system was installed, from 2.8 % in the 13 months before. A separate study on CPOE system showed that the rate of computer-related pediatric errors was 10 errors per 1000 patient-days, and the rate of serious computer-related pediatric errors was 3.6 errors per 1000 patient-days [16].

The incidence of medication errors associated with technology has been explored in several other studies [17–21]. A report on 4416 medication incidents submitted to the Dutch central medication incidents registration showed that 16 % of incidents were linked to HIT [18]. Incorrect selection of medication is the leading cause of medication errors, followed by failure to enter prescription data in the CPOE. Two patients died as a result, and 20 patients were seriously harmed. Similar types of errors were observed in an observational study in an Australian hospital [21]. Of the 1164 prescribing errors observed, 43.4 % were caused by selection errors, 32 % were due to failure to complete prescription task, and 21.1 % were a result of editing errors.

Another unintended consequence arising from the digitalization of the medical records is the risk of data breach (Table 2.4). The number of medical data breaches has increased dramatically in recent years. According to the US Department of Health and Human Services (HHS), in 2012, about 125 large breaches affected about 2.2 million people [22]. In the same year, a biannual survey of 250 health care organizations showed that 27 % of the respondents had at least one security breach over the past year, compared to 19 % in 2010 and 13 % in 2008 [23]. The rise in data breach incidents was largely due to the proliferation of laptops and mobile devices. The number of cases where data were compromised as a result of a lost or stolen device had doubled. Concerns about data security has prompted the HHS to update the Health Insurance Portability and Accountability Act (HIPAA) in 2013, to expand security protections requirements of health care providers that contract or subcontract with business associates to handle medical information [24]. Providers can be penalized up to $1.5 million if business associates do not comply.

Cyber-security is also a growing concern. In June 2013, the FDA issued a safety communication, warning medical device manufacturers and hospitals of the risk of cyber-security [25]. While the actual number of incidents is difficult to assess, news reports on cyber-attacks continue to proliferate. In a recent case, research computers at Kaiser Permanente (KP) were infected with malicious software for more than two

Table 2.4 Data breach results in $4.8 million HIPAA settlements US Department of Health and Human Services

Two health care organizations have agreed to settle charges that they potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to secure thousands of patients' electronic protected health information (ePHI) held on their network. The monetary payments of $4,800,000 include the largest HIPAA settlement to date.
The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) initiated its investigation of New York Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated September 27, 2010, regarding the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results.
The investigation revealed that the breach was caused when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI. Because of a lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines. The entities learned of the breach after receiving a complaint by an individual who found the ePHI of the individual's deceased partner, a former patient of NYP, on the internet.

and a half years before being discovered, affecting in excess of 5000 patients [26]. In another high profile case, the infamous hacker group, Anonymous, allegedly launched a cyber-attack against Boston Children's Hospital [27]. Such events can bring down HIT systems, causing disruptions in care delivery. With increased interconnectedness of health care information systems, the potential for large-scale failure as a result of cyber-attack is real.

HIT Errors Are Linked to System Design, Implementation and Use

Processes undertaken to design, build, implement and use HIT provide the fundamental system safety against errors [28]. As we have seen in the previous sections, patients are harmed when systems fail or when they behave in unexpected ways. For example, a decision support system that fails to provide an alert or provides an alert for the wrong patient may lead to an adverse drug event. HIT may behave in unexpected ways when the *system design does not reflect how it will be used.* When designers have a poor understanding of clinical work they will often make wrong assumptions about how a system will be used, the tasks it must support and the clinical workflow in which those tasks need to be executed. As a consequence the designed system will result in clinical tasks being missed or executed incorrectly.

Incomplete or wrong assumptions about the clinical tasks that a system must support are one of the most important sources of error. For instance, an order entry system that does not support discontinuation and modification of orders is likely to cause medication errors. Errors are also generated when there is a mismatch of the system with the mental model of users. An example is an EHR that does not represent weight in the unit of measure used by clinicians, e.g., displaying weight in pounds instead of kilograms.

Safe use is also influenced by the system user interface. *Inadequate or poorly designed user interfaces* increase cognitive load causing clinicians to make errors in using systems (use errors) [29]. HIT use is hampered by poor usability when systems are hard to learn, and do not allow users to complete tasks in an efficient manner. Ease of use is also affected when users cannot easily reestablish proficiency after a period of not using the system. An interface that results in severe use errors can be hazardous to patients. Consider the case of a prescribing system that requires users to scroll through a drop down menu with an excessive number of options that are counter-intuitively arranged. As a result of using this system a patient may receive an excessive dose of a medication. Risks to patients are also increased when systems do not facilitate recovery from use errors. For example, an order entry system that does not allow clinicians to modify or cancel an order for a chemotherapy protocol once it is entered into the system.

Another design related issue is a *mismatch between the system model and actual clinical workflow* which can lead to errors in task execution [30, 31]. For instance, a nurse cannot review medication lists at the time of administration because the system is not accessible at the patient's bedside. Errors are also generated when system functions and the display of information do not account for the sequence in which clinical tasks are carried out. For example, prescribing decision support is ineffective in an order entry system that does not require users to complete allergy information before medications are entered because allergies cannot be checked if that information is not known by the system prior to the entry of orders. Another example is an order entry system that does not separate preoperative and postoperative orders resulting in a wrong procedure being undertaken based on a preoperative order.

Software defects introduced during development also cause HIT to behave in unexpected ways. Such defects will remain if software is not adequately tested. For instance, an EHR system that allocates test results to the wrong patient due to a programming flaw that is exposed when the system processes large volumes of test results.

Beyond system design, HIT safety is influenced by sociotechnical variables of the clinical setting in which systems are used [4]. For instance installation of an order entry system in a hospital with a poor safety culture or an inadequate IT network might lead to new errors. Introduction of new technology into an organization or *system implementation* may involve a changeover from a paper-based to an electronic system or from an existing electronic system to a new one. This period is characterized by a high degree of sociotechnical change which can pose safety risks when the transition to new technology, changes to clinical workflows and, organizational policies and procedures are not effectively managed (Table 2.5) [32]. Creation of a hybrid paper and electronic records system due to partial system implementation has also been shown to create new opportunities for error [33]. Any changes to an HIT system post-implementation such as updates to software or installation of new hardware can similarly be a threat.

Errors can arise from unexpected interactions between system modules or with other systems [7]. HIT systems are usually composed of multiple modules and they seldom operate in isolation. For instance, an ambulatory care system will contain

Table 2.5 Case study—Implementation of an order entry system at two pediatric hospitals

Two US hospitals, one in Pittsburgh and the other in Seattle, implemented the same EHR and order entry system in their pediatric intensive care units (ICUs) [15, 34]. At 5-months after implementation the mortality rate in the Pittsburgh hospital increased from 2.8 to 6.6%. In contrast there was no change at the Seattle hospital (13-months post-implementation, nonsignificant decrease, 4.2–3.5%). The disparity in patient outcomes reflects the sociotechnical nature of computer systems and was most likely due to differences in adaptation to the local environment.
Speed of implementation: Implementation at the Pittsburgh hospital followed a "big bang" approach occurring hospital wide over a 6-day period not allowing staff enough time to adapt to new routines and responsibilities.
User training: At the Seattle hospital all clinical staff were required to attend role specific training programs for 2–4 h and were supported by a peer group of super users during and after implementation. Users were also provided with 24 h a day support during implementation.
User interface: The system in the Seattle hospital had been locally adapted to reduce the time taken by doctors to enter orders. Specific order sets were created for the ICU, including frequently used orders. No such adaption occurred in Pittsburgh resulting in delays in initiating treatment.
Poor integration with workflow: Unlike the paper-based system the new order entry at the Pittsburgh hospital did not allow entry of orders prior to arrival of critically ill patients, delaying life-saving treatment. Additionally the new workflow around the system caused a breakdown in doctor–nurse communication. In contrast user interface changes facilitated rapid processing of patients who were transported into the Seattle hospital.
Changes in other processes: In parallel with the order entry implementation, the Pittsburgh hospital made changes to policies and procedures for dispensing and administering medications which delayed treatment. For instance all medications including ICU vasoactive drugs were relocated to a central pharmacy.

modules for record keeping, prescribing and ordering tests. The system could also be connected to a medical device such as a spirometer and other systems like a laboratory information system to download test results. Errors can arise from communication failures between system modules and other systems. For example, images from a full body X-ray of a child were lost when they were transferred from the X-ray machine to a PACS. And the X-ray needed to be repeated to acquire the missing images, reexposing the child to high levels of radiation.

The *supporting IT infrastructure* including computer hardware, software, networks, and data storage facilities are critical to safe operation. Analysis of US and Australian data indicates that technical failure is a major contributor to IT incidents [7, 10]. Ninety-six percent of the problems reported to the FDA were associated with technical failure [10]. Problems with the IT infrastructure that hosts software affect safety because poor availability of systems disrupts delivery of care to patients. For example, when their desktop computer or printer fails, a primary care physician cannot access the EHR in their consultation room or provide a prescription to the patient. Another example relates to a network problem in a hospital that caused a PACS to be inaccessible for 6 h making it impossible to read or create records while the system was unavailable. As a result procedures were canceled and clinics were rescheduled. Failure of back up facilities and computer viruses can similarly disrupt care delivery.

Safe HIT use is a product of the system and the environment in which it is used. When system use is compromised by human factors which include environmental influences like the structural, cultural and policy related characteristics of an organization, risks to patients are increased [35].

The *knowledge and skills* of users are fundamental to safe use of HIT. Training programs are thus essential and need to be appropriately tailored to the needs of different clinical seniorities and roles to ensure safe operation of systems. For example, training for a prescribing system that will be used by physicians, pharmacists and nurses will need to be tailored to the needs of each group respectively. Equally when users are unaware of system limitations, errors of omission will be generated [36]. For instance, a clinician may inadvertently prescribe the wrong medication wrongly assuming that the system will alert them about any drug interactions [37, 38]. Errors can also be generated when *cognitive resources* devoted to using a system are inadequate. A clinician's workload plus environmental influences like distractions and interruptions can lead to errors [39]. For example, when interrupted by a phone call a physician writes a prescription for the wrong patient because they returned to the wrong record at the end of the call.

Deficiencies in *organizational policies and procedures* for system use are another threat. As we have already discussed training is critical to safe operation of HIT. However, the lack of a policy or a failure to enforce the requirement to complete training may result in untrained clinicians accessing systems. Thus an organization might create a procedure for new staff to complete mandatory training and then receive access to systems in a timely manner. Policies that govern system access directly impact safety as lack of access to systems or critical information can potentially delay care increasing risks to patients. For example, an attending physician is unable to access critical test results from a previous hospital admission because the results of an HIV test are only visible to the ordering physician due to privacy considerations.

Thus we have seen that the safety of HIT is an emergent property of the broader sociotechnical system. As safety is an emergent system property it needs to be addressed throughout the life cycle of HIT systems including design, build, implementation, and use [40]. All the possible interactions among system components are not predictable at design, especially when HIT systems are used in context of a broader sociotechnical system. In large complex systems, safety problems tend to emerge from unexpected interactions between system components and human users. There is potential for unsafe interactions when HIT systems are integrated with local clinical workflows including other technology and the organizational structure. Therefore safety must also be addressed during and after the implementation of systems.

Classification of HIT Errors

Classification systems have been developed to understand the underlying types of problems with HIT that pose risks to patients. As we saw in a previous section, reports about critical incidents are an important source of information about

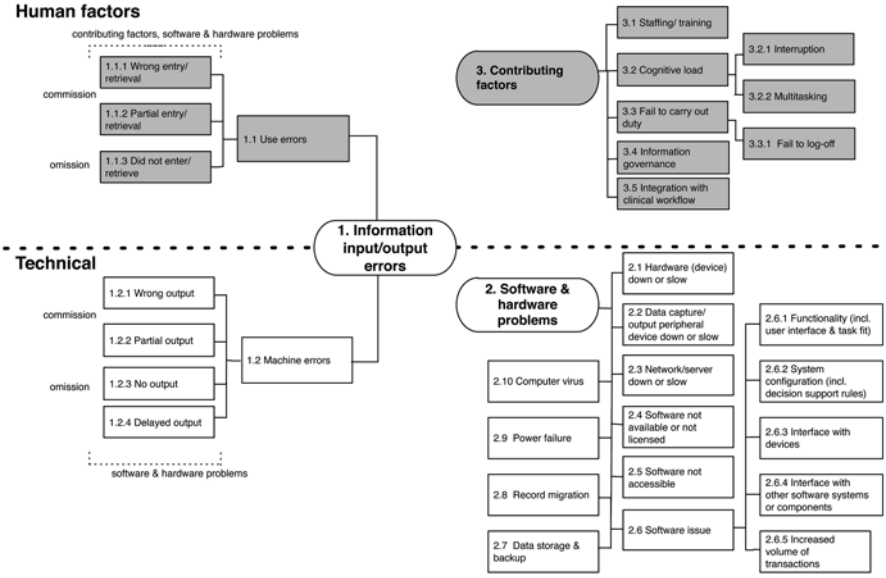


Fig. 2.1 A classification of human and technical problems that contribute to HIT errors. Permission to reprint from ref. [41], granted by Elsevier Limited

problems with HIT. One classification system that has been widely used takes a *bottom-up* approach based on the *natural categories* of problems described in incident reports [7, 10, 41]. In this system incidents are firstly subdivided as primarily relating to human factors or technical issues (Fig. 2.1). For incidents primarily involving human factors, the type of use error and contributing factors such as training, cognitive load and clinical workflow are then identified. For incidents falling into the technical space, the type of machine error and technical problems including a range of hardware and software issues are examined.

Another approach to classification takes a *top-down* approach grouping problems into eight broad dimensions including hardware and software; clinical content; human–computer interaction; people; workflow and communication; organizational policies and procedures; external rules, regulations, and pressures; and system measurement and monitoring (Table 2.6). Problems can also be grouped by the phases of HIT implementation [42]. An initial phase characterized by immature technology where problems primarily relate to technical factors. A second phase in which use errors start to emerge and a final phase where problems primarily relate to the lack of monitoring of safety concerns. Regardless of specific approach classification allows problems with HIT to be collated and classified, providing an objective basis for comparing patterns over time and between settings, and for the development and prioritization of preventive and corrective strategies [43].

Table 2.6 Sociotechnical dimensions associated with HIT errors [4]

Hardware and software: required to run the health care applications
Clinical content: data, information, and knowledge entered, displayed, or transmitted
Human-computer interface: aspects of the system that users can see, touch, or hear
People: the humans involved in the design, development, implementation, and use of HIT
Workflow and communication: the steps needed to ensure that each patient receives the care they need at the time they need it
Organizational policies and procedures: internal culture, structures, policies, and procedures that affect all aspects of HIT management and health care
External rules, regulations, and pressures: external forces that facilitate or place constraints on the design, development, implementation, use, and evaluation of HIT in the clinical setting
System measurement and monitoring: evaluation of system availability, use, effectiveness, and unintended consequences of system use

Conclusion

Minimizing risks to patient safety is critical to realizing the benefits of HIT. The risks of data breach and cyber-crime are also important concerns. We have seen that safety is an emergent property of the broader sociotechnical system in which HIT are used, and errors arise from processes to design, build, implement, and use systems. Thus we need a holistic system approach that addresses HIT errors throughout the system life cycle. Classification of errors is important to understand underlying causes and to facilitate early detection of new problems that pose threats to patient safety.

References

1. Health IT, Safety P. Building safer systems for better care. Washington, DC: The National Academies Press: Institute of Medicine.; 2012.
2. Metzger J, Welebob E, Bates DW, Lipsitz S, Classen DC. Mixed results in the safety performance of computerized physician order entry. Health Aff (Millwood). 2010;29(4):655–63.
3. 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):104–12.
4. Sittig DF, Singh H. Defining health information technology-related errors: new developments since to err is human. Arch Intern Med. 2011;171(14):1281–4.
5. Vincent C, Taylor-Adams S, Chapman EJ, Hewett D, Prior S, Strange P, et al. How to investigate and analyse clinical incidents: clinical risk unit and association of litigation and risk management protocol. BMJ. 2000;320(7237):777–81.
6. 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):387–8.
7. Magrabi F, Ong MS, Runciman W, Coiera E. An analysis of computer-related patient safety incidents to inform the development of a classification. J Am Med Inform Assoc. 2010;17(6):663–70.

8. Koppel R, Kreda D. Health care information technology vendors' "hold harmless" clause: implications for patients and clinicians. JAMA. 2009;301(12):1276–8.
9. Walker JM, Hassol A, Bradshaw B, Rezaee ME. Health IT Hazard Manager Beta-Test: Final Report. (Prepared by Abt Associates and Geisinger Health System, under Contract No. HHSA290200600011i, #14). AHRQ Publication No. 12-0058-EF. Rockville, MD: Agency for Health care Research and Quality;2012.
10. Magrabi F, Ong MS, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. J Am Med Inform Assoc. 2012;19(1):45–53.
11. Myers RB, Jones SL, Sittig DF. Review of reported clinical information system adverse events in US food and drug administration databases. Appl Clin Inform. 2011;2:63–74.
12. Warm D, Edwards P. Classifying health information technology patient safety related incidents - an approach used in Wales. Appl Clin Inform. 2012;3(2):248–57.
13. Sparnon E, Marella WM. The role of the electronic health record in patient safety events. Pa Patient Saf Authority. 2012;9(4):1276–8.
14. Blumenthal D. Launching HITECH. N Engl J Med. 2010;362(5):382–5.
15. Han YY, Carcillo JA, Venkataraman ST, Clark RS, Watson RS, Nguyen TC, et al. Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. Pediatrics. 2005;116(6):1506–12.
16. Walsh KE, Adams WG, Bauchner H, Vinci RJ, Chessare JB, Cooper MR, et al. Medication errors related to computerized order entry for children. Pediatrics. 2006;118(5):1872–9.
17. Ash JS, Sittig DF, Poon EG, Guappone K, Campbell E, Dykstra RH. The extent and importance of unintended consequences related to computerized provider order entry. J Am Med Inform Assoc. 2007;14(4):415–23.
18. Cheung KC, van der Veen W, Bouvy ML, Wensing M, van den Bemt PM, de Smet PA. Classification of medication incidents associated with information technology. J Am Med Inform Assoc. 2013;21(e1):63–70.
19. Koppel R, Metlay JP, Cohen A, Abaluck B, Localio AR, Kimmel SE, et al. Role of computerized physician order entry systems in facilitating medication errors. JAMA. 2005;293(10):1197–203.
20. Littlejohns P, Wyatt JC, Garvican L. Evaluating computerised health information systems: hard lessons still to be learnt. BMJ. 2003;326(7394):860–3.
21. Westbrook JI, Baysari MT, Li L, Burke R, Richardson KL, Day RO. The safety of electronic prescribing: manifestations, mechanisms, and rates of system-related errors associated with two commercial systems in hospitals. J Am Med Inform Assoc. 2013;20(6):1159–67.
22. US Department of Health and Human Services. Breaches Affecting 500 or More Individuals: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html. Accessed 27 Sept 2014.
23. Ponemon Institute LLC. Fourth annual benchmark study on patient privacy & data security, Ponemon Institute Research Report, March 2014.
24. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5566 (25 Jan 2013).
25. US Food and Drug Administration, Cybersecurity for medical devices and hospital networks: FDA safety communication. 2013. http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm. Accessed 27 Sept 2014.
26. Government Health IT. Computer virus at heart of Kaiser data breach. 2014. http://www.govhealthit.com/news/computer-virus-heart-kaiser-data-breach-.U6zuahara38. Accessed 27 Sept 2014.
27. The Boston Globe. Hacker group Anonymous targets Children's Hospital. 2014. http://www.bostonglobe.com/business/2014/04/24/hacker-group-anonymous-targets-children-hospital-over-justina-pelletier-case/jSd3EE5VVHbSGTJdS5YrfM/story.html. Accessed 27 Sept 2014.
28. Walker JM, Carayon P, Leveson N, Paulus RA, Tooker J, Chin H, et al. EHR safety: the way forward to safe and effective systems. J Am Med Inform Assoc. 2008;15(3):272–7.

29. Nielsen J. Usability engineering. San Francisco: Morgan Kaufmann; 1993.
30. Novak LL, Holden RJ, Anders SH, Hong JY, Karsh BT. Using a sociotechnical framework to understand adaptations in health IT implementation. Int J Med Inform. 2013;82(12):e331–44.
31. Debono DS, Greenfield D, Travaglia JF, Long JC, Black D, Johnson J, et al. Nurses' workarounds in acute healthcare settings: a scoping review. BMC Health Serv Res. 2013;13:175.
32. Karsh BT. Beyond usability: designing effective technology implementation systems to promote patient safety. Qual Saf Health Care. 2004;13(5):388–94.
33. Spotlight on Electronic Health Record Errors: Paper or Electronic Hybrid Workflows, Pennsylvania Patient Safety Advisory Vol. 10, No.2 June 2013.
34. Del Beccaro MA, Jeffries HE, Eisenberg MA, Harry ED. Computerized provider order entry implementation: no association with increased mortality rates in an intensive care unit. Pediatrics. 2006;118(1):290–5.
35. Karsh BT, Holden RJ, Alper SJ, Or CK. A human factors engineering paradigm for patient safety: designing to support the performance of the healthcare professional. Qual Saf Health Care. 2006;15 Suppl 1:i59–65.
36. Horsky J, Kuperman GJ, Patel VL. Comprehensive analysis of a medication dosing error related to CPOE. J Am Med Inform Assoc. 2005;12(4):377–82.
37. Goddard K, Roudsari A, Wyatt JC. Automation bias: a systematic review of frequency, effect mediators, and mitigators. J Am Med Inform Assoc. 2012;19(1):121–7.
38. Parasuraman R, Manzey DH. Complacency and bias in human use of automation: an attentional integration. Hum Factors. 2010;52(3):381–410.
39. Li SY, Magrabi F, Coiera E. A systematic review of the psychological literature on interruption and its patient safety implications. J Am Med Inform Assoc. 2012;19(1):6–12.
40. Leveson NG. Engineering a safer world: systems thinking applied to safety. Cambridge, MA: Massachusetts Institute of Technology; 2011.
41. Magrabi F, Baker M, Sinha I, Ong M, Harrison S, Kidd MR, et al. Clinical safety of England's national program for IT: a retrospective analysis of all reported safety events 2005 to 2011. Int J Med Inform. 2015;84(3):198–206. doi:10.1016/j.ijmedinf.2014.12.003.
42. Sittig DF, Singh H. Electronic health records and national patient safety goals. N Engl J Med. 2012;367(19):1854–60.
43. Runciman WB, Williamson JA, Deakin A, Benveniste KA, Bannon K, Hibbert PD. An integrated framework for safety, quality and risk management: an information and incident management system based on a universal patient safety classification. Qual Saf Health Care. 2006;15 Suppl 1:i82–90.

Part I
Errors Related to Various Types of Health Information Technologies

Chapter 3
Errors Related to CPOE

Jan Horsky

Introduction

Information technology permeates most areas of health care work. It supports management of patient records, care documentation, ordering, decision making, viewing and interpreting laboratory and imaging studies, direct care of patients at the bedside and often mediates many aspects of professional collaboration [1]. Routine use may augment human cognition, making large amounts of information amenable to easier recognition of trends or quick identification of abnormalities, for example, but is also known to have unanticipated or negative implications for care [2]. Electronic health records (EHRs) were in part developed to reduce the risk of injury to patients and although their potential to increase the quality and safety of care is well documented, concerns remain about the consequences of poor design and inadequate adaptation to established practices and realities of clinical work [3].

The close and causal relationship between the design of system interfaces, their use in complex work processes and safety has been clearly established [4]. The layout and salience of artifacts on a computer screen such as icons, controls and the appearance of textual information critically affect their perception and interpretation by humans and may lead to cognitively based errors [5]. For example, long, dense pick lists that are poorly organized predispose a clinician to selecting the wrong patient name, medication, order or any adjacent item with similar visual or semantic characteristics [6] and to other juxtaposition problems without realizing that an error has occurred. As large amounts of information are often available for a single patient, effective presentation becomes increasingly dependent on appropriate selection and organization that avoids cognitive overload [7] or bias (e.g., from over alerting) that may lead clinicians to miss critical information in displays saturated with irrelevant or less important content.

J. Horsky, Ph.D. (✉)
Division of General Internal Medicine and Primary Care, Brigham & Women's Hospital, 1620 Tremont St, Boston, MA 02120, USA
e-mail: jhorsky@partners.org

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_3

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 authorized incentive payments to physicians and institutions to migrate their clinical documentation process from paper charts and forms to electronic records systems [8]. The new technology needs to support a specified set of core objectives that demonstrably advance safety, effectiveness, and quality of patient care [9] such as electronic ordering and a comprehensive list of medications, and that provide evidence of safety-enhanced design. This initiative has substantially increased the initially low proportion (18 %) of office-based clinicians using EHRs in 2001 to 78 % in 2013, with about half of all practices reporting that their system meets the required basic standards and functionality [10]. Adoption of electronic records for inpatient care has increased more than fivefold since 2008 so that nine in ten (93 %) hospitals had a certified system in 2013 [11].

The efficacy of EHRs in reducing medical errors was apparent from the beginnings of the technology's routine use in large hospitals [12]. Studies completed over the last 15 years [13–15] have largely substantiated the notion that benefits in safety, quality, organization, and continuity of care are tangible and lasting, provided that systems are sophisticated, well implemented and maintained periodically [16]. Decision support interventions, for example, have positive effect on the performance of providers when they alert about allergy and drug interactions during medication prescribing and remind about preventive care [17] and when they deliver relevant, unambiguous, and actionable advice that is well integrated into patient care [18].

The Institute of Medicine (IOM) estimated in 2000 that health care is a decade or more behind many other high-risk industries in its attention to ensuring basic patient safety [19]. The gap in routine use and sophistication of information systems is closing today but emerging and growing evidence of errors and unintended consequences suggests that the technology is not yet entirely mature in the health care domain [20]. Many errors are the results of failures in human interaction with systems that are deficient in some aspects of design or implementation rather than due to technical malfunctions [21]. Research reports have described problems ranging from extraneous work for clinicians, paper persistence, changes in workflow, unsafe workarounds, inadequate support for clinical reasoning (e.g., presented information failed to reduce uncertainty or increased potential for harm) and "hidden dependencies" in the system [22–24] to medical errors resulting in patient injury [25, 26].

Experts suggest that improving the usability of EHRs may be critical to the continued successful diffusion of the technology [27]. This goal can be advanced in part by establishing and enforcing regulatory and certification standards. The long-term health of the HIT marketplace, however, is necessary to sustain and accelerate the innovation and design quality process. The confluence of initiatives from vendors, providers and other stakeholders should reinforce competitiveness and act to ensure patient safety, interoperability, clinical efficiency, regulatory prudence and cost reductions [28].

Case Study

The following adverse event was reported to the quality assurance committee of a large hospital that had previously implemented electronic ordering in part to minimize the risk of overdose, drug interaction and other medication-related injury to patients [26].

Clinical Summary

An 85-year-old male with coronary artery disease, congestive heart failure (EF 20 %) and mitral valve repair was admitted to a medical intensive care unit with acute-on-chronic renal failure, aspiration pneumonia, and respiratory failure requiring intubation. The patient was transferred 8 days after admission to inpatient pulmonary service with a plan to treat for presumed endocarditis. Routine labs done on Saturday morning indicated hypokalemia (serum K^+ 3.1 mEq/L) and renal insufficiency (Cr 1.7 mg/dL). A house officer (Clinician A) decided to replete potassium and entered an order into the electronic system for 40 mEq KCl, to be delivered over 4 h through an IV route. The patient already had a central line (PICC) inserted for intravenous fluids and, in an effort to minimize further pain, the clinician changed the type of delivery to KCl additive in the running dextrose solution (D5W). The revised order was therefore set for infusing 100 mEq KCl in 1 L of D5W at the rate of 75 mL per hour. The intended prior injection order, however, was not canceled because the clinician inadvertently discontinued a similar KCl order from the previous day instead.

The pharmacy called an hour later to alert that the dose exceeded the 80 mEq KCl maximum allowed by hospital policy and Clinician A changed the order accordingly before the medication was administered. Although the intent was to infuse exactly 1 L of D5W with added 80 mEq of KCl, the system automatically entered a stop time in 7 days, a default period for all fluid drips ordered on hospital floors. The clinician, however, did not change it so that the time interval would correspond to the delivery of 1 L of fluid, the intended KCl dose and rate of 75 mL per hour. The medicated drip therefore continued to be administered as ordered for 36 h before it was stopped, delivering 216 mEq of KCl in 2.7 L of fluid (almost three full bags) in addition to the initial 40 mEq KCl that also ran to completion.

The next day, a covering house officer on a new shift (Clinician B) examined serum potassium value in routine daily labs and concluded that the patient was hypokalemic at 3.1 mEq/L. However, that result was in fact derived from a blood sample taken prior to the last potassium repletion which the clinician misinterpreted as the current value and ordered an injection of 60 mEq KCl without noticing that a medicated drip was still running. The laboratory alerted a covering Clinician C on Monday morning that the patient's serum K^+ level was critically high at 7.8 mEq/L. The medicated drip was then stopped and the patient immediately treated for severe hyperkalemia after having received 316 mEq of KCl over a 42 h period.

Analysis

Two clinicians made three separate errors of commission that interacted in such a way that as they propagated through the system for over 2 days and across three shifts, their effects compounded and culminated in a serious medication overdose. Several opportunities to detect the errors early and to mitigate the severity of potential injury to the patient were missed.

In the chronology of events (Fig. 3.1) Clinician A intended to cancel (discontinue) an IV injection order that had just been entered so that it could be replaced by a medicated drip. The first failure was a misidentification of an entry in the EHR's summary view of active, completed and discontinued orders. Such errors are not uncommon when screens have a high density of content (example in Fig. 3.2) and require extraneous cognitive and visual effort to scan many lines of text, data tables, icons, controls, and graphics to find the information of immediate interest and to interpret it correctly (e.g., *this* is the KCl injection order I recently entered). Long lists or tables consisting of similarly worded entries (e.g., multiple variants of KCl orders) that differ only slightly in details such as date, time or dose, combined with small font size and the need to scroll to see items hidden from view increase considerably the probability of an identification error, especially in the fast-paced and highly interruptive environment of a busy hospital floor. Such errors are also difficult to recognize and correct in real time as the task itself (e.g., discontinuing an

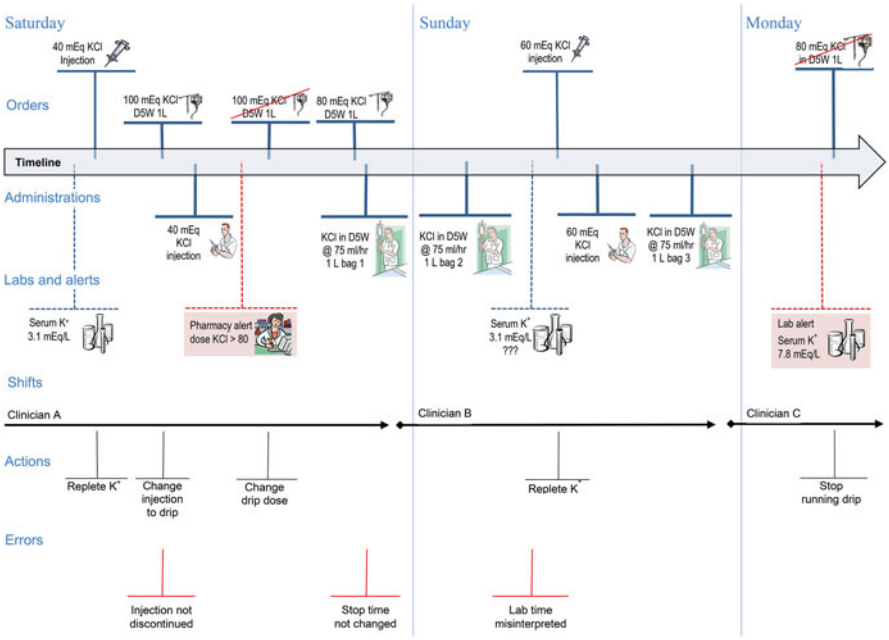


Fig. 3.1 Chronology of orders, actions and errors that produced an adverse event

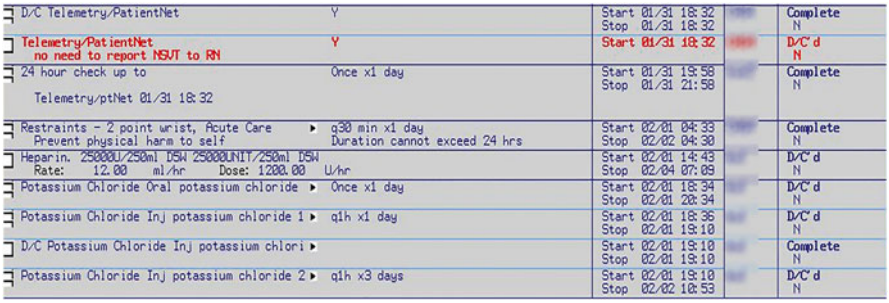


Fig. 3.2 Example of a summary screen showing order history for one patient

injection order) is completed with apparent success, without error messages, warnings, or missing entries that would otherwise signal to the clinician that something is amiss. Visual displays of large amounts of safety-critical information need to be designed in strict compliance with known usability principles grounded in human perception process and cognitive science and informed by research in human–computer interaction to minimize the risk of similar errors.

The second error which precipitated the gradual increase in risk severity and the magnitude of the resulting adverse event was also made by Clinician A during the ordering of a medicated drip. A crucial value for fluid volume on the drip entry form was interpreted differently when it was used for a complex order of fluid with a medication additive than what the designers perhaps intended it to mean in the context of routine maintenance fluid therapy (e.g., the repletion of electrolytes, hydration, etc.) In continuous hydration and parenteral nutrition drips, for example, the crucial values are ingredient concentration (e.g., 5 % dextrose in water solution) and the rate of flow per hour (e.g., 75 mL/h). The duration of therapy and the size (volume) of each bag that is replaced when empty are of secondary importance to the ordering clinician. A medicated drip, however, needs to infuse an exact dose of the drug in a specific concentration and at a set speed of flow. The dose is therefore dependent on both the flow rate and duration—in critical difference from maintenance fluids—as the drug accumulates in the body over time and is metabolized differently than sodium or glucose.

Designers of the ordering module likely assumed that fluids are ordered more frequently than medicated drips and the system was therefore set to automatically calculate a stop time in seven days from initiation (or according to local hospital policy). The value labeled “Total Volume” on the ordering screen (Fig. 3.3) simply means, in the routine scenario, the size of one bag, not the cumulative volume of fluid that would be infused over the active period. However, when an additive is present in the solution, the stop time is one of the criteria determining the dose, along with concentration and rate. In this context, “Total Volume” may be interpreted to mean that no more than that (e.g., 1 L) will be given to the patient, similarly to an intravenous injection for which it substitutes in this case. In fact, this is exactly what the clinician reported as thinking in a subsequent interview after the

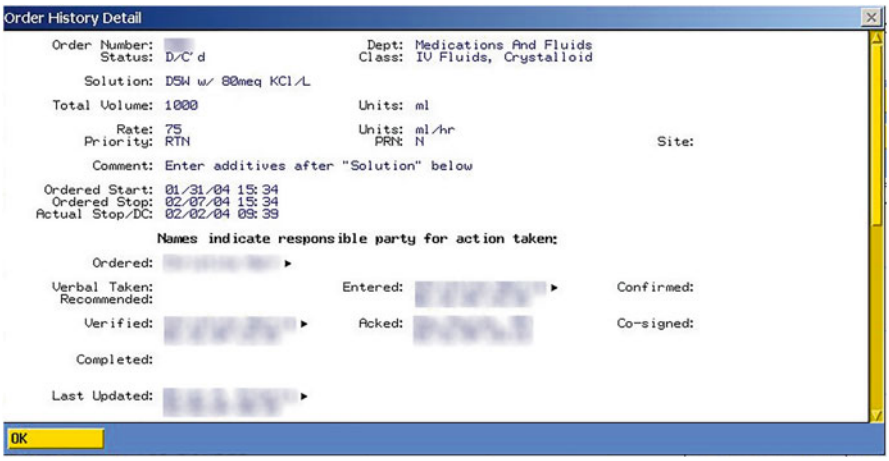


Fig. 3.3 Detail of an order form for a medicated drip indicating an ambiguous term

incident. The exact stop time, however, needs to be calculated: for example, at the rate of 75 mL/h, 1 L of the medicated fluid would take 13.3 h to deliver the dose indicated on the bag. The clinician would also need to decide whether that infusion rate is appropriate for the drug, adjust the flow and recalculate.

Free-text fields are sometimes used for special instructions and clarifications to the nursing staff, as evidenced in many reports, but their effectiveness is sporadic and they are "invisible" to the system for processing. Clinician A wrote in the comment field "For 1 L only" to indicate that subsequent bags should not contain the additive. However, this instruction was either missed or not interpreted correctly. A safer design of the entry form would visually indicate (e.g., by color or an icon) that medication is present in the fluid and that the default stop time needs to be adjusted. Automatic calculation of the dose derived from concentration, flow rate and duration would also be a safer way to indicate the exact drug amount that is scheduled to be infused.

An error unrelated to ordering further aggravated the risk of injury when Clinician B examined routine labs on the following day and misjudged the patient's current level of blood potassium. The misidentification of an existing record of patient care is conceptually similar to the first mistake made by Clinician A. It is unclear whether a new potassium lab from Sunday morning existed and if it did, it likely did not show an abnormal K^+ value as an automated lab alert would have been generated. The clinician considered the last known level of 3.1 mEq/L to be still relevant, as there were no records of recent potassium injections, and therefore ordered appropriate treatment. Medicated fluids were grouped together with crystalloid drips on the EHR's display and their additives, although shown in the summary view, could have been missed if not specifically looked for or may have been scrolled off screen. Entries of laboratory results had visible day and time stamps but their appearance on screen was dense, in a pattern similar to the lists of orders, and therefore carried the same risk of misreading and interpretation error. Safety-critical data whose validity

is dependent on time and events occurring in parallel (e.g., intravenous therapy had already increased the blood potassium level) should be presented in a way that makes the contingency and interrelatedness of data and events apparent. Automated checking for recent labs or duplicate therapy that includes medicated drips at the time of ordering would also reduce the risk of this type of error.

Over the 40-h span in which the events unfolded, several clinicians providing direct care to the patient missed opportunities to recover from errors. Nurses who presumably administered both injections and drips of the same drug, for example, could have questioned the validity of those orders. A 40 mEq/L injection took 4 h to infuse while the IV bag with KCl additive was likely hanged by the bedside during that period on Saturday; the apparent cumulative dose increase could have been noticed and reported. A similar situation occurred again on Sunday with the second injection (60 mEq/L) without anyone noticing a concurrent infusion of the same drug. Clinician A did not inform Clinician B about the patient's initial hypokalemia in the sign out note as it appeared to have been treated and resolved by the time of shift change. The pharmacy correctly identified the 100 mEq/L dose as being higher than allowed by hospital policy and quickly intervened. However, they did not detect the fact that three consecutive bags and two injections—although in safe doses and concentration—were ordered in a relatively short period for the same patient and amounted cumulatively to an overdose.

Solutions

Errors described in this clinical summary occurred as the result of human interaction with an electronic information system that had many design and functional characteristics inconsistent with common usability conventions and principles of cognitive engineering [29]. Clinicians misperceived, failed to notice or made flawed inferences about information presented on the screen. A dense, visually cluttered and poorly organized display layout contributed to the first two errors where similar items such as records of previous intravenous injection orders and multiple lab results were confused. The ambiguity of the term "total volume" was likely a factor in the third error that led to its misinterpretation in an atypical ordering context. Cognitive support was also lacking for making accurate judgment about the temporal sequence and interdependency of clinical events (serum potassium levels contingent on the timing of repletion therapy) and for situational awareness about concurrent drug treatments (medicated drips and injections).

Cognitive errors with the potential to engender adverse events may occur relatively frequently when complex information technology is used routinely in safety-critical work environments. The risk of certain type of error can be effectively reduced by employing safe design practices during software development while others can be addressed during implementation and by monitoring and periodic evaluation of critical processes under normal working conditions. Interventions that can be taken by clinical consumers and those by vendors and developers are outlined in the sections below.

Consumers

Redesign or reorganization of system components that may be required to eliminate more extensive or conceptual flaws can be only undertaken in full by the original development teams [30] but many improvements that can lower the risk of specific errors can be achieved by implementation and local IT teams on site. Certain modifications to screens, system configuration and medical logic algorithms by consumers generally fall within the scope of many licensing and vendor agreements.

A revision of the way active orders for medications and medicated intravenous drips are shown on the screen could make the duplicate drug therapy error described in this case less likely. Both order variants could be aggregated into a single group on the screen for a simpler visual inspection of ongoing interventions. A decision support alert triggered during ordering could also inform clinicians that potassium chloride is being currently delivered via another route, show that the last known serum potassium result was elevated (e.g., greater than 4.0) or that the lab was not done within the previous 12 h or so. "Total Volume," the vendor's label on a drip order form, could be changed by consumers to show a perhaps less ambiguous term for the given context to reduce the likelihood of potential overdose. Such edits are often allowed by vendors in order to incorporate local terms established at different institutions. However, this approach may also introduce further inconsistencies and produce unanticipated effects if done without rigorous analysis of use context and respect to the organizing and thematic structures of the existing terminology. Substantial changes to naming conventions, controlled vocabulary and standardized visual characteristics are often challenging endeavors best undertaken by vendors as a part of planned release cycles.

Activity logs examined during the investigation showed that clinicians made several attempts to enter and discontinue orders in a pattern of trial-and-error behavior that is usually indicative of interaction difficulties even though all involved clinicians completed standard training and have spent at least several months working daily with the EHR. An essential aspect of safe system use is training that extends beyond the usual several hours of practice with routine scenarios and the acquisition of procedural knowledge [31]. Problem-solving exercises framed in realistic clinical scenarios are generally more effective learning approaches. Training cases of moderate difficulty foster conceptual understanding rather than procedural skills and help develop robust mental models of the system. More complex scenarios can be used to practice safe interaction strategies in less familiar or infrequent clinical contexts.

Well-trained and attentive clinicians are still subject to cognitive errors and the effects of fatigue, interruptions, forced workarounds and inconsistent or flawed design. As training alone cannot be completely effective, high-quality design and careful implementation are necessary to create and maintain a safe working environment.

Vendors and Institutional Developers

One of several core design principles is to maintain the consistency of visual appearance and of interactive and automatic behavior of modules, forms and screens in order to avoid any ambiguity about the expected results of human

actions. For example, order forms for continuous fluids that are limited by time could be visibly distinct (e.g., differentiated by background color or by specific layout of entry fields) from drips with specified volume to provide a visual cue to clinicians that they do not dose a medication in the same way. Forms for complicated orders such as medicated drips could also directly calculate the resulting drug dose based on duration and amount per bag so that a potentially unsafe amount is clearly shown.

The chance of misreading or misinterpreting how current a specific test is at any given time can be lowered by calculating and showing the temporal distance of a timestamp from the present. Singular time points often need to be interpreted in terms of elapsed duration for comparison with other contextual data such as the time it takes to metabolize a dose of medication. This cognitive process is prone to mistakes, especially when a day change after midnight complicates the perception of duration (e.g., 11:30 pm Thursday was 2 h ago). Adding elapsed time automatically next to laboratory results and other time-critical values would directly show that the most recent results, for example, may not reflect the current clinical state of the patient. Such interventions would have likely lowered the risk of the type of error made by Clinician B. Changes to the interface and to algorithms calculating dose and frequency would likely reduce the risk of hyperkalemia as a result of events similar to those described in this case and improve the safety of medication ordering in general.

Discussion

Investigation of this overdose error showed that clinicians made correct medical decisions and acted in a timely manner but their judgments were based on erroneous interpretations of information on the screen. Activity logs further suggested that even after a considerable period of routine use, some clinicians were still not proficient in ordering medications with the EHR. Expecting error-free performance at all times is unrealistic in a highly complex, time-constrained environment that characterizes much of clinical care. In a socio-technical view of system performance [32], safety risks often emerge from human activity and interactions with technology, people (clinicians, patients) and processes (e.g., workflows) within the constraints of organizational and regulatory policies [20].

A frequent reaction by safety committees to accidents and near misses is to mandate additional training for selected clinical roles, targeted at the perceived cause. However, this intervention rarely succeeds in isolation or without a comprehensive analysis of how such incidents develop within the socio-technical context of system use. Examining the confluence of factors such as nonintuitive interfaces, laborious processes for routine tasks and a persistent use of workarounds that may sidestep important safety features or the ambiguity of displayed information may lead to more lasting remedies. The notion that inattentive or inadequately trained clinicians are solely responsible for errors should be strongly resisted [33].

An effective response to emergent risks is to develop and implement robust and resilient systems that continuously detect errors, mitigate risk and prevent the deterioration of simple mistakes into safety hazards so that the provision of patient care (or, in other domains, keeping air traffic or energy production in a safe state) is maintained or quickly restored [34]. Achieving this level of safety is predicated on the availability of technology developed according to the best practices of User Centered Design (UCD) and human factors but also, in equal measure, on its careful and methodical implementation [35].

The Office of the National Coordinator for Health IT (ONC) requires developers to employ UCD [36] in order to meet certification criteria for Safety Enhanced Design under the Meaningful Use 2 Act for 2014 [9]. This method, developed by the National Institute for Standards and Technology (NIST), is based on findings derived from decades of usability and safety research in human–computer interaction and emphasizes iterative refinement and testing of design prototypes with clinicians to achieve a high level of usability. Research and trade organizations such as AMIA and HIMSS also provide guidelines and best practices suggestions [35, 37] that vendors can use to evaluate and refine their products. Collectively, these approaches minimize latent safety-critical design errors and help improve usability.

The best opportunity that clinicians have to influence productivity and safety of their EHR is during its implementation. Large institutions and smaller practices alike should follow a rigorous, iterative process such as the Safety Assurance Factors for EHR Resilience (SAFER) that provides tools and a strategy to proactively evaluate potential risks [38]. Clinicians or larger teams can identify specific areas of vulnerability and make appropriate setup adjustments to best mitigate apparent risks and to better align the system to clinical workflows. Although risks emanating from design flaws would be difficult to address effectively at this stage, inadequately performed implementation can further increase the overall possibility that serious errors will develop. Continuous monitoring, nonpunitive error reporting and periodic analyses of incidents and near misses are good sources of insight to inform redesign efforts to be done either on site or reported back to vendors for remedial action.

Excellent usability characteristics are among the key aspects of safe and effective use of EHRs. The acquisition process of new systems and search for a suitable vendor should therefore include usability metrics as a standard part of any Request for Proposal (RFP) document [39]. An institution implementing a newly purchased EHR conducted a usability inspection study at the outset of its use at an oncology service [40]. Clinicians were able to identify over a 100 problems, most recognized as important by an expert panel and recommended for resolution. The expertise of informaticians and usability professionals should always be included in any comparative purchasing analysis preceding the acquisition or modernization of an EHR.

Key Lessons Learned

- Cognitively based errors cannot be avoided but can be reduced and managed so that they do not propagate, combine and escalate in severity to cause patient harm.
- Health information technology does not guarantee the absence of medical errors.
- Electronic records, order entry and decision support technology are socio-technical systems in which humans, computers and processes interact, collectively affecting communication and decision making, sometimes with unintended consequences.
- Errors emerge from the interaction of people and technology—they are rarely attributable only to one or the other. Clinicians should not be held solely responsible for errors.
- Design and implementation of EHRs can have positive and negative effects on safety.
- Safety-critical electronic systems need to be developed according to the principles of User-Centered Design and optimal usability.
- Procurement process for an EHR needs to include criteria describing usability standards.
- Rigorous, evidence-based implementation and continuous monitoring are essential to long-term safe performance.
- Culture of safety encompasses nonpunitive reporting of errors, continuous monitoring for unintended effects and periodic reviews of process and policies.

References

1. Hollnagel E, Woods DD. Joint cognitive systems: foundations of cognitive systems engineering. Boca Raton, FL: CRC Press; 2005. p. 223. xii.
2. Holden RJ. Cognitive performance-altering effects of electronic medical records: an application of the human factors paradigm for patient safety. Cogn Technol Work. 2011;13(1):11–29.
3. Blumenthal D, Glaser J. Information technology comes to medicine. N Engl J Med. 2007;356(24):2527–34.
4. Karsh B-T, Weinger MB, Abbott PA, Wears RL. Health information technology: fallacies and sober realities. J Am Med Inform Assoc. 2010;17(6):617–23.
5. Zhang J, Patel VL, Johnson TR, Shortliffe EH. A cognitive taxonomy of medical errors. J Biomed Inform. 2004;37(3):193–204.
6. The Joint Commission, Institute for Safe Medication Practices. List of confused drug names Horsham, PA: Institute for Safe Medication Practices; 2010. Accessed 28 October 2014. From: http://www.ismp.org/Tools/confuseddrugnames.pdf.
7. Singh H, Spitzmueller C, Petersen NJ, Sawhney MK, Sittig DF. Information overload and missed test results in electronic health record-based settings. JAMA Intern Med. 2013;173(8):702–4.
8. Blumenthal D. Stimulating the adoption of health information technology. N Engl J Med. 2009;360(15):1477–9.

9. Office of the Secretary, Department of Health and Human Services. 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule. Washington, DC: Office of the Federal Register; 2015. p. 62601–759.
10. Hsiao C-J, Hing E. Use and characteristics of electronic health record systems among office-based physician practices: United States, 2001–2012. Hyattsville, MD: National Center for Health Statistics; 2012.
11. Charles D, King J, Patel V, Furukawa MF. Adoption of Electronic Health Record Systems among U.S. Non-federal Acute Care Hospitals: 2008–2012, ONC Data Brief, no 9. Washington, DC: Office of the National Coordinator for Health Information Technology; 2013.
12. Bates DW, Leape LL, Cullen DJ, Laird NM, Petersen LA, Teich JM, et al. Effect of computerized physician order entry and a team intervention on prevention of serious medication errors. J Am Med Assoc. 1998;280(15):1311–6.
13. Chaudhry B, Wang J, Wu S, Maglione M, Mojica W, Roth E, et al. Systematic review: Impact of health information technology on quality, efficiency, and costs of medical care. Ann Intern Med. 2006;144(10):742–52.
14. Garg AX, Adhikari NKJ, McDonald H, Rosas-Arellano MP, Devereaux PJ, Beyene J, et al. Effects of computerized clinical decision support systems on practitioner performance and patient outcomes: a systematic review. J Am Med Assoc. 2005;293(10):1223–38.
15. Bates DW, Gawande AA. Improving safety with information technology. N Engl J Med. 2003;348(25):2526–34.
16. Buntin MB, Burke MF, Hoaglin MC, Blumenthal D. The benefits of health information technology: a review of the recent literature shows predominantly positive results. Health Aff (Millwood). 2011;30(3):464–71.
17. Jaspers MWM, Smeulers M, Vermeulen H, Peute LWP. Effects of clinical decision-support systems on practitioner performance and patient outcomes: a synthesis of high-quality systematic review findings. J Am Med Inform Assoc. 2011;18(3):327–34.
18. Kuperman GJ, Bobb A, Payne TH, Avery AJ, Gandhi TK, Burns G, et al. Medication-related clinical decision support in computerized provider order entry systems: a review. J Am Med Inform Assoc. 2007;14(1):29–40.
19. Institute of Medicine (US) Committee on Quality of Health Care in America, Kohn LT, Corrigan JM, Donaldson MS, editors. To Err is Human: Building a Safer Health System. Washington, DC;2000.
20. Institute of Medicine. Health IT and patient safety: building safer systems for better care. Washington, DC: The National Academies Press; 2011. p. 197.
21. 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):104–12.
22. 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(5):547–56.
23. Meeks DW, Smith MW, Taylor L, Sittig DF, Scott JM, Singh H. An analysis of electronic health record-related patient safety concerns. J Am Med Inform Assoc. 2014;21(6):1053–9.
24. Berger RG, Kichak JP. Computerized physician order entry: helpful or harmful? J Am Med Inform Assoc. 2004;11(2):100–3.
25. Koppel R, Metlay JP, Cohen A, Abaluck B, Localio AR, Kimmel SE, et al. Role of computerized physician order entry systems in facilitating medication errors. JAMA. 2005;293(10):1197–203.
26. Horsky J, Kuperman GJ, Patel VL. Comprehensive analysis of a medication dosing error related to CPOE. J Am Med Inform Assoc. 2005;12(4):377–82.
27. DesRoches CM, Campbell EG, Rao SR, Donelan K, Ferris TG, Jha AK, et al. Electronic health records in ambulatory care: a national survey of physicians. N Engl J Med. 2008;359(1):50–60.

28. Koppel R, Lehmann CU. Implications of an emerging EHR monoculture for hospitals and healthcare systems. J Am Med Inform Assoc. 2014;23:2014. doi:10.1136/amiajnl-2014-003023.
29. Woods DD, Roth EM. Cognitive engineering: human problem solving with tools. Hum Factors. 1988;30(4):415–30.
30. Vicente KJ. Ecological interface design: progress and challenges. Hum Factors. 2002 Spring;44(1):62–78.
31. Kushniruk AW, Myers K, Borycki EM, Kannry J. Exploring the relationship between training and usability: a study of the impact of usability testing on improving training and system deployment. Stud Health Technol Inform. 2009;143:277–83.
32. Sittig DF, Singh H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. Qual Saf Health Care. 2010;19 Suppl 3:i68–74.
33. Horsky J, Schiff GD, Johnston D, Mercincavage L, Bell D, Middleton B. Interface design principles for usable decision support: a targeted review of best practices for clinical prescribing interventions. J Biomed Inform. 2012;45(6):1202–16.
34. World Alliance For Patient Safety Drafting Group, Sherman H, Castro G, Fletcher M, Hatlie M, Hibbert P, et al. Towards an International classification for patient safety: the conceptual framework. Int J Qual Health Care. 2009;21(1):2–8.
35. Middleton B, Bloomrosen M, Dente MA, Hashmat B, Koppel R, Overhage JM, et al. Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from AMIA. J Am Med Inform Assoc. 2013;20(e1):e2–8.
36. Schumacher RM, Lowry SZ. NIST guide to the processes approach for improving the usability of electronic health records. Washington, DC: National Institute of Standards and Technology; 2010. NISTIR 7741.
37. HIMSS Usability Task Force. Defining and testing EMR usability: principles and proposed methods of EMR usability evaluation and rating. Chicago, IL: Healthcare Information and Management Systems Society; 2009.
38. Sittig DF, Ash JS, Singh H. The SAFER guides: empowering organizations to improve the safety and effectiveness of electronic health records. Am J Manag Care. 2014;20(5):418–23.
39. Schumacher RM, Webb JM, Johnson KR. How to select an electronic health record system that healthcare professionals can use. Oakbrook Terrace, IL: User Centric, Inc; 2009.
40. Corrao NJ, Robinson AG, Swiernik MA, Naeim A. Importance of testing for usability when selecting and implementing an electronic health or medical record system. J Oncol Pract. 2010;6(3):120–4.

Chapter 4
Errors Related to Alert Fatigue

Heleen van der Sijs

Introduction

Implementation of a computerized physician order entry (CPOE) system with integrated clinical decision support (CDSS) is considered an important measure to prevent prescribing errors and patient harm. The first studies in the USA showed an 81 % reduction in non-missed dose medication errors and an 86 % reduction in non-intercepted serious medication errors when a CPOE system was utilized [1]. Ten years later a Dutch study confirmed a reduction in medication errors upon implementation of CPOE/CDSS [2]. However, a reduction in preventable adverse events could not be demonstrated. The authors concluded that patient harm could not be prevented because of a lack in the reduction of therapeutic errors like drug–drug interactions, drug–disease interactions, incorrect monotherapy, and duplicate therapy. They attributed the absence of therapeutic error reduction to the fact that the CDSS was originally developed for community pharmacies and general practitioners, where patient monitoring is absent or scarce as compared to the hospital setting. The inappropriateness of the CDSS for hospitals causes an overload of irrelevant alerts and consequently alert fatigue.

Alert fatigue is defined as the mental state that is the result of alerts consuming too much time and mental energy, which can cause relevant alerts to be unjustifiably overridden along with clinically irrelevant ones [3]. This definition encompasses important issues that are sometimes overlooked. It is not only the number of alerts that may cause alert fatigue, but also the time and mental energy required for understanding and handling the alerts. Clear presentation and good usability may attribute to a good effect. Furthermore, overriding per se is not the problem; overriding is required if the alert is incorrect, and may be justified if the benefits outweigh the risks.

H. van der Sijs, Pharm.D., Ph.D. (✉)
Department of Hospital Pharmacy, Erasmus University Medical Centre,
PO Box 2040, Rotterdam 3000 CA, The Netherlands
e-mail: i.vandersijs@erasmusmc.nl

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_4

Fortunately, not all prescribing errors—whether or not due to alert fatigue—result in patient harm. Other health care professionals, like pharmacists and nurses may prevent medication errors by checking or questioning the orders before dispensing or administering the drugs.

In the Netherlands, almost all CPOE systems make use of the Dutch national drug database, G-standard, which is the professional standard and is updated monthly [4]. The G-standard contains safety information on all licensed drugs in the Netherlands with respect to dosing, duplicate orders, drug–drug interactions, allergies, drug–disease interactions, pregnancy, renal function, and pharmacogenetics. Dose limits are present for both hospital and outpatient settings and dose checks can be tailored to the preferred context. A national working group of professionals decides whether interactions mentioned in the literature require action. A significant number is classified as "no action required" and does not result in an alert in the CPOE. However, alert fatigue is still present as demonstrated by the following cases.

Case Study 1: International Normalized Ratio (INR) Overshoot

Clinical Summary

A 3-year-old girl weighing 14 kg was admitted to hospital for a total cavopulmonary shunt, creating Fontan circulation. On day 3 postoperatively, acenocoumarol was started with the target INR of 2.5–3.5. The orders were entered in the patient data management system in the intensive care unit (ICU), which lacks CDSS. On day 5, the patient was transferred from the ICU to a medium care pediatric ward (MC). The resident entered all the drugs in the CPOE/CDSS that is used for all MC inpatients as well as for outpatients. The resident overrode the drug safety alert that was generated for the combination co-trimoxazole – acenocoumarol. On day 6, the INR result was >6.3 which was thought to be an erroneous value, but the same result was measured with a new sample 2 h later.

The hospital pharmacist checking overridden drug–drug interaction (DDI) alerts called the resident to choose an alternative antibiotic because of the serious risk of INR overshoot. The resident could not tell the indication for the prophylactic co-trimoxazole dose (18 mg/kg once daily). On day 18 the hospital pharmacy called again, asking why the co-trimoxazole had not been stopped. The INR had not been within therapeutic range since the start of the anticoagulant therapy (now 15 days). Another resident now caring for the patient said the co-trimoxazole was very relevant and they would monitor the INR intensively (every 3 days). On day 20, the supervising pediatrician asked the hospital pharmacist if an explanation could be given for the long period the INR was outside the preferred range of 2.5–3.5. The pharmacy again explained the mechanism of the DDI and the need for stopping the co-trimoxazole, which he had discussed with the other caregivers. On day 26

postoperatively, the INR was within limits for the first time since start of the anticoagulant therapy, 23 days earlier. The patient was discharged 3 days later with acenocoumarol as well as co-trimoxazole. Anticoagulant doses are not prescribed "according to scheme" in the Children's hospital, but with the calculated doses based on INR. During admission, 12 DDI-alerts for the combination acenocoumarol – co-trimoxazole were overridden. Fortunately, bleeding remained absent and vitamin K as an antidote was not required. However, frequent blood drawings were necessary in this child which probably could have been prevented if trimethoprim alone or another antibiotic had been chosen for prophylaxis.

Analysis

What Happened?

Co-trimoxazole (trimethoprim/sulfamethoxazole) is a strong inhibitor of CYP2C9, the main liver enzyme involved in the metabolism of the vitamin K antagonists warfarin, acenocoumarol, and probably phenprocoumon, resulting in an increased anticoagulant effect. The combination of co-trimoxazole with a vitamin K antagonist results in severe anticoagulation due to decreased coumarin metabolism and the same is true for systemic as well as cutaneous and vaginal therapy with miconazole [5, 6]. The alert text of this DDI recommends to avoid the combination and choose an alternative antibiotic, which is possible for all indications but *Pneumocystis carinii*. This DDI alert had been overridden 12 times over a 23-day period.

Why Did It Happen?

Lack of Knowledge

All vitamin K antagonists are involved in many drug–drug interactions (DDIs) with serotonin reuptake inhibitors, nonsteroidal anti-inflammatory drugs and antibiotics used for febrile illness. In the Netherlands, all systemic antibiotics result in a DDI alert when prescribed in a patient using vitamin K antagonists. However, it is not clear whether overanticoagulation in patients using antibiotics is the result of fever or the antibiotic itself [7]. The alert text explains that coagulation time increases and is probably due to increased metabolism of coagulation factors during fever and it recommends to monitor INR.

Physicians generally know that the INR should be checked on a regular basis for patients on anticoagulants, that these drugs are involved in many DDIs, and that more frequent INR monitoring is required in case of DDIs [8]. The fact that the mechanism for the DDI is different for co-trimoxazole as compared to other antibiotics appeared to be unknown.

The effect of the coumarin may increase by co-trimoxazole. By this, the clotting time increases. This is also true for the combination sulfametrol+trimethoprim.
Trimethoprim alone does not have a relevant drug-drug interaction.

Recommendation:
Avoid the combination, replace cotrimoxazol.
Co-trimoxazole given chronically: a therapeutic alternative is possible almost always. It appears sometimes in *Pneumocystis carinii*.

Fig. 4.1 Alert text DDI anticoagulant – co-trimoxazole

Antibiotics indirectly increase the effect of coumarins. By this, the clotting time increases. The increased effect of coumarins is probably due to increased metabolism of clotting factors during fever.

Recommendation:
Tell the patient to contact the thrombosis service.

Fig. 4.2 Alert text DDI anticoagulant–antibiotics

Severity Unclear from Alert Text

The alert text for the DDI with co-trimoxazole is worded rather cautiously, and it does not become very clear that the combination is contraindicated, whereas the combination of an anticoagulant with other antibiotics can be prescribed safely with INR monitoring (Figs. 4.1 and 4.2).

It appeared that the first two sentences of the alert text and font size were similar, the recommendation was not put in capitals, and the word contraindicated was not used. Furthermore, the sentence "It appears sometimes in *Pneumocystis carinii*" was unclear: was it allowed to prescribe co-trimoxazole for this indication in patients on anticoagulants or not? It is recommended to use a signal word to indicate the severity like "warning" or "danger" and to use a mixture of upper and lower cases for easier reading [9].

Severity Rating Similar

In the Dutch drug database G-standard, all DDIs have been assigned an alphanumeric code comprising the level of evidence (0–4) and the level of severity (A–F) based on the type of adverse reaction if a combination is prescribed [10]. All DDIs with vitamin K antagonists have been assigned severity level D: increased risk of bleeding or deep venous thrombosis. Although co-trimoxazole (and miconazole) should be avoided in combination with vitamin K antagonists and other antibiotics can be prescribed together with these drugs if INR is monitored, the severity levels

of these DDIs are the same. The severity level only includes the adverse event that may arise and does not take into account the risk (incidence) of serious INR overshoot. It can be questioned whether this incidence should be included in the severity level. In several CPOEs a difference in severity level results in a distinct presentation of the alert.

Furthermore, the DDIs with antibiotics and co-trimoxazole have the same level of evidence as these combinations have been studied in controlled published interaction studies in patients or healthy volunteers with surrogate endpoints.

Severity Unclear from Alert Pop-Up

In the CPOE/CDSS Medicatie/EVS® (Leiden, the Netherlands), utilized in the institution above, all DDIs look similar, regardless of the severity level (Fig. 4.3). There are no possibilities to improve visibility by implementing colors, different icons or shapes either, as recommended for good usability [9].

Too Many Alerts

DDI alerts with anticoagulants are generated frequently. A Dutch study in an academic hospital using the CPOE/CDSS Medicatie/EVS® showed that 34 % of the orders generated a drug safety alert; DDIs were generated in 19 % of orders. In 10–13 % of overridden DDI alerts, an anticoagulant was involved [11]. In this case,

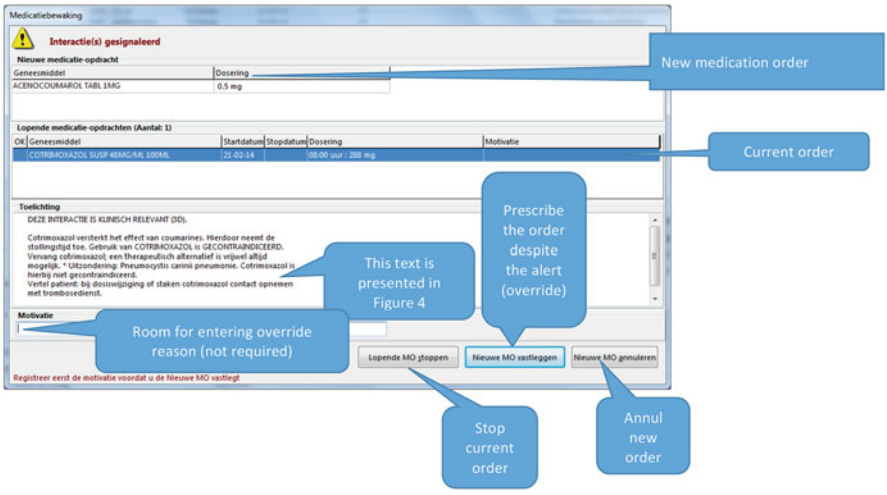


Fig. 4.3 Alert for DDI acenocoumarol–co-trimoxazole

one of the physicians replied "there are so many alerts and generally you can override them without problems."

Overriding Default Option

In the CPOE/CDSS Medicatie/EVS® it is very easy to override a DDI. Figure 4.3 shows that three options to handle the alert are present: (1) Stop the current order, (2) Prescribe the new order despite the alert, and (3) Annul the new order. Default is the second option, which results in overriding the alert. A "motivation" can be given, but is not required. It is not possible to change the default option to annul the new order or to make the motivation for overriding a required field.

Different Specialties

In this case, different specialties (pediatrics, pediatric cardiology) and several pediatric residents were caring for the patient during the 4 weeks of admission. This could have resulted in indecision: "there should be a reason why my colleague did not dare to stop the co-trimoxazole." Eventually the indication for co-trimoxazole appeared to be relapsing airway infections in the past. Also, different hospital pharmacists handled this DDI and not everybody called the prescribing resident when they saw a colleague had already asked to stop the co-trimoxazole.

Summary of Causes

The unjustified overriding in this case was probably due to a combination of the abovementioned causes. The sociotechnical approach helps us to analyze and group the different causes of the HIT-related error of this case [12]. Technology, people, organization, and external environment—all attributed to this potential adverse event in this case.

Technology: All DDI alerts look the same and it is impossible to adjust colors. Furthermore, changing the default handling option to annul the order is not possible either.

People: The majority of prescribers do not know that co-trimoxazole and miconazole are contraindicated in patients on vitamin K antagonists.

Organization: Several specialists and residents were involved in this case. The resident is the central person that prescribes and has to be called, but supervisors decide and probably do not have all the relevant information provided by the CDSS and the pharmacist.

External environment: The national drug database, G-standard, is the professional standard and provides the DDI alerts that are relevant, its severity level and evidence index.

Solutions

It is difficult to solve the problem of lack of knowledge on the relevance of the DDI with vitamin K antagonists. We included this case in the training given to pediatric residents and the pharmacist explained the difference between the DDI with co-trimoxazole and with other antibiotics. It is not known whether this lesson is really helpful in preventing the unjustified overriding of the DDI anticoagulant–co-trimoxazole. Specialists were not invited for this lesson; however, they often eventually determine therapy.

A clearer alert text may result in a learning effect. The original text was worded very cautiously and in one font size. The G-standard changed the text for better understanding. For better visibility, we put part of the alert text in capitals (Fig. 4.4). These adjustments are in line with the recommendations for implementation of human-factors principles in medication-related CDSS [9].

Physicians often complain about the high number of alerts generated. To counteract alert fatigue, they often ask to turn off DDI alerts. In the Netherlands, the G-standard is the professional standard and therefore, turning off DDIs can be rather tricky from a legal point of view. Patient harm due to a suppressed DDI included in the professional standard would probably result in blaming (or suing) the professional that deliberately turned it off.

A more subtle presentation of the alert (just a warning icon in front of the order instead of an intrusive pop-up that has to be acknowledged) can be an option to meet both wishes: not deviating from the professional standard and avoiding too many intrusive alerts. Although this option can be performed in theory, the implementation and maintenance is so time-consuming that it is not really feasible to free all prescribers from these intrusive alerts and keep the system up-to-date. First, every prescriber in a specialty has to be entered separately in the system. Furthermore, all DDIs that have to be shown non-intrusively should be linked manually to all specialties. This is not feasible in the biggest academic hospital in the Netherlands with on an average 35 new prescribers every month.

Therefore, we chose to implement another measure to increase patient safety by reducing alert fatigue in the hospital pharmacy. We decided to skip all DDIs with coumarins, except for those with co-trimoxazole and miconazole from the lists of DDIs to be handled by the pharmacist. This measure was easy to perform.

Another option to reduce alert fatigue is to develop clinical rules. These are algorithms in which other parameters, for example laboratory values, are used to increase

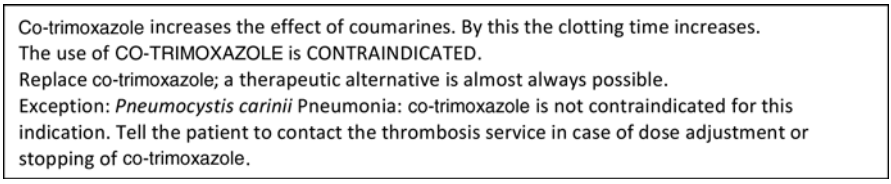

Co-trimoxazole increases the effect of coumarines. By this the clotting time increases.
The use of CO-TRIMOXAZOLE is CONTRAINDICATED.
Replace co-trimoxazole; a therapeutic alternative is almost always possible.
Exception: *Pneumocystis carinii* Pneumonia: co-trimoxazole is not contraindicated for this indication. Tell the patient to contact the thrombosis service in case of dose adjustment or stopping of co-trimoxazole.

Fig. 4.4 New alert text DDI anticoagulant – co-trimoxazole

specificity of the DDI. A clinical rule could select those patients using an anticoagulant for which a recent INR is not available or is outside normal limits and those using an anticoagulant in combination with a contraindicated drug, such as cotrimoxazole. If this type of clinical rule is put in place, DDIs for anticoagulants can be turned off without impairing patient safety. For those patients on anticoagulants without a DDI the clinical rule can also identify lacking recent INR measurements, so further improving patient safety.

The problem of different specialties caring for the patient and indecision by residents can be solved by a procedural measure to call the supervising specialist if the resident does not want to change the order himself.

In conclusion, as the causes of this medication error is multifactorial, several solutions including simple as well as more complex measures can be proposed.

Case Study 2: An Overdose of Paracetamol

Clinical Summary

A 4-year-old boy weighing 16 kg suffering from malaise, weight loss, and frequent blood-containing stools was admitted to a Childrens' hospital for a colonoscopy to confirm the diagnosis of ulcerative colitis with anemia. He was transferred from a general hospital with a medication list of prednisolone 20 mg once daily intravenously and paracetamol 355 mg 4 times daily orally. Upon admission, it was decided to change all medication to the parenteral route, except for the drugs required for intestinal lavage before colonoscopy. The resident entered paracetamol infusion fluid 360 mg four times daily. A drug safety alert was generated and overridden (See Fig. 4.5). The next day the pharmacist checked the list of overridden alerts and asked the resident to change the dose from 90 mg/kg/day to 60 mg/kg/day, which is the maximum daily dose for the intravenous route. The resident changed the dose to 240 mg 4 times daily (60 mg/kg/day), but again received a pop-up for overdose. Adverse events were prevented because the order was changed timely.

Background Information

Dose checks in the CPOE are derived from dose limits from the G-standard and are based upon the Dutch Pediatric Formulary, developed by pediatric hospital pharmacists and pediatricians. For each drug used in children, the G-standard contains maximum standard and absolute dose limits in mg, as well as in mg/kg and mg/m^2, per age and weight category. For antibiotics, minimum doses limits are available as well. Exceeding the standard dose limits should result in a warning in the CPOE. Absolute dose limits should not be exceeded. Dose limits are present for each dose frequency known for that drug and for each route of administration. Furthermore, a distinction between inpatient and outpatient care and between different indications is made.

Fig. 4.5 Overdose alert for paracetamol 90 mg/kg/day for a child weighing 16 kg

The pediatric dose check in the CPOE was thoroughly tested and adjusted before implementation. In 2008, we entered 560 orders of 33 pediatric patients of different age groups and subspecialties into a test version of the CPOE with the new pediatric dose check. We counted all intrusive dose alerts, intrusive indication inquiries and non-intrusively shown warning icons that a dose check could not be performed. Furthermore, dose alerts were recorded as irrelevant if the dose was between 100 and 120 % of the maximum dose because of rounding off doses to the nearest available dosage form (e.g., a rectal paracetamol dose of 110 mg rounded off to a suppository of 120 mg). Indication inquiries were recorded as irrelevant if dose limits were equivalent for different indications or dose limits were absent for the indication and patient at hand. Overdose alerts were generated in 10.5 % of orders and 36 % of the alerts was deemed irrelevant, as were 79 % of the indication inquiries. In 35 % of orders, dose checking was not feasible.

An adjustment in software was required to reduce the risk of alert fatigue. We requested the software vendor to generate an alert only if the dose was ≥120 % of the dose limit, but showing the original dose limits in the overdose alert. Furthermore, we asked to prevent indication inquiries and use the highest dose limits for that age or weight group. Reason for this was that a physician not knowing what to choose from the list of indications automatically would select the first option, which is the combination of all dose limits and thus the highest dose limits for that age or weight group.

To reduce the number of orders for which no dose check could be performed, we asked the G-standard to include more dose limits that were already available in the Dutch Pediatric Formulary. Furthermore, we entered dose limits for drugs manufactured by the hospital pharmacy and for intravenous solutions that are often given orally in children. We also adjusted the dose limits for paracetamol orally and rectally to the absolute maximum dose of 90 mg/kg/day preventing alerts when exceeding the

standard dose of 60 mg/kg/day. Exceeding an absolute maximum dose limit results in a red alert requiring a motivation, whereas exceeding a standard dose limit results in an orange alert which can be overridden without motivating it.

The pediatric dose check was implemented stepwise in 2013 in Erasmus MC-Sophia Children's Hospital. Dose limits were shown at the bottom of the ordering screen and dose checks were performed per dose and per day for standard and absolute maximum doses, in mg, mg/kg, or mg/m^2. For each subspecialty a lesson was given by the pediatric hospital pharmacist emphasizing that each dose alert should be given attention because irrelevant alerts were suppressed. After implementation, overridden alerts were checked for relevance and if dose checks could not be performed due to lacking dose limits, these were added whenever possible.

Analysis

What Happened?

A pediatric resident changed an existing order for oral paracetamol to the same intravenous dose and overrode the dose alert that the absolute maximum per administration and per day were exceeded (Fig. 4.5). The physician had to enter a motivation for the order to be prescribed and entered "home medication," which was not completely true, because dosage form and route differed.

Why Did It Happen?

Lack of Knowledge

Prescribers do not realize that a switch from oral to intravenous medication often requires dose adjustment, and is dependent on the bioavailability of the drug, even though this is included in the general courses and exams for medical students.

Alert Pop-Up Too Complicated

As seen in Fig. 4.5, overdoses are presented as bars for all doses over a period of 3 days, whereas one day would be sufficient. The right part of the alert shows the extent to which the daily dose has been exceeded; the left part shows whether every single dose exceeds the dose limit. Physicians perceive the daily dose as relevant and are not really interested whether a single dose exceeds the dose limit. The daily dose is preferably presented in the left part, but is now shown at the right part and therefore easily overlooked. Dose limits can be exceeded per kg, per m^2 or in mg; this is presented in text above the bars. There is so much text in the alert that it is not easily interpreted. Alerts can be presented with green and red bars, green and orange bars, or green, orange, and red bars. When standard and absolute dose limits are

equal, only red bars will be shown. Orange may indicate that a standard dose limit has been exceeded and an absolute dose limit has not been exceeded. However, it may also indicate that an absolute dose limit is absent. The interface design of the pediatric dose check is not adequately designed to support a quick perceptual judgment and to reduce cognitive effort.

Too Many Alerts

The CPOE/CDSS Medicatie/EVS® generates intrusive drug safety alerts in about one-third of orders [11]. A yellow triangle with an exclamation mark is shown in the medication overview screen just left to each order with an overridden alert. However, for each order for which a pediatric dose check could not be performed because of lack of dose limits for that drug, age or weight category a yellow triangle is shown as well. The high number of yellow triangles desensitizes physicians to these icons.

The test performed before implementation focused on the correctness of the dose check for single orders. After implementation, it appeared that dose adjustment of an existing order results in adding up the dose of both the existing and the new order, thereby almost always exceeding maximum dose limits. This functionality flaw in ignoring start and stop time of the order has to be solved by the software vendor in order to reduce the number or irrelevant alerts.

Trust in Checks by Other People

Every day a pharmacist checks the orders with overridden alerts and for which no dose check could be performed. The pharmacist calls the physician when the order should be adjusted. This may result in a situation in which the physician overwhelmed by the information of the alerts may trust that he/she will be called when action is required. This "trust in checks by other people" may further contribute to alert fatigue.

Default is "Adjusting the Order"

If an alert occurs, there are three options to handle the alert: 1. Adjusting the dose, 2. Prescribing the dose despite the alert, and 3. Annul the order. Default is the first option of adjusting the dose. This is in contrast with the DDI alerts in which overriding is the default option. However, in spite of this better design, dose alerts are frequently overridden as well.

The second option of overriding the alert is only possible when the standard dose limit has been exceeded and the absolute dose limit has not. When the absolute dose has been exceeded, the prescriber has to give a motivation in the pop-up. After entering a (free text) motivation, the order can be prescribed. However, entering a comma or a letter is sufficient to enable prescribing.

Summary of Causes

The unjustified overriding in this case was probably due to a combination of the abovementioned causes.

Technology: Dose alerts are very complicated, with redundant information and orange colors with different meanings, and are sometimes erroneously generated in order adjustment.

Process: Pharmacists check whether errors are made and this may make prescribers relying on the pharmacy checks.

People: Prescribers do not know that changing the route from oral to intravenous may imply different dosing because of drug-dependent differences in bioavailability.

Organization: Although dose limits are shown at the bottom of the ordering screen as a help for prescribers, it appears that these are not used very often.

External environment: The G-standard uses rather low standard dose limits for paracetamol for inpatients, which results in alert overload.

Solutions

It is difficult to solve the problem of lack of knowledge as IV-to-oral shift and vice versa is already included in the regular training for medical students.

Although guidelines for human-factors principles in medication-related decision-support systems are followed to a great extent to reduce the problem of alert pop-ups that are too complicated, further guidelines for dose checks should be developed.

The superfluous dose alerts because of adding up doses when dose adjustment has taken place should be removed as soon as possible by the software vendor. A prescriber should not be bothered by a yellow triangle in front of the order if a dose check could not be performed; instead the pharmacist should be warned. The number of irrelevant alerts has already been reduced and this is an ongoing process. If prescribers motivate their overdose-override, they provide the pharmacy with relevant information. The pharmacy can ask the national drug database to adjust dose limits or adjust dose limits themselves if safety can be guaranteed.

As it is also pharmacists' job to check orders and prevent medication errors, the problem of desensitization of prescribers by trust in other people cannot be solved.

Discussion

These cases show that errors due to alert override take place and may have many causes.

Alert fatigue is certainly present; although measures to prevent it already have partly been undertaken, these measures are at times hampered by technical constraints. A balance should be found between safety and legal aspects versus alert fatigue. Poor CDSS may be worse than no CDSS [13], but patient harm because of alerts that have been turned off is probably more reproachable than patient harm because of erroneously overridden alerts.

James Reason advocated a system approach for error analysis that proposes that error-producing and latent conditions are present in a system and if unaddressed, these enable humans to make active errors [14]. Figure 4.6 shows how alert fatigue is caused and demonstrates the opportunities for counteracting alert fatigue. The best way to prevent alert fatigue is to increase specificity and to improve usability of the alerts. Furthermore prescribers should have enough training in drug therapy and related safety alerts. Good usability of the alerts may contribute to a learning effect.

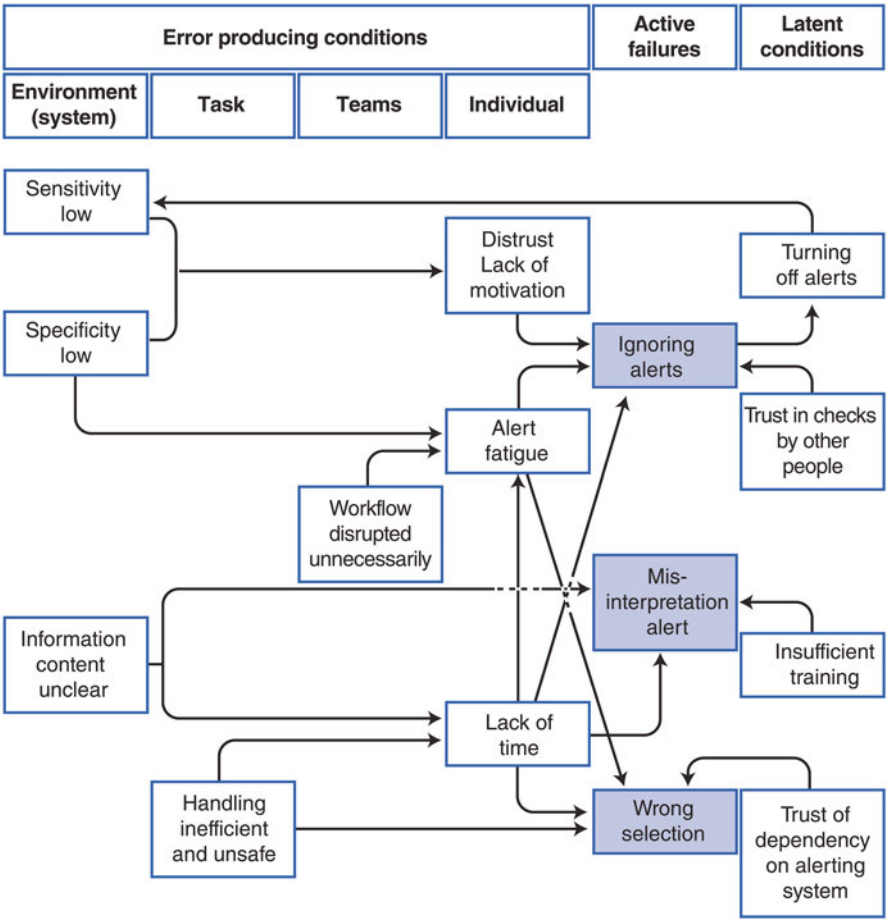


Fig. 4.6 Reason's model applied to drug safety alerts in CPOE

Key Lessons Learned

- Alert fatigue is present even when measures to reduce it have been taken.
- Usability of alerts should be improved by following guidelines for human-factors principles in medication-related decision support.
- Specificity of alerts should be improved by using lab values in alert suppression and generation, by developing clinical rules.

References

1. Bates DW, Teich JM, Lee J, Seger D, Kuperman GJ, Ma'Luf N, et al. The impact of computerized physician order entry on medication error prevention. J Am Med Inform Assoc. 1999;6:313–21.
2. Van Doormaal JE, van den Bemt PM, Zaal RJ, Egberts AC, Lenderink BW, Kosterink JG, et al. The influence that electronic prescribing has on medication errors and preventable adverse drug events: an interrupted time-series study. J Am Med Inform Assoc. 2009;16(6):816–25.
3. Van der Sijs H. Drug Safety Alerting in Computerized Physician Order Entry. Unraveling and Counteracting Alert Fatigue. PhD Thesis Erasmus University Rotterdam. http://hdl.handle.net/1765/16936. Accessed 15 June 2014.
4. G-standard: https://www.z-index.nl/english. Accessed 15 June 2014.
5. Visser LE, Penning-van Beest FJ, Kasbergen AA, De Smet PA, Vulto AG, Hofman A, et al. Overanticoagulation associated with combined use of antibacterial drugs and acenocoumarol or phenprocoumon anticoagulants. Thromb Haemost. 2002;88(5):705–10.
6. Schalekamp T, Van Geest-Daalderop JHH, Kramer MHH, Holten-Verzantvoort V, De Boer A. Coumarin anticoagulants and co-trimoxazole: avoid the combination rather than manage the interaction. Eur J Clin Pharmacol. 2007;63:335–43.
7. Baxter K. Stockley's drug interactions, 8th edn. Pharmaceutical Press: London. 2008; 365–6.
8. Van der Sijs H, Aarts J, van Gelder T, Berg M, Vulto A. Turning off frequently overridden drug safety alerts. Limited opportunities for doing it safely. J Am Med Inform Assoc. 2008;15:439–48.
9. Zachariah M, Phansalkar S, Seidling H, Neri PM, Cresswell KM, Duke J, et al. Development and preliminary evidence for the validity of an instrument assessing implementation of human-factors principles in medication-related decision-support systems – I-MeDeSA. J Am Med Inform Assoc. 2011;18 Suppl 1:i62–72.
10. Van Roon EN, Flikweert S, le Comte M, Langendijk PN, Kwee-Zuiderwijk WJ, Smits P, et al. Clinical relevance of drug-drug interactions: a structured assessment procedure. Drug Saf. 2005;28(12):1131–9.
11. Van der Sijs H, Mulder A, van Gelder T, Aarts J, Berg M, Vulto A. Drug safety alert generation and overriding in a large Dutch university medical centre. Pharmacoepidemiol Drug Saf. 2009;18:941–7.
12. Institute of Medicine. 2012. Health IT and Patient Safety. Building Safer Systems for Better Care.
13. Coleman JJ, van der Sijs H, Haefeli WE, Slight SP, McDowell SE, Seidling HM, et al. On the alert: future priorities for alerts in clinical decision support for computerized physician order entry identified from a European workshop. BMC Med Inform Decis Mak. 2013;13:111.
14. Reason J. Human error: models and management. BMJ. 2000;320:768–70.

Chapter 5
Errors Related to Bar Code-Assisted Medication Administration

Jonathan S. Bagby

Introduction

The initial patent for a bar code titled "Classification Apparatus and Method" was issued in 1952, but the patent expired 5 years before the first commercial use of the technology [1]. In 1973, the International Business Machine (IBM) Corporation developed the Universal Product Code pattern for bar codes which was used commercially in 1974 to scan a pack of Wrigley's chewing gum at a supermarket in Troy, Ohio [2]. Although the bar code has been around for over 60 years, its use in health care is relatively new and using the bar code as a tool to improve the safety of medication administration has been on the rise for only the last 15 years.

In 1999, the US Department of Veterans Affairs' Veterans Health Administration rolled out its Bar Code Medication Administration (BCMA) software application to all inpatient medical facilities [3]. The application uses a simple concept to help ensure that the right patient is receiving the right medication at the right dose, at the right time, and via the right route. The BCMA user, while verifying these five rights manually, uses a bar code scanner to input the patient data into the application. The application compares the number from the scanned item, such as the bar code on the patient's wristband, to the patient database and after the patient's identity is confirmed by the user, the user scans the bar code on each drug. The application then compares the numbers represented by the bar code on the scanned drug to those of the drug assigned by the pharmacist as well as comparing the current time to the due time. If the numbers match and time is within an acceptable time frame, BCMA records the medication as administered. If the numbers do not match or the time is beyond the acceptable time limit, BCMA provides an indication to the user of the mismatch so the user can take corrective action, such as obtaining the correct drug or waiting until the appropriate administration time.

J.S. Bagby, M.S.N., M.B.A., R.N-.B.C. (✉)
United States Department of Veterans Affairs, 2663 Willowlawn St,
Roanoke, VA 24018, USA
e-mail: jonathan.bagby@gmail.com

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_5

BCMA systems have generally been shown to improve medication administration accuracy [4–9]. Additionally, since the US Food and Drug Administration (FDA) requirement to bar code all unit-dose medications produced for hospital point-of-care administration went into full effect in 2006 [10], the number of medications without bar codes has dropped significantly. The research demonstrating the improved medication administration accuracy and the support of the FDA for bar coding products has led to the US Office of the National Coordinator (ONC)'s endorsement of the technology by including the use of automatic identification and capture technology (such as bar coding) as a requirement for Meaningful Use certification of the Electronic Health Record (EHR) [11]. The technology in health care has become ubiquitous with nearly every major manufacturer of EHR software offering its own unique version of a BCMA solution. The recommendation to employ bar coding is laudable; however, this chapter seeks to point out a few cases where the technology did not improve patient care. In fact, there are some scenarios when bar code technology has inadvertently led to medication errors.

Clinical Case Studies

Case 1

Clinical Summary

Seventy-six year old Andrew Taylor was admitted to the hospital following surgery to repair an abdominal hernia. He had been prescribed metoprolol at the same dose and rate he had been taking at home, 50 mg by mouth twice per day. A week earlier, the pharmacy had sent a message to the inpatient staff alerting them that they were having trouble obtaining metoprolol from their usual vendor and that the pills may look different than the ones they usually dispense. Following Mr. Taylor's surgery, the nurse searched for the patient's medications. He had only arrived from surgery a few hours ago, so his medications had not yet been delivered by the pharmacy. He was on the same basic medications that many other patients on the same floor had been prescribed, so the nurse went to the med room and looked through the drawer of a patient who had recently been discharged. "Ah ha, here we go," she thought as she snatched several metoprolol SA tablets from the discharged patient's drawer and placed them in a drawer for her patient. She took the medication cart to the bedside and scanned the bar code on the patient's wristband. After confirming the patient's identity, she started scanning the medications. Everything worked fine until she got to the metoprolol SA. When she scanned the medication, the program showed an error that said "incorrect medication, do not give." She was used to seeing this kind of error frequently, but usually if she cleared the error and scanned the medication again, it would work. Not this time; she scanned the medication a second time and it still did not work. Then she remembered the email she had seen the other day from the pharmacy about the hospital getting new metroprolol pills. She thought, "Hmm, it must not be

in the system yet." and proceeded to ignore the error and administer the metroprolol SA tablet to the patient. Over the course of the evening, the pharmacy came with the patient's medications and refilled the cart for the next day. The practice by the pharmacy is to take any medications still in the patient's drawer at the end of the day and transfer them to the new drawer, so there may always be a few extras in case something does not scan correctly. The day shift nurse scanned the patient's regular metoprolol, but when the evening shift nurse came on and pulled out the metroprolol SA to scan, she received the same error as the night before. "Oh well, I guess they are never going to enter this one in the system." and proceeded to administer the metoprolol SA again. For three more days, this continued until finally, Mr. Taylor's heart rate became dangerously low. He became lethargic and was having apneic spells. He was eventually transferred to the ICU where he later recovered.

Analysis

Many medications come in various compositions such as normal, short acting, and long acting; as such, "SA" can often be confusing because it could stand for either "short acting" or "sustained action." It was this hospital's policy that "SA" would be used along with the generic name for all non-branded long acting medications, but that was not common knowledge among all the nurses. This can be especially problematic for nurses who work in other facilities, such as traveling nurses, who are not as familiar with local policies as full-time employees.

Another factor contributing to the errors above was the use of other patient's medications. Borrowing medications from another patient's drawer has long been a workaround employed by nurses to ensure medications are available for their patients in a timely manner [12]. The unit dose medications are not labeled with the individual patient names, so it is possible to share unit dose medications between patients. In fact, it is somewhat of a necessity. If every medication had to be labeled specifically for every patient, the logistics of packaging, stocking, and tracking every medication for every patient would be overwhelming; consider all the ward stock medications such as acetaminophen, milk of magnesia, and so on that would have to be labeled for each individual patient. Then consider the IT burden of having to store and process all that information and the potential waste from personally labeled medications that are not consumed upon discharge. Many pharmacies would need to double the amount of staff to process medications if it were not for the ability to have ward-stocked medications. At any rate, the nursing staff should not be allowed to pilfer from other patients' drawers.

The lack of knowledge regarding the abbreviation and the poor practice of pilferage notwithstanding, this story represents a bigger problem which is the lack of trust in the system. The nurse had seen the same error message many times before and when she usually scanned the second time, the medication worked properly. This leads to the problem where users begin to doubt whether the system works as it should and the error messages go from being a useful troubleshooting tool to merely a roadblock around which the nurses quickly learn to navigate.

Solutions

Some hospitals have created systems requiring staff to place a discharged patient's medications in a tamper resistant bag to prevent nurses from creating their own ward stock. However, who is to say the nurse does not just remove what she wants to keep on-hand before sealing the bag? One potential solution to that would be to have the patient's medication drawer rendered inaccessible upon discharge. Of course, for facilities that stock most of the patient's medications in an automated dispensing cabinet (ADC) and not in individual patient drawers this is not an ongoing issue.

Using the acronym "SA" for sustained action is acceptable and necessary in some situations. For example, in a situation where everyone is trained on the use of acronyms, abbreviations, and policy and a demonstration of competency requirement is in place. It may be necessary to use abbreviations and acronyms when the print or display area is very limited in size. However, in this case, not all users are trained on this specific policy and therefore, a large population of staff are at risk for misunderstanding the acronym. Information should be made available to the user and not expected to be remembered [13]. The hospital should do their best to figure a way to spell out such important acronyms when there is a strong possibility of a misinterpretation.

Finally, the system has to work seamlessly to build up the trust in the system. Once that trust is lost, it can take a very long time to rebuild that trust. This is why many relationships often fail; one breach of trust can lead to a lifetime of distrust even if the breach never occurs again. If an issue has been fixed but the user does not know the issue has been fixed and the user receives another error, he or she is likely to think the system is still broken and not bother to report the new error. Additionally, if they must use the system to get their work done, the user will do whatever he or she has to in order to complete the task, including finding a workaround. Koppel et al. [14] identified numerous workarounds employed by staff. Any system is likely to have hiccups during the "go-live" phase that did not appear during testing. The key is not only to get those issues fixed as soon as possible, but to quickly communicate to the staff that the issue has been fixed to provide reassurance and to help build trust in the system.

Case 2

Clinical Summary

Bonnie was a new nursing assistant and had recently started working in the community living center (CLC). One of her duties was to replace the bar code wristbands on the residents every other Tuesday. During her first pass down the hall to replace wristbands, Mr. Eagles was in the bathroom. When she returned later to Mr. Eagles' room she found a man on the side of the bed. "Mr. Eagles," she said. "Yes" the man replied. "Hold out your arm, I have to put this new wristband on you." The

man obliged, the nursing assistant applied the wristband and went down the hall searching for other residents to label. Shortly after the nursing assistant left the room, Mr. Eagles emerged from the restroom. "Ok Fred, are you ready to go to the dining room?" Mr. Eagles said to the man sitting on the side of his bed.

About a week later, the CLC's nurse manager received a call from the laboratory. "How's Mr. Eagles doing? We have noticed his blood glucose results have been really out of range, but when we looked back at his record, we do not see an order for blood glucose testing on him." The nurse manager looked in the record and sure enough, Mr. Eagles did not have an order to test his blood glucose. She went to Mr. Eagles' room and asked him directly who had been checking his sugar levels. He said that no one had performed any tests on him in several weeks.

Later that day, the nurse practitioner caring for several residents in the CLC asked one of the staff nurses why Fred's blood sugar was not being checked regularly. When the staff nurse looked at Fred's record, she could see that the nurses had not been documenting blood glucose levels regularly before meals and at bedtime. The results seemed to be varied; some results were there but some were not and there was not any appreciable pattern. When the staff nurse mentioned it to the nurse manager, the two visited Fred's room together and discovered that Fred was wearing two wristbands! The one on his left wrist belonged to him, but the one on his right wrist actually belonged to Mr. Eagles.

Analysis

Both Fred and Mr. Eagles had been residents of the CLC for several years. All the nurses knew them well; so well, that when it came to checking Fred's blood glucose with the point-of-care glucometer or administering his medications, the nurses never even bothered to make sure they had the correct patient. The users scanned the patient's wristband, followed the prompts on the glucometer to scan the user's badge, and performed the test. The test results were then uploaded to the blood glucometer system. The glucometer system used the information from the transaction to stuff the results into the record of the patient whose band was scanned. Only when the system could not find a matching patient in the database after the information is uploaded, would the laboratory personnel receive an error. In this case, since both patients were in the database, the information flowed directly into the wrong patient's record.

A bar code can be used to open a patient's record, enter information into a patient's record, or check to ensure a match between the scanned patient and an open patient record; however, no bar code can ensure the application is actually opening the correct patient's record; this requires manual human vigilance. The blood glucometer system in this case is not linked to the EHR. When the user scans the patient's band, there is no opportunity for the nurse to ensure that the scanned patient is the correct patient. The glucometer does not review the patient database to ensure the scanned information matches a patient in the database; moreover it does not display this patient's information and then require the nurse to verify it is correct.

This case illustrates several issues, including overreliance on the system, rote processes, and using an incorrect mental model. In certain practice settings, it is common for health care staff to get to know long-term patients. This is common in behavioral health, residential treatment centers, and CLCs (a.k.a. nursing homes). The patients may live in these care areas for years and consider them home. As a result, some residents find wearing identification bands like a stigma, especially for residents of behavioral health domiciliary programs where the residents are often out working in the general public during the day; a wristband draws unwelcome attention. For this reason, many of these programs rely on visual identification of the patient, with photographic identification as a backup. This visual identification coupled with the rote process of scanning and an incorrect mental construct can lead to the errors as seen above.

With the BCMA system, users were taught to pull up the patient's record and then scan the patient's band. If the open record and the band did not match, the system produced an error. The problem here is that the users were trying to apply the mental model they have created of the medication administration system to the glucometer system. Both systems use bar codes to scan the patient's wristband and both use bar codes to scan the user's badge to identify the user. So why would the user think there is any difference between the two systems? As far as the user is concerned, both systems function the same way and therefore, if there was a problem with the patient identification, the user believed the system would warn the user.

Solutions

One of the key features of any bar coding system used for safety is the requirement that human interaction still occurs. The elegant solution many readers may lean towards is to have the glucometer systems interact directly with the EHR. While that is a potential solution that may cost millions of dollars to develop, not to mention contracts between glucose monitoring systems and EHR developers, or at the least paying a third-party to develop an interface between the two, there is a much simpler solution that really tackles the root of the issue. The root of the issue was misidentification of the patient when the wristband was initially applied. Local processes that ensure competency in basic patient identification and wristband applications would be far less time consuming and expensive than integrating the disparate glucometer and EHR systems. A simple requirement that the patient's identification be adequately checked when applying a new wristband could potentially reduce numerous errors; an ounce of prevention is worth a pound of cure. Below are some relatively "low-tech" solutions to the real root cause of the issue:

1. Require the patient to state full name and other personally identifiable information, such as date of birth and address, before placing the new wristband, i.e., the staff should require "active identification" by the patient as opposed to "passive" acceptance.

2. Require the presence of two staff members (at least one who is familiar with the patient for residential care areas) when placing or replacing a wristband. This would be similar to the process most facilities use for validating blood products prior to administration.
3. Use a photographic identification method as an adjunct to verbal confirmation by the patient when placing a new wristband (when the patient's visual appearance is not significantly impaired).
4. Use the bar code scanner to scan the patient's wristband when applying to ensure the wristband is functional and opens the correct patient's record.
5. Assess for and remove any objects that may lead to misidentification (such as other wristbands).

Case 3

Clinical Summary

A new nurse was giving her first dose of medication during the implementation phase of BCMA at her facility. She had attended the training session just two days earlier, but this was her first encounter with the system alone. She logged in to the network, then logged into the BCMA application, opened the patient record and ran a report of the medications she needed to pull out of the ADC. She looked at the list of items to pull from the ADC and saw an order for heparin 10,000 units/ml. She thought that was a little strange since she had not had a patient on heparin in a long time; at least not within the last 9 months or so. Most of the patients on her unit were taking enoxaparin as the anticoagulant of choice these days. She pulled the vial of heparin from the ADC and returned to the patient's bedside. She logged into the computer at the bedside, scanned the patient's wristband, and validated the patient's identity just the way she was shown in class. After validating the patient's identity, she looked at the list of medications on the BCMA screen (Fig. 5.1). She recalled the class a few days ago and thought to herself it did look a little different because there were only five orders on this patient's screen as opposed to the 15 or more on the screen in the training class.

"This may be easier than I thought," she said to herself. She looked at the Medication column, confirmed heparin 10,000 units/ml, and looked across to the cell to the right in the table displayed on the screen. In the next column, it read 5000 units/0.5 ml. She nodded and said, "Yes, 10,000 units/ml is the same concentration as 5000 units/0.5 ml," and proceeded to scan the drug. BCMA did not display any sort of error, confirming the nurse's suspicions that this must be the correct drug. A new window then appeared in BCMA asking her to enter the amount of the drug administered. She typed in "10,000 units" being sure to spell out the word "units," as she was taught in class and proceeded to administer a dose of 10,000 units of heparin to the patient.

Patient: Doe, John MR#: 12345678 DOB: 01/01/1965 Height: 72 in Weight: 242 lbs		Provider: Smith, Robert Room: 263 Bed: 1	Vital Signs: T: 98.2 C HR: 72 B/P: 132/84 R: 18 Allergies: Meperidine			
Status	Type	Medication	Dose	Route	Due Time	Last Action
Given	Scheduled	Lisinopril Tab Lisinopril 10mg tab (UD)	10mg, QDay	PO	10/10@0900	Given 10/10 09:21
	Scheduled	Heparin Inj Heparin 10,000units/ml (INJ)	5000units/0.5ml , Q12H	SQ	10/10@0900	Given 10/09 21:12
Held	Scheduled	Bisacodyl Tab Bisacodyl 5mg tab (UD) **Hold if patient has loose stool**	5mg, BID	PO	10/10@0900	Held 10/10 09:19
	PRN	Morphine Inj Morphine 2mg/ml (INJ) **For pain equal to or greater than 5/10**	4mg/2ml, q2H PRN	IV Push		Given 10/10 07:45
	PRN	Acetaminophen Tab Acetaminophen 325mg Tab (UD) **For pain < 5/10**	650mg, q6H PRN	PO		

Fig. 5.1 BCMA screen

Analysis

The error in this case is that the dose ordered for the patient was 5000 units, not 10,000 units. There are several factors that led to this mistake including training, preceptorship, human factors, and system design. Training courses for BCMA can be overwhelming. There is often a desire by the instructor to cover every aspect of the new application and often in a very limited time. Conversely, many facilities have adopted online training as their preferred mode of training because it improves availability and enables asynchronous learning. However, there is rarely a happy medium; the users end up overwhelmed by too much information or do not have quite enough training to use the system safely. In this case, the desire of the instructors to cover every possible scenario during training required numerous orders for a variety of medications to be available on the training patient's record. This led to the user feeling overwhelmed and having difficulty transferring the information she had learned in the training class to the real-life scenario.

Regardless of the training modality, preceptorship is a key ingredient to success. No new user should be allowed to use the system alone until a competent user of the system, system manager, or supervisor has deemed the new user competent to use the application. Simply sitting through a training class, either in person or via web-based instruction, is generally not sufficient enough to support safe use. Preceptors, super-users, and supervisors should have a checklist of items that must be demonstrated before the user is allowed to be on his or her own. Almost everything people do when it comes to safety involves specialized training, observation, and successful solo demonstration of practical skills and/or knowledge prior to issuing a statement of competency. Can you imagine if people were allowed to

drive vehicles after just watching a video or simply mimicking the actions of a driving instructor in a classroom without having to demonstrate competence?

In this case the blame could not be placed squarely on training, preceptorship, or user competence, because there are human factors and systems issues involved as well. Recall Fig. 5.1 and the design of the user interface. One column is labeled "Medication" and the column to the right is labeled "Dose." The visual display of the Medication column can be somewhat confusing. There are two lines, both containing the name of the medication, one with a number and one without. Even though it was shared during training that the line containing the number is actually what is being dispensed by the pharmacy, not what is given to the patient, the line containing the number could easily be misunderstood to be the dosage. To make matters worse, the pharmacists input both the number of units and the volume in the dosage column ("5000 units/0.5 ml"). While this likely made perfect sense to the pharmacist and the pharmacist thought he was being helpful, this actually added to the confusion of the nurse. The nurse scans the screen from top to bottom and left to right. As she moved down the medication column and sees the order for heparin, she immediately sees "10,000 units/ml." At this point, she has already made up her mind that she is supposed to give 10,000 units. When she moves over to the right, her eyes are still tracked on the information in the row. She did not look back up at the column header to see that the information in the next column was actually the dose. The two columns presented similar information in the exact same manner, but the context between the two pieces of information are different. In the first column "10,000 units/ml" is the concentration of the medication. In the second column "5000 units/ml" is the dose, not the concentration. How could anyone expect the user to look at two sets of characters using the exact same pattern right next to one another and expect the user to know that one is in the context of a medication concentration and the other is the dose? It is a basic human factors principle that we attempt to find and apply patterns and build mental models to help us understand and solve problems [13, 15–17]. From a human factors design standpoint, the user interface could be improved to prevent this type of confusion.

If this had been a typical tablet or unit dose medication, this error may not have occurred. In most other scenarios, such as for all unit dose medications, the system checks the scanned drug (which includes the dose) against the drug database. If the bar code of the scanned drug does not match the drug/dose combination ordered for the patient, the system reacts by: (1) telling the user it is the wrong medication, or (2) requiring the user to scan additional units of the item (e.g., if multiple tablets are needed to complete the dose), or (3) alerting the user that the scanned medication needs to be split and only a partial amount of the scanned drug is to be administered. This system is designed such that when a medication is provided in a multidose container and that container is scanned, the computer does not have any way to know how much of that multidose container was actually administered to the patient and asks the user to document how much was administered. This is where the system design somewhat fails in the "5-rights" department. While the system displays the dose that should be given and allows the user to document the dose that was given, only the drug and the multidose container are checked for accuracy.

Solutions

How can these issues be rectified? As much as training needs to be designed to work for the trainer, it needs to work more so for the student. In the situation above, the orders for the patient were scheduled every 3 h to support around-the-clock training, so every class would have fresh orders and the trainer would not have to reset or clean-up between classes. This resulted in many orders displaying on the screen during training, which was overwhelming to the students. Ideally, the students should have only seen the number and types of orders that they are most likely to encounter in their own day-to-day operations. Also, the training should not try to address every possible scenario. The training should focus on the main concepts of the software, but then special scenarios should be addressed by the preceptors in the real world. There are big differences in the medication administration routines between the intensive care unit (ICU) and the CLC. If the training classes could be coordinated so that all students were from the ICU for example, then the training could focus mainly on intravenous medication administration. However, if the students' workplace assignments are varied, the class should be tailored to the students, keeping the information at a higher level and let the preceptors and super-users introduce the workplace variances in the context in which they will actually occur.

If system design is within your purview, you may consider designing the system such that the amount of medication being dispensed and the dose to be administered are not as easily confused as well as providing a way to ensure the amount of drug being administered from multidose containers can more accurately be communicated to the user. These are best accomplished by formal usability testing. The US National Institute for Standards and Technology [18] offers guidance to vendors and developers of health information technology such as how to integrate a framework of usability into software development and testing procedures incorporating standards developed by the International Organization for Standardization (ISO) [19].

Discussion

Implementing a BCMA system has been shown to reduce certain types of medication errors [4–9]. However, like other health information technology solutions, it comes with an inherent set of unintended consequences [17]. Some of the issues may be introduced by the implementation of the technology and some of the issues, which were there before the technology was implemented, were either not solved by the implementation or worse yet, aggravated by the technology.

Although BCMA is often considered a nursing application, it is really the endpoint of a fairly linear process that begins with the pharmacy (procuring medications) and relies on providers to properly enter orders and the pharmacy to process these orders. All of the pieces of those previous processes have to align perfectly in order for BCMA to even have a chance at being successful. If the pharmacy does not have a good system of entering medications into inventory as they are procured to

ensure bar codes are in the system to be recognized or relabeling the items with bar codes that work, the medications are not going to scan at the point-of-care and the users will almost immediately lose trust in the system.

Only after the processes that can adequately support BCMA have been put in place should the BCMA software be considered. The software must be designed to support the best process. If the software is designed around a poor process, problems inherent in the poor process will become overwhelmingly evident as soon as the technology is implemented [20]. This is why the software design must also incorporate human factors and usability principles.

Koppel et al. [14] categorized numerous workarounds employed by end-users to overcome barriers to proper BCMA use. These workarounds are typically in response to unintended consequences of a new solution. Unfortunately, it is often difficult to assess the potential consequences until a system is put in place. Adopting a framework to assess usability of any new solution and including end-users as well as staff specializing in informatics, such as an informatics nurse specialist, will go a long way in identifying potential issues before a solution is implemented [21]. For example, a usability study may have uncovered the potential issue noted in our heparin case before it was too late. The Office of the National Coordinator within the Centers for Medicare and Medicaid Services is attempting to ensure these principles are being applied by including them as requirements for certified EHR systems in the USA [11]. This is a key point since more and more hospitals are buying commercial solutions rather than building them in house. In theory, the certification process should help reassure customers that adequate safety enhanced design principles have been incorporated into the design.

Of course, certification only addresses the software design aspect and does not have any bearing on processes, training, proper competency assessment and the organizational resources needed to ensure a safe and successful implementation. Those factors absolutely must be considered with as much rigor as that used in the design of the system. Any organization that believes a BCMA system can be purchased, implemented, and successfully operated without a significant investment in the pre and post-implementation phases is surely doomed to fail.

Key Lessons Learned

- The importance of usability testing during software development cannot be overstated.
- Human factors principles (such as understanding how humans develop and apply mental models to solve problems) must be incorporated into the software design process as well as the processes that support BCMA implementation.
- Information should not always be expected to be considered common knowledge or retained in memory, e.g., when a system is used by people from varying backgrounds and disciplines, acronyms, abbreviations, and shorthand jargon can easily be misunderstood.

- Not every problem requires an elegant software solution. Sometimes the elegant software solution is nothing more than a patch placed over a poor process and fixing the true root cause is simply a matter of fixing the process.
- BCMA is a linear process that relies on many moving pieces. All of these moving parts must be in perfect synchronization for a successful implementation.
- BCMA is not a "plug and play" application; it requires proper training, competency, and ongoing resources to support the processes, application, and equipment needed to operate BCMA on a day-to-day basis.

References

1. Adams R. A short history of bar code [Internet]. Adams Communications; 2013 [updated 20 May 2013, cited 20 October 2014]. Available from: http://www.adams1.com/history.html.
2. Laurer G. Engineering was fun. May 2012. Published by lulu.com.
3. Mims E, Tucker C, Carlson R, et al. Quality-monitoring program for a bar-code-assisted medication administration. Am J Health Syst Pharm. 2009;66:1125–31.
4. Seibert HH, Maddox RR, Flynn EA, et al. Effect of barcode technology with electronic medication administration record on medication accuracy rates. Am J Health Syst Pharm. 2014;71(3):209–18.
5. Bonkowski J, Carnes C, Melucci J, et al. Effect of barcode-assisted medication administration on emergency department medication errors. Acad Emerg Med. 2013;20(8):801–6.
6. Szczepura A, Wild D, Nelson S. Medication administration errors for older people in long-term residential care. BMC Geriatr. 2011;11(1):82.
7. Poon EG, Hayes J, Churchill WW, et al. Effect of bar-code technology on the safety of medication administration. N Engl J Med. 2010;362(18):1698–707.
8. Helmons PJ, Wargel LN, Daniels CE. Effect of bar-code-assisted medication administration on medication administration errors and accuracy in multiple patient care areas. Am J Health Syst Pharm. 2009;66(13):1202.
9. DeYoung JL, Vanderkooi ME, Barletta JF. Effect of bar-code-assisted medication administration on medication error rates in an adult medical intensive care unit. Am J Health Syst Pharm. 2009;66:1110–5.
10. U.S. Department of Health and Human Services Food and Drug Administration. Guidance for industry: bar code label requirements questions and answers. Silver Spring, MD: Office of Communications; 2011.
11. United States. Medicare and Medicaid Programs: Electronic Health Record Incentive Program-Stage 2. Federal Register; 2012 Sep. Retrieved 24 October 2014 from the Internet at https://federalregister.gov/a/2012-21050.
12. Eisenhauer LA, Hurley AC, Dolan N. Nurses' reported thinking during medication administration. J Nurs Scholarsh. 2007;39:82–7.
13. Norman DA. The design of everyday things. New York: Basic Books; 1988.
14. Koppel R, Wetterneck T, Telles JL, et al. Workarounds to barcode medication administration systems: their occurrences, causes, and threats to patient safety. J Am Med Inform Assoc. 2008;15(4):408–23.
15. Chabris CF, Simons DJ. The invisible gorilla: and other ways our intuitions deceive us. New York: Crown Publishing Group; 2010.
16. Holden RJ, Rivera-Rodriguez AJ, Faye H, et al. Automation and adaptation: nurses' problem-solving behavior following the implementation of bar-coded medication administration technology. Cogn Tech Work. 2013;15(3):283–96.

17. Holden RJ, Brown RL, Alper SJ, et al. That's nice, but what does IT do? Evaluating the impact of bar coded medication administration by measuring changes in the process of care. Int J Ind Ergon. 2011;41:370–9.
18. National Institute for Standardization and Technology. Usability. 2010 [updated March 2014, cited 22 October 2014]. Available from: http://www.nist.gov/healthcare/usability/index.cfm.
19. International Organization for Standardization. About ISO. Geneva, Switzerland. 2014 [cited 22 October 2014]. Available from: http://www.iso.org/iso/home/about.htm.
20. Grigg SJ, Garrett SK, Craig JB. A process centered analysis of medication administration: identifying current methods and potential for improvement. Int J Ind Ergon. 2011;41:380–8.
21. Rojas C. The informatics nurse specialist role in electronic health record usability evaluation. Comput Inform Nurs. 2014;32(5):214–20.

Chapter 6
Errors Related to Outpatient E-Prescribing

Olufunmilola Abraham, Loren J. Schleiden, and Michelle A. Chui

Introduction

Outpatient settings (such as physician offices and retail pharmacies) are where the majority of healthcare is provided and medication errors are a substantial public health problem in these settings. Medication errors in outpatient settings are known to occur frequently, are often preventable, and can lead to adverse drug events and significant patient harm [1–3]. Electronic prescribing, commonly referred to as e-prescribing, has been introduced to many outpatient settings to reduce medication errors, thereby improving quality of care and patient safety. E-prescribing allows prescribers to electronically generate and send prescriptions to pharmacies [4]. The recommendation to adopt e-prescribing to reduce medication errors in the 2003 Medicare Modernization Act [5] and the 2006 Institute of Medicine (IOM) report "*Preventing Medication Errors*: *Quality Chasm*" [6] gave rise to widespread publicity of its role in enhancing patient safety. A core objective of the meaningful use policy for electronic health records (EHRs) required physicians to transmit more than 40 % of all prescription orders using e-prescribing in order to receive federal financial incentives [7]. These federal requirements for adherence to the meaningful use of EHRs resulted in an increase in adoption of e-prescribing in ambulatory care practices [8]. Between 2010 and 2013, the number of physicians using e-prescribing rose by 80 % [9], and 55 % of physicians in ambulatory practices now have

O. Abraham, Ph.D., M.S., B.Pharm. (✉) • L.J. Schleiden, B.S.
Department of Pharmacy and Therapeutics, University of Pittsburgh School of Pharmacy, 3501 Terrace Street, Pittsburgh, PA 15261, USA
e-mail: olufunmilola.abraham@pitt.edu; ljs24@pitt.edu

M.A. Chui, Pharm.D., Ph.D.
Social and Administrative Sciences Division, University of Wisconsin-Madison School of Pharmacy, 777 Highland Avenue, Madison, WI 53705, USA
e-mail: michelle.chui@.wisc.edu

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_6

e-prescribing capabilities [10]. Consequently, the number of e-prescriptions received in pharmacies has dramatically increased within the past 5 years, from 29 million in 2007 to more than 1.04 billion in 2013 [11].

The rapid adoption of e-prescribing was expected to facilitate prescription processing in pharmacies and improve ambulatory medication safety by preventing medication errors that result from poor handwriting, misspelling, or illegibility [3]. Unfortunately, medication error rates did not diminish as expected [12]. E-prescribing reduced certain types of errors, particularly those resulting from illegible handwriting [13], but it introduced new types of errors caused by design flaws in EHRs or workflow issues associated with its use [14–16]. An estimated 11 % of e-prescriptions sent from physician offices to community retail pharmacies are known to have errors such as wrong drug, wrong dosage, wrong dosage form, wrong directions, wrong duration of therapy, and wrong patient [12, 17, 18]. Pharmacists, who are recipients of e-prescriptions sent from physician offices, have suggested that omitted or inaccurate information accounts for most errors associated with e-prescribing [19].

A recent qualitative analysis of pharmacists' perceptions identified five themes when e-prescribing is not completely implemented or suboptimally designed. These include communication issues, workflow disruption, cost, poor design of technology, and opportunity for new errors [17]. Community retail pharmacy personnel have described some negative consequences of e-prescribing issues which include increase in time required to process e-prescriptions when inaccuracies and software design issues occur (drop-down menus, poor screen design, and automatic filling functions which may result in wrong, missing, or contradicting information in an e-prescription) [19]. In summary, further evaluation of the impact of e-prescribing on patient safety is warranted to ensure efficient and safe medication management in outpatient settings.

In this chapter, we present two case studies that illustrate some unintended consequences of e-prescribing in outpatient settings and what can be done to prevent them.

Case Studies

Case Study 1: Retrieving Incorrect E-Prescriptions

Clinical Summary

A 63-year-old man with multiple medical problems was seen by his primary care doctor for a routine follow-up appointment. Despite receiving psychotherapy, the patient admitted that he continued to struggle with anxiety. In light of these complaints, the primary care doctor elected to prescribe alprazolam, an antianxiety agent. The clinic had just implemented e-prescribing, so the physician reassured the patient that he did not need a paper prescription; he could simply go to the pharmacy to pick up his medications. While entering the prescription for alprazolam, the clinic nurse

inadvertently entered an additional medication, atenolol, a prescription intended for a different patient. Quickly recognizing her error, she deleted the atenolol order. Unfortunately, despite her efforts, the e-prescription went through to the pharmacy. When the patient arrived at the pharmacy, he was given both medications. Although he thought that it was a bit strange to receive two medications for his problem, he was willing to do anything to reduce his anxiety. Consequently, he took both medications as instructed. A few days later, during his cardiology appointment, the error was noted, and the atenolol was discontinued.

Analysis

The above case study, taken from a commentary by the Agency for Healthcare Research and Quality web morbidity and mortality reports [20], illustrates the unintended errors that can take place with e-prescribing and potentially result in patient harm. The clinic nurse entered the atenolol without checking the name and date of birth on the patient profile and then, after realizing her mistake, did not verify that the medication was deleted from the medication list before or after transmission to the pharmacy. In addition, the system allowed the nurse to prescribe on behalf of the doctor and transmit without first being verified by the doctor. Analysis of this case study depicts two primary sociotechnical issues that contributed to this e-prescribing error.

Communication Lapses

Insufficient Doctor–Patient Communication

During the clinic visit, there was insufficient information presented to the patient about the medication prescribed and sent to the pharmacy. For effective communication to occur, the patient could have been aware of the names or the number of medications to be picked at the pharmacy. The patient could also have received a paper artifact to enable verification of the medications once received at the pharmacy. There has been very limited research to better understand how physicians engage with patients about their medications during the e-prescribing process, how patients participate in this process, or how patients perceive e-prescribing's impact on the quality of care they receive. There is increasing awareness of the importance of engaging patients during care delivery [21], especially as health IT, such as e-prescribing, is being used by providers [22, 23]. Engaged patients are known to have higher levels of satisfaction, increased understanding of their care, more engagement in health-improving behaviors, and improved health outcomes [24–28]. As noted by Lapane and colleagues, introduction to computer hardware in the form of e-prescribing or EHRs into patients' examination rooms may be a barrier to effective communication between patients and providers by reducing eye contact and interpersonal connection [29]. As shown in Fig. 6.1, patients and their family caregivers need to be active participants throughout the e-prescribing process in outpatient settings, since it is known that patients' engagement in their care is critical for safety.

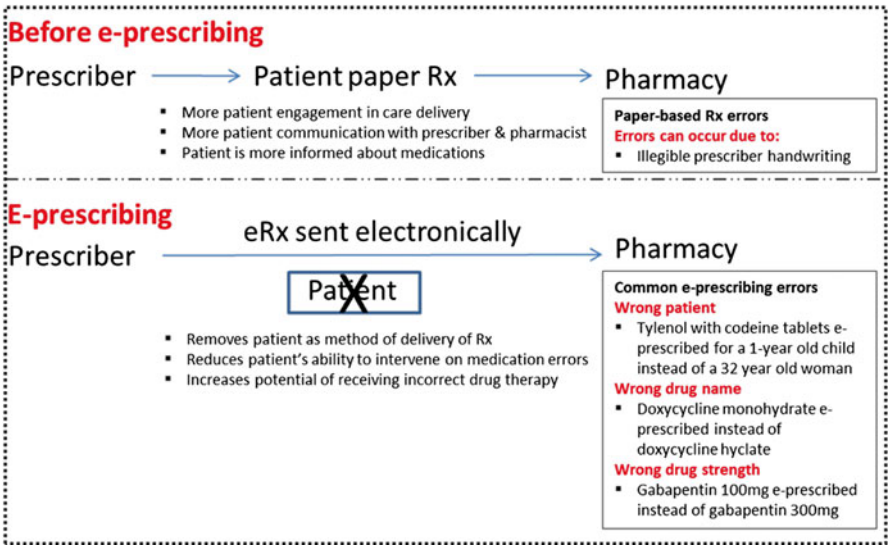


Fig. 6.1 E-prescribing: medication errors and need for patient engagement

Inadequate Clinic–Pharmacy Communication

Communication issues within the healthcare system can impact medication errors as more healthcare professionals gradually transition to electronic means of transmitting information. In this case, the clinic nurse failed to verify that the correct e-prescription information was received in the pharmacy by assuming that the e-prescription had been canceled. This error initially resulted from the inadvertent unwarranted medication (atenolol) for a different patient as the nurse entered the prescription for alprazolam. Nonetheless, adequate communication between the clinic nurse and the pharmacist through a phone call or online messaging would have ensured that the e-prescription was actually canceled and not dispensed to the patient. Because healthcare settings are busy and clinicians have significant time constraints, such communication to proactively prevent medication errors might be neglected. Verbal communication between prescribers and pharmacists to clarify e-prescribing information has been strongly recommended to help address the shortcomings of e-prescribing systems that can lead to medication errors [30].

Previous research has demonstrated that reduction in communication among healthcare professionals can increase the likelihood of errors that result from miscommunication and poor coordination of patient care [31–33]. Since e-prescribing has potential to be a two-way communication system between prescribers and pharmacists, effective communication with pharmacists who are usually the last safety check before ambulatory patients receive prescribed medication is necessary [17]. Currently, e-prescribing communication between prescribers and pharmacies is predominately unidirectional (from prescribers to pharmacists) and pharmacists typically rely on telephone and facsimile to clarify e-prescription discrepancies with

prescribers [17, 34, 35]. The pharmacy software does not provide complete seamless electronic communication with prescriber systems and the cost of this electronic communication is borne by the pharmacies which might limit its use [17]. E-prescribing systems that optimize communication and workflow within outpatient practices may help minimize both cost and the potential for the introduction of errors.

Training on E-Prescribing Capabilities

There is commonly a lack of knowledge about the true capabilities of health IT systems such as e-prescribing once they have been implemented in a practice setting. This usually results from insufficient training of users such as doctors, nurses, or pharmacists [36]. In this case study, the clinic had just implemented e-prescribing and the nurse assumed that, by deleting the e-prescription in the clinic computer, the e-prescription had automatically been deleted from the pharmacy system.

Several researchers have indicated that lack of adequate training is a cause of e-prescribing errors [37–39] and is a limitation of successful implementation of e-prescribing in healthcare settings [40]. In addition, researchers have recommended that ongoing training for users needs to be continually maintained and updated to reflect new clinical guidelines and to minimize unintended consequences such as medication errors [41]. Although potential cost of such training and employees and clinicians' willingness to undergo training might be barriers, the value of efficient training will be actualized over time.

Solutions

There are multiple ways this medication error could have been prevented throughout the prescribing process. A paper summary of prescriptions, including the name, indication, form, and directions, could help a patient to check that medications picked up at the retail pharmacy is what was initially prescribed. This patient might have questioned receiving multiple medications if the provider had given him a list of medications to be picked up at the pharmacy. A direct line of communication from provider to pharmacist can help facilitate increased communication regarding any possible errors, making it easier for the clinic nurse to check that her error had not reached the pharmacy. Enhanced training on e-prescribing features can clear up confusion on capabilities of e-prescribing systems.

Prescriber-focused interventions may be necessary to optimize medication safety; specifically, implementing some system functionalities can significantly prevent future e-prescribing errors. For instance, a forcing function that requires prescribers to review e-prescribing order entries before they are sent to pharmacies might have prevented the nurse from sending the atenolol e-prescription to the pharmacy. E-prescribing systems can also be modified to provide a return receipt of prescriptions from pharmacies to prescribers; this would have alerted the nurse that two prescriptions arrived at the pharmacy. The prescriber's system can also

require an additional step to confirm deletions with pharmacies. Although such functionality would be useful, it could add extra steps to a workflow that is already complicated by new technology.

In addition, prescribers need to continue to inform their patients of the name and appropriate use of medications even when e-prescribed. Providing and reviewing a current medication list with patients as part of the visit summary would also help to identify discrepancies when they occur before the patient leaves the office and picks up medications in the pharmacy. The sharing of patient care summaries at transitions of care as a requirement for meaningful use incentives should extend to include the pharmacist as a specialist in the care of each patient. Sharing such summaries can alert the pharmacist to treatments without appropriate diagnoses, as well as provide valuable clinical information to monitor management of chronic conditions with various drug therapies.

Case Study 2: Incorrect Drug Quantity Detected in Community Pharmacy

Clinical Summary

An e-prescription for antibiotic cephalexin was received at a community retail pharmacy for a 45-year-old woman being treated for a streptococcal infection. The e-prescription dosage directions stated "*take one capsule 4 times a day for 5 days*, *total quantity requested 40 capsules*." Upon inputting the e-prescription information into the pharmacy computer system, the community pharmacist noted a mismatch between the quantity the physician requested to be dispensed to the patient (40 capsules) and the actual quantity that the dosage directions implied (20 capsules). This presented confusion for the pharmacist who wondered "*is 40 capsules right or is 5 days right*?" The pharmacist proceeded to call the urgent care office from which the e-prescription had been sent to ask and double-check which was intended. The doctor eventually verified that the quantity requested was inaccurately calculated and the pharmacist should dispense the antibiotic as a 5-day supply (quantity 20 capsules).

Analysis

To protect privacy of patients and institutions, this case study has been modified to be fictional. In this scenario, the doctor's e-prescribing system allowed the prescriber to document conflicting drug quantity and dosing direction information. Incorrect drug quantity selection has been reported as a common problem with e-prescriptions received in community pharmacies [18]. These errors may be caused by inappropriate use of drop-down menus, auto-populate features, or a lack of final review of the e-prescription before being sent to the pharmacy. One study analyzed 3,850 computer-generated prescriptions from a commercial pharmacy chain in

three states and found that 11.7 % of the prescriptions contained some sort of error and 4 % contained errors that were serious enough to potentially cause an adverse drug event [42]. In this study, anti-infective agents, including antibiotics such as cephalexin, accounted for 17.3 % of medication errors. As described below, retail pharmacists have developed strategic approaches for detecting and addressing these e-prescription errors.

Detection of Medication Errors in E-Prescribing

A double-check of the e-prescription by the prescriber would help prevent a simple miscalculation from turning into a medication error. When an e-prescription with an error makes it to the pharmacy, pharmacy technicians are often the first staff members to encounter prescriptions sent to community pharmacies, and, as such, they have the first opportunity to identify discrepancies [34]. A pharmacy technician can be responsible for receiving the e-prescription, reviewing for accuracy, preparing orders, packaging and labeling medicine, assisting patients, and maintaining patient records [43]. Characteristics of pharmacy technicians, such as experience, certification, education, personality, and full- versus part-time status can impact how well a technician performs his or her duties, including the detection and resolving of e-prescribing errors.

Errors could be detected by the pharmacy technician throughout any of the steps they perform leading up to the pharmacist review, but it is the ultimate responsibility of the pharmacist to detect any errors through reviewing the order before it is dispensed to the patient. Most e-prescription errors in the community pharmacy are detected during the entering of information into the pharmacy computer system [34]. Some strategies used in community pharmacies by both pharmacists and pharmacy technicians include performing double-checks, printing the e-prescription to confirm information on the computer screen, and using colored pens to highlight pertinent information [34].

E-Prescription System Design

Provider Interaction with E-Prescribing Systems

Though e-prescribing systems are designed with usability in mind, some features of e-prescribing systems can facilitate unintended medication errors. For instance, auto-population features are meant to make updating an order faster and more convenient, but they can also lead to old, inappropriate, and/or inaccurate information remaining on repeated e-prescriptions if information is not updated properly [44]. This can occur when a prescriber might use old e-prescriptions to generate a refill prescription, which might have obsolete or inaccurate information. Drop-down menus also open up the possibility of accidentally choosing a wrong option, and scrolling features can lead to inadvertent changing of information entered.

Solutions

It is important for prescribers to develop best practices for using e-prescribing systems and to receive additional training to double-check or review prescription information before sending to the pharmacy to avoid mistakes. Pharmacy technicians would provide a great service by first detecting the error and possibly resolving the error before it reaches the pharmacist for final review. E-prescribing system features could be implemented so that miscalculations of drug dosages do not cause conflicting information on prescriptions. Another feature that would be useful in the case described is that of "auto-calculation." Auto-calculation could be applicable to e-prescriptions which require a set dose for a set amount of time to ensure that the quantity described in the e-prescription directions matches the quantity prescribed. Such built-in calculators would prevent incorrectly calculated drug quantities on e-prescriptions.

Summary

The 1999 IOM report "To Err is Human: Building a Safer Health System" shed light on the potential role of health IT in reducing harm and healthcare costs that result from medication errors [45]. However new technologies like e-prescribing may also introduce unintended consequences such as medication errors that can negatively affect patient safety. As more outpatient settings implement these systems, technology-related errors are increasingly evident and significant. To help prevent these errors, healthcare professionals need to track and report the errors even if they do not reach the patient through user-friendly reporting systems. Thus, aggregated error data can be analyzed, and shared with users and vendors to develop and identify redesign strategies and best practice guidelines. All stakeholders such as prescribers, pharmacists, and patients can play an important role in proactively mitigating these errors.

Key Lessons Learned

- E-prescribing has undergone a rapid and widespread implementation within the last decade, and is now used by a majority of prescribers.
- The implementation of e-prescribing has not reduced the occurrence of medication errors, as new errors specific to e-prescribing have emerged.
- Communication lapses, insufficient e-prescribing system training, and e-prescribing system design flaws can contribute to e-prescription errors reaching community pharmacies.
- Detection of e-prescription errors through pharmacist medication review of the prescription has become a key "last line of defense" to prevent medication errors from reaching patients.

- Engaged patients that are more active participants in their care may be more familiar with their self-care regimen and medications, and would be more likely to assist in detecting and preventing medication errors.

References

1. Galt KA, Rule AM, Clark BE, Bramble JD, Taylor W, Moores KG. Best practices in medication safety: areas for improvement in the primary care physician's office. In: Henriksen K, Battles JB, Marks ES, Lewin DI, editors. Advances in patient safety: from research to implementation (Volume 1: research findings). Rockville, MD: Agency for Healthcare Research and Quality (US); 2005. p. 101–27.
2. Bates DW, Boyle DL, Vander Vliet MB, Schneider J, Leape L. Relationship between medication errors and adverse drug events. J Gen Intern Med. 1995;10(4):199–205.
3. Marceglia S, Mazzola L, Bonacina S, Tarquini P, Donzelli P, Pinciroli F. A comprehensive e-prescribing model to allow representing, comparing, and analyzing available systems. Methods Inf Med. 2013;52(3):199–219.
4. Centers for Medicare & Medicaid Services. E-Prescribing overview 2013 (updated February 26, 2014). http://www.cms.gov/Medicare/E-Health/Eprescribing/index.html?redirect=/eprescribing. Accessed May 2014.
5. Bell DS, Friedman MA. E-prescribing and the medicare modernization act of 2003. Health Aff (Millwood). 2005;24(5):1159–69.
6. Institute of Medicine (US). Committee on Quality of Health Care in America. Crossing the quality chasm: a new health system for the 21st century. Washington, DC: National Academy Press; 2001. p. 337.
7. Grossman JM, Cross DA, Boukus ER, Cohen GR. Transmitting and processing electronic prescriptions: experiences of physician practices and pharmacies. J Am Med Inform Assoc. 2012;19(3):353–9.
8. Fischer MA, Vogeli C, Stedman MR, Ferris TG, Weissman JS. Uptake of electronic prescribing in community-based practices. J Gen Intern Med. 2008;23(4):358–63.
9. Hsiao C-J, Hing E. Use and characteristics of electronic health record systems among office-based physician practices: United States, 2001-2013. NCHS data brief, no 143. Hyattsville, MD: National Center for Health Statistics; 2014.
10. Patel V, Swain MJ, King J, Furukawa MF. Physician capability to electronically exchange clinical information, 2011. Am J Manag Care. 2013;19(10):835–43.
11. Surescripts. 2013 National Progress Report and Safe-Rx Rankings. http://surescripts.com/docs/default-source/national-progress-reports/surescripts_2013_national_progress_report.pdf?sfvrsn=2. Accessed 20 Nov 2014.
12. Gilligan AM, Miller K, Mohney A, Montenegro C, Schwarz J, Warholak TL. Analysis of pharmacists' interventions on electronic versus traditional prescriptions in 2 community pharmacies. Res Social Adm Pharm. 2012;8(6):523–32.
13. Flynn EA, Barker KN, Carnahan BJ. National observational study of prescription dispensing accuracy and safety in 50 pharmacies. J Am Pharm Assoc. 2003;43(2):191–200.
14. 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):104–12.
15. Ash JS, Sittig DF, Dykstra R, Campbell E, Guappone K. Exploring the unintended consequences of computerized physician order entry. Stud Health Technol Inform. 2007;129(Pt 1):198–202.
16. Ash JS, Sittig DF, Dykstra RH, Guappone K, Carpenter JD, Seshadri V. Categorizing the unintended sociotechnical consequences of computerized provider order entry. Int J Med Inform. 2007;76 Suppl 1:S21–7.

17. Nanji KC, Rothschild JM, Boehne JJ, Keohane CA, Ash JS, Poon EG. Unrealized potential and residual consequences of electronic prescribing on pharmacy workflow in the outpatient pharmacy. J Am Med Inform Assoc. 2014;21(3):481–6.
18. Hincapie AL, Warholak T, Altyar A, Snead R, Modisett T. Electronic prescribing problems reported to the Pharmacy and Provider ePrescribing Experience Reporting (PEER) portal. Res Social Adm Pharm. 2014;10(4):647–55.
19. Ducker M, Sanchez C, Taylor SR. Pros and cons of e-prescribing in community pharmacies. US Pharmacist. 2013;8(38):P&T suppl 4–7.
20. AHRQ. E-prescribing: E for error? 2012. http://webmm.ahrq.gov/case.aspx?caseID=260. Accessed 26 Jun 2014.
21. Carman KL, Dardess P, Maurer M, Sofaer S, Adams K, Bechtel C, et al. Patient and family engagement: a framework for understanding the elements and developing interventions and policies. Health Aff (Millwood). 2013;32(2):223–31.
22. Bird AP, Walji MT. Our patients have access to their medical records. Br Med J (Clin Res Ed). 1986;292(6520):595–6.
23. Schleiden LJ, Odukoya OK, Chui MA. Older adults' perceptions of e-prescribing: impact on patient care. Perspect Health Inf Manag. 2015;12(Winter):1–15.
24. Nelson DE, Kreps GL, Hesse BW, Croyle RT, Willis G, Arora NK, et al. The Health Information National Trends Survey (HINTS): development, design, and dissemination. J Health Commun. 2004;9(5):443–60. Discussion 81-4.
25. Street Jr RL, Millay B. Analyzing patient participation in medical encounters. Health Commun. 2001;13(1):61–73.
26. Tang PC, Lansky D. The missing link: bridging the patient-provider health information gap. Health Aff (Millwood). 2005;24(5):1290–5.
27. Tang PC, Newcomb C. Informing patients: a guide for providing patient health information. J Am Med Inform Assoc. 1998;5(6):563–70.
28. Verlinde E, De Laender N, De Maesschalck S, Deveugele M, Willems S. The social gradient in doctor-patient communication. Int J Equity Health. 2012;11:12.
29. Lapane KL, Dube CE, Schneider KL, Quilliam BJ. Misperceptions of patients vs providers regarding medication-related communication issues. Am J Manag Care. 2007;13(11):613–8.
30. Odukoya OK, Chui MA. E-prescribing: characterisation of patient safety hazards in community pharmacies using a sociotechnical systems approach. BMJ Qual Saf. 2013;22(10):816–25.
31. 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(5):547–56.
32. Gallagher RM, Gallagher HC. Improving the working relationship between doctors and pharmacists: is inter-professional education the answer? Adv Health Sci Educ Theory Pract. 2012;17(2):247–57.
33. Bodenheimer T, Grumbach K. Electronic technology: a spark to revitalize primary care? JAMA. 2003;290(2):259–64.
34. Odukoya OK, Stone JA, Chui MA. How do community pharmacies recover from e-prescription errors? Res Social Adm Pharm. 2013;10(6):837–52.
35. Warholak TL, Rupp MT. Analysis of community chain pharmacists' interventions on electronic prescriptions. J Am Pharm Assoc. 2009;49(1):59–64.
36. Odukoya OK, Chui MA. Relationship between e-prescriptions and community pharmacy workflow. J Am Pharm Assoc. 2012;52(6):e168–74.
37. Rupp MT, Warholak TL. Evaluation of e-prescribing in chain community pharmacy: best-practice recommendations. J Am Pharm Assoc. 2008;48(3):364–70.
38. Redwood S, Rajakumar A, Hodson J, Coleman JJ. Does the implementation of an electronic prescribing system create unintended medication errors? A study of the sociotechnical context through the analysis of reported medication incidents. BMC Med Inform Decis Mak. 2011;11:29.

39. Odukoya OK, Stone JA, Chui MA. Barriers and facilitators to recovering from e-prescribing errors in community pharmacies. J Am Pharm Assoc (2003). 2015;55(1):52–8.
40. Hahn A, Lovett A. Electronic prescribing: an examination of cost effectiveness, clinician adoption and limitations. Univ J Clin Med. 2014;2(1):1–24.
41. Devine EB, Wilson-Norton JL, Lawless NM, Hansen RN, Hollingworth W, Fisk AW, et al. Implementing an ambulatory e-prescribing system: strategies employed and lessons learned to minimize unintended consequences. In: Henriksen K, Battles JB, Keyes MA, Grady ML, editors. Advances in patient safety: new directions and alternative approaches (Vol 4: technology and medication safety). Rockville, MD: Agency for Healthcare Research and Quality (US); 2008. p. 185–98.
42. Nanji KC, Rothschild JM, Salzberg C, Keohane CA, Zigmont K, Devita J, et al. Errors associated with outpatient computerized prescribing systems. J Am Med Inform Assoc. 2011;18(6):767–73.
43. Odukoya OK, Schleiden LJ, Chui MA. The hidden role of community pharmacy technicians in ensuring patient safety with the use of e-prescribing. Pharmacy. 2015;3(4):330–343.
44. Odukoya OK, Stone JA, Chui MA. E-prescribing errors in community pharmacies: exploring consequences and contributing factors. Int J Med Inform. 2014;83(6):427–37.
45. Kohn LT, Corrigan JM, Donaldson MS. To err is human: building a safer health system. Washington, DC: Institute of Medicine; 2000.

Chapter 7
Errors Related to Alarms and Monitors

JoAnne Phillips

Background

The presence of technically complex medical devices in the clinical environment has increased significantly over the past three decades. In 1983, critical care units averaged six different types of clinical alarms; by 2011, that number had increased to 40 [1, 2]. ECRI Institute, a nonprofit organization that researches the safety and quality of medical devices, procedures, and drugs, has named alarm hazards as the number one health technology safety hazard 4 years in a row [3].

Clinical alarms are designed to notify staff of a change in the patient's physiologic status or the failure of a medical device [4]. Medical devices obtain data from sensors that measure biophysical signals, interpret the data, and convert it to information for clinicians to use in making decisions. Many medical devices, such as cardiac monitors, are designed to filter the data through pre-programmed settings to notify staff when the data are outside set parameters by sounding an alarm. Clinicians are challenged by the high sensitivity and low specificity associated with clinical alarms that result in an overabundance of non-actionable alarms [5]. Many reports state that 86–99 % of clinical alarms are non-actionable and thus considered nuisance alarms [5–8].

The high percentage of nuisance alarms may result in staff disabling, silencing or ignoring alarms [7]. These actions may result in actionable alarms going unnoticed, increasing the risk for patient harm. Staff may develop a mistrust of alarms as a result of the overwhelming number of alarms. If a clinician believes that the alarm is accurate 90 % of the time, they will respond 90 % of the time. If they believe that it will be accurate 10 % of the time, they will answer it 10 % of the time [9].

J. Phillips, D.N.P., R.N., C.P.P.S. (✉)
Penn Care at Home, 150 Monument Rd, Bala Cynwyd, PA 19004, USA
e-mail: joanne.phillips@uphs.upenn.edu

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_7

Alarm-Related Harm Data

Alarm-related harm data are reported to several databases; two key examples are the manufacturer and user facility device experience (MAUDE) database of the Food and Drug Administration (FDA) and the sentinel event database at the Joint Commission (TJC). Reporting to the MAUDE database is mandatory for manufacturers and users of medical devices when there is a reasonable suspicion that their device has contributed to patient harm or death [10]. Reporting to the TJC sentinel event database is voluntary; thus adverse events are believed to be under-reported, possibly by a factor of ten [11].

From 2005 to 2010, 566 reports of alarm-related deaths were submitted to the MAUDE database. Follow-up investigations often revealed that users were not familiar with how the monitoring equipment worked or had not checked the monitor's alarm status [10].

From 2009 to 2012, ninety-eight alarm-related sentinel events were reported to The Joint Commission (TJC). Harm from the reported sentinel events included 80 deaths, 13 patients with permanent loss of function, and 5 patients with unexpected additional care or extended stay [11].

Contributing Factors to Alarm-Related Patient Harm

Alarm fatigue is the most common factor contributing to alarm-related patient harm [11]. It is defined as the "limited capacity to identify and prioritize alarm signals, which has led to delayed or failed alarm responses and deliberate alarm deactivations" [12]. Recently, there has been a tremendous focus in the literature on the clinical alarm [1, 2, 5, 13–15].

Other contributing factors include alarms that are not customized to individual patients, inadequately trained staff, inadequate nurse staffing, alarms not integrated with other technology, and equipment malfunction [5, 11].

Alarm Hazards and Potential Failures

Clinical alarm management is a complex process with multiple vulnerabilities. ECRI has identified a number of alarm hazards, including alarm activation, alarm load, alarm notification process, alarm content, alarm escalation, policies, practice, and education [14].

Alarm Activation

Once a variable or physiologic data point crosses a threshold or alarm limit, an alarm should be activated. The first failure point in the complex alarm process is the failure of an alarm to sound or be activated. If the alarm does not activate, the clinician must

investigate and understand whether the alarm limit was set correctly to notify the clinician of a change in condition or a mechanical failure [14]. Activation failure could be associated with a lack of training or equipment failure [11]. The case study discussed later in the chapter on ECG bedside monitor signal disruption is an example of a failure of alarm activation.

Alarm Load

Patients and the staff caring for them may be exposed to as many as 700 alarms in a day [7], which creates an overwhelming alarm load for the patient and the nurse. The large percentage of non-actionable or nuisance alarms (86–99 %) creates a cognitive burden for clinicians, who have to process every alarm. Alarm fatigue is an adaptive mechanism to manage the complex cognitive burden associated with alarms [16]. The high number of alarms is indicative of a large number of nuisance or non-actionable alarms, potentially resulting from a lack of customization of the alarms.

Alarm Notification Process

There are several mechanisms for clinicians to be notified of an alarm, each with a potential for failure. Once an alarm activates, the information must be sent either directly to the clinician who is going to respond or to the backup responder. Alarm notification can be direct, where the clinician hears or sees the alarm as it is occurring. Notification can be indirect, from a middleware device, such as a pager, voice badge, or smartphone, or from a telemetry technician in a remote location. Communication about an alarm must be clear and direct to avoid missing important messages. Technology failures, such as the alarm volume being turned down, the staff forgetting to connect a device, or middleware failure, may create a failure at this stage [1, 2, 5, 13, 15]. There are four barriers to the alarm notification process.

The first barrier is an inadequate notification process. If an alarm sounds and staff with primary and backup responsibility do not acknowledge it, an appropriate response will not occur. The second barrier is failure to use technology correctly. In the case study on middleware failure, staff may be unfamiliar with how to operate the pagers correctly, which contributes to their inability to recognize device failure. Limitations of technology are the third barrier, and include battery failure or network failure. Environment is the final barrier. The environment or physical space can influence the clinician's ability to hear or acknowledge an alarm. Long hallways and structural barriers may result in a delay in the nurse or other clinician recognizing and responding to an alarm [14].

Alarm Content

The alarm must contain enough information for the clinician to know how to respond. Important data points in the alarm content include which patient is alarming, the patient's location, and the priority of the alarm [14]. If an alarm sounds at the central station, the clinician must be able to look at the monitor and know the identification of the patient and the patient's location. If an alarm is sent over a middleware device, such as a pager or smartphone, the device may be able to transmit the electrocardiographic tracing for the nurse to review. Clinicians must also be able to discriminate between the audible content of different alarms to establish the priority of the alarms. Discrimination of alarm sounds is an important part of education and training.

Alarm Escalation/Backup

Alarm response protocols must be developed for each clinical area. Notification of an alarm must be delivered to the clinician who has primary responsibility for responding to the specific alarm. There will be situations where staffs with primary responsibility are not able to respond, in which case a plan for backup responsibility must be part of the alarm response protocols. Backup notification can be sent to another clinician on the unit, the charge nurse, the nurse manager or other leader, or all staffs [8, 14]. Staffs need to be educated on alarm response protocols to understand their primary and backup responsibilities.

Policies, Practice, and Education

Improving the safety of clinical alarm systems is now a Joint Commission National Patient Safety Goal (NPSG) 6.01.01; the associated elements of performance define key requirements for policies, practice, and education associated with clinical alarm (Table 7.1) [17].

Case Study 1: Middleware Failure

To support the acuity and unique needs of its patients, a large academic medical center is committed to a model of care in which patients are aggregated to specific patient care units where the nurses and other team members are experts in the care of the patient's primary diagnosis. To support that model, telemetry monitoring is available on every floor with nurses accountable for the telemetry monitoring of their own patients. Two other commonly seen telemetry models use telemetry technicians, either on the clinical unit or in a common area, often referred to as a war room. In the model at the Hospital

Table 7.1 National patient safety goal 6.01.01

Improve the safety of clinical alarm systems—elements of performance
1. Leaders establish alarm system safety as a hospital priority.
2. Identify the most important alarm signals to manage based on the following: • Input from the medical staff and clinical departments • Risk to patients if the alarm signal is not attended to or if it malfunctions • Whether specific alarm signals are needed or unnecessarily contribute to alarm noise and alarm fatigue • Potential for patient harm based on internal incident history • Published best practices and guidelines
3. As of January 1 2016, establish policies and procedures for managing the alarms identified in EP 2 above that, at a minimum, address the following: • Clinically appropriate settings for alarm signals • When alarm signals can be disabled • When alarm parameters can be changed • Who in the organization has the authority to set alarm parameters • Who in the organization has the authority to change alarm parameters • Who in the organization has the authority to set alarm parameters to "off" • Monitoring and responding to alarm signals
4. Checking individual alarm signals for accurate settings, proper operation, and detectability
5. As of January 1 2016, educate staff and licensed independent practitioners about the purpose and proper operation of alarm systems for which they are responsible

The Joint Commission (2015). Hospital: 2015 National Patient Safety Goals. Retrieved from http://www.jointcommission.org/assets/1/6/2015_NPSG_HAP.pdf (November 14, 2015)

of the University of Pennsylvania (HUP), when a telemetry alarm is activated, the nurse is alerted via pager (middleware device) that the patient has violated the set alarm parameter and the nurse is responsible to respond to the alarm.

After an upgrade of the telemetry system, a number of unscheduled telemetry pager downtimes occurred over a 3-month period, placing the patients at risk. The alarm at the central station is the primary notification. The notification is carried through a gateway system (Emergin) to the telemetry pagers, and is considered an alert (i.e., secondary notification). The clinical nurses rely on the pager for notification as they are often away from the central station. When pager failures occurred, nursing staffs were not immediately aware, and continued to rely on notification from the pagers for their telemetry alarms. With the diffusion of telemetry on every unit, pager failures can occur on one floor, in one building, or on all 12 units across five buildings that rely on pagers for notification.

Once a pager failure is identified on one unit, all units require pager testing by the charge nurses to ensure that their pagers are functioning. The impact of the downtime is contained in a summary of the reported pager failures over a 3-month period, including the causes of failures, the number of units affected, the hours the pagers were down, and the support required to maintain the standard of care (Table 7.2). These failures were brought to the attention of the Patient Safety Steering Committee, who suggested a Failure Modes and Effect Analysis (FMEA) to identify potential failures in this complex system [18]. FMEA is a strategy for proactive risk assessment once a potentially high risk or complex process is identified.

Table 7.2 Unscheduled telemetry pager downtime: 3 months of data

Reason for failure	Number of clinical units effected	Time period of failure Supportive resources
Month 1		
Emergin system incorrectly programmed, resulting in alerts to the pagers every 30 s	12 units (all units)	Average time out of service in month one: 5 h/each occurrence
Server failure, no communication, no pages	1 unit	
Cause not identified—no pages	2 units	
Month 2		
Firewall failure—no pages	2 units	Total time down, 40 h. Required RN monitor watchers 24/7
Month 3		
Firewall re-boot caused pager failure	2 units	8 days of intermittent issues; total of 40 h; intermittent monitor watchers required
Alert messages, but no real issue	2 units	
"Emergin Disconnect" message, but paging was functional (occurred twice)	2 units	
Alarms in the alarm log, but no message to pagers	1 unit	

Table 7.3 Roles of stakeholders

Manager of nursing technology
Director of nursing systems
Nursing administrative coordinator
Coordinator of nursing quality and patient safety
Director of clinical engineering
Associate director of clinical engineering
Clinical engineering technologist
Associate executive director
Information security engineer
Network engineer
Entity information officer
Clinical nurses (4)

Steps in FMEA

Assemble the Team. The complexity of the upgraded telemetry system required the team to have broad representation. The upgraded system increased the complexity of signal processing and required the engagement of a number of stakeholders from information technology to enable the team to map out the process and identify the failure modes and potential effects. Including diverse roles on the team members was essential to success (Table 7.3).

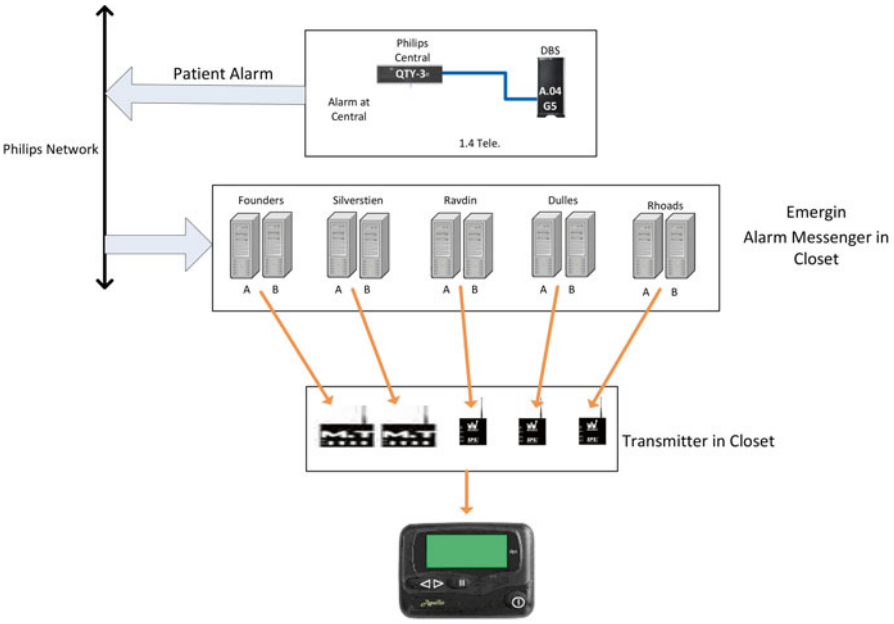


Fig. 7.1 Emergin paging (previous configuration)

Map the Process

To map the process, the team began with the process before the upgrade (Fig. 7.1), and then mapped the process after the upgrade (Fig. 7.2), which included the potential failure modes.

Hazard Analysis

Using the steps within the process map, a hazard analysis was calculated to determine potential failure modes. The FMEA worksheet (Table 7.4) describes each step, the associated potential failure modes, the potential effects of each failure, and the risk priority number (RPN). After mapping out the process, the team met several times to identify the potential failure modes and effects, and to calculate the risk priority numbers. The team ranked almost all the failure modes with a severity of four (the highest score is five) because the effects were the same, no paging. The step with the most failure modes was the alarm to telemetry pager, with five different failure modes. In calculating the RPN, these failure modes had the top RPNs, which ranged from 24 to 48.

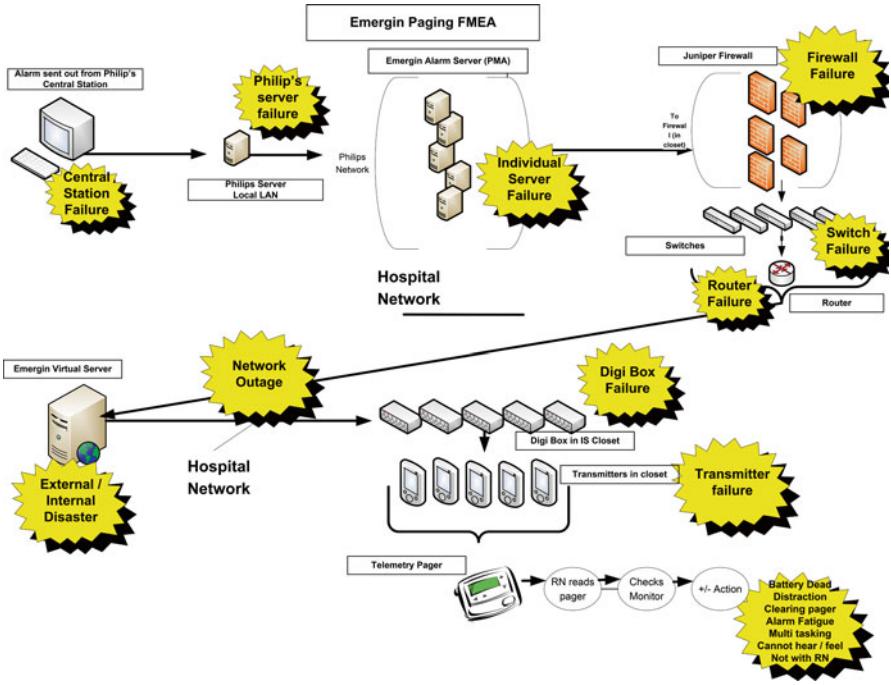


Fig. 7.2 Emergin paging system (new and modified configuration) created by Renee Herkloz, MSN, RN. Used with permission

Action Plan

An action plan was developed to enable nursing leadership to take action once pager failure was recognized (Fig. 7.3). One of the challenges was to identify the breadth of the issue, to understand whether the pager failure was on one floor, one building, or across all the floors. The process map helped to identify where the technology failure was based on whether pagers fail on one unit, in one building, or across all units/buildings. Once the pager failure was identified and clinical engineering is contacted, a separate action plan was put into place (Table 7.5). Communication of both action plans was provided through multiple venues. For nursing, communication was provided through huddles, Nursing Quality and Patient Safety Council, Nursing Leadership Council, and patient safety walkrounds. Clinical engineering and information technology staff provided communication of the action plan during staff meetings.

Table 7.4 FMEA focus: Telemetry Emergin paging unscheduled downtime

Column 1	Column 2	Column 3	C4	C5	C6	C7
Step or link in process	List all potential failure modes	Potential effect(s) of failure (if failure occurs, what are the consequences)	Severity (1–5)	Likelihood (1–5)	Detectability (1–5)	RPN (C4 × C5 × C6)
Alarm sent out from Philips Central station	Central station failure	No paging No central station monitoring	5	2	1	10
Philips server receives alarm	Philips server failures	No paging—limited amount of events stored	4	2	3	24
Alarm to Emergin server (building specific servers in equipment closet)	Individual Emergin server failure	No paging—affects entire building	4	2	4	32
Alarm through Juniper Firewall	Firewall failure	No paging—affects entire building	4	2	1	8
Sent to Emergin Virtual Server through network	Network outage	Switch—no paging; unit level Router—no paging; global effect	4	2	1	8
Emergin server	Internal/external disaster	No paging	4	2	1	8
Alarm back through hospital network	Network outage	No paging	4	2	1	8
Message to on-site Digi Box	Digi Box failure	No paging	4	2	1	8

(continued)

Table 7.4 (continued)

Column 1	Column 2	Column 3	C4	C5	C6	C7
Step or link in process	List all potential failure modes	Potential effect(s) of failure (If failure occurs, what are the consequences)	Severity (1–5)	Likelihood (1–5)	Detectability (1–5)	RPN (C4×C5×C6)
Alarm to telemetry pager	Pager battery dead	Inadequate response	4	3	3	36
	Alarm fatigue	Inadequate response	4	4	3	48
	RN multi-tasking	Inadequate response	4	4	3	48
	Pager not with RN	Inadequate response	4	2	3	24
	Cannot hear/feel pager	Inadequate response	4	2	3	24

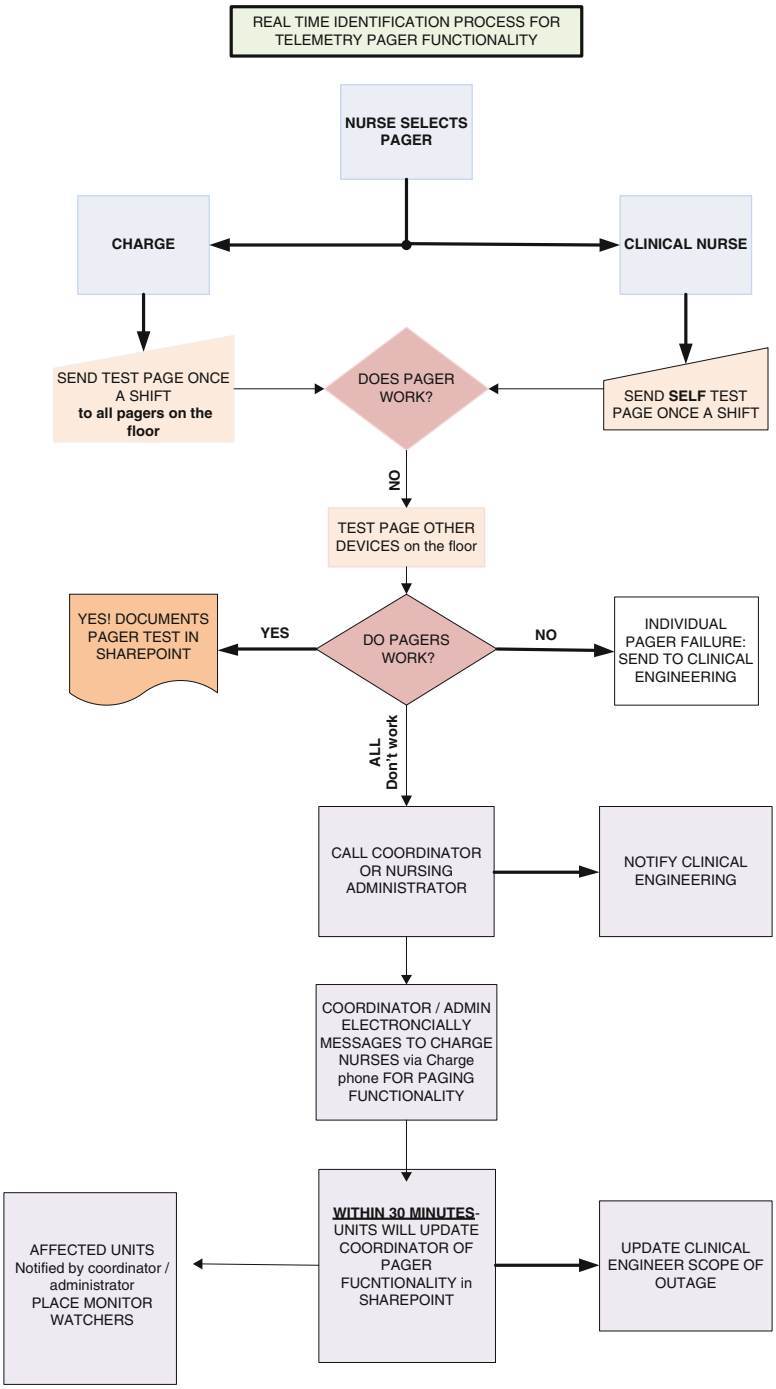


Fig. 7.3 RN pager failure identification process. Created by Renee Herkloz, MSN, RN. Used with permission

Table 7.5 Pager failure

Issue	Action
No paging	1. Follow the pager failure algorithm 2. Verify no paging by using orchestrator, remote access (VM) or attempt a test page at the PIIC 3. Note any paging-related message on PIIC application (top)
Verify if paging is down on one alarm server (PMA) or all	1. Log into PMA server in affected building 2. If unable to log in, restart PMA server 3. If logged in, document any error messages or notices 4. Remote into VM (if unable to remote in, all PMAs are down) 5. Visually check all buildings or all PMAs
If all paging down, all buildings	1. Virtual server is issue, call IS, let them know all paging is down, virtual server or network is the issue
If one alarm server (PMA) is down, and you verified other floors are getting paging	1. Check application, make sure Alarm Messenger (red clock) is running and paging service is running (check top left, there is a "Stop" and a "Go" icon; Stop icon should be highlighted) 2. If disconnected from VM server, alarm messenger application will continue to attempt to connect 3. Check Orchestrator application for paging activity and/or queued messages 4. Check hardware, make sure that Digi Box is connected and has one red light for power and one green light for connection, Ping IP Address 5. Check Firewall for power and indicator lights 6. Check transmitter for power (power light)
If PMA in closet cannot connect to VM	1. Call IS help desk and ask for a conference line, you'll need security for the firewall and networking for server 2. Networking (a) Ping the VM server IP (include the IP address) • Fails: server issue (b) Ping the gateway • Fails: the link is down to the port (c) Ping the PTP server • Issue with route through network security (d) Ping the firewall 3. Call Philips/Emergin 800 number; provide site ID number) or provide IS with Philips/Emergin support number to get Emergin technician added to the conference line

NOTE: Always keep the appropriate nursing staff up to date on any problems or resolutions
Orchestrator: Application on the server that allows review of all messages from the VMA
VMA Virtual machine
PMA Patient message alarm

Case Summary

Because of the physical layout of the units, nursing staffs depended on the middleware to notify them of alarms from the telemetry monitors. One of the challenges was that pager failures occurred in the middle of the shift and staffs were not immediately aware. All members of the interdisciplinary team learned that the process for notification had become much more complex with the telemetry upgrade. After the development of the new process, there were no further pager failures, but all team members felt confident that a clear process was developed to respond if the situation arose.

Case Study 2: ECG Bedside Monitoring Signal Disruption

This case study took place in a unit devoted to the care of patients in an observation status. In this 18-bed unit, all rooms are equipped with multiparameter monitors that allow staff to intermittently or continuously monitor electrocardiogram, pulse oximetry, and respiratory rate. Noninvasive blood pressure could be set to cycle at predetermined intervals from 2 min to 2 h. Patients with an evidence-based indication for cardiac monitoring are continuously monitored while in the observation unit. The monitors have a smaller monitor (Philips *X*2 monitors) that detaches from the parent monitor that enables the patient to walk to the bathroom or walk in the hallways with ECG signals continuously transmitting to the central monitor. Once the *X*2 is disconnected from the parent monitor, the transmission of the signal to the central station transitions from wired to wireless.

Observation Unit Signal Loss

Nurse staffing in the Emergency Department Observation Unit (EDOU) is a 4:1 ratio. All staff attended the basic dysrhythmia course and were assessed for their competence in cardiac monitoring. Staff also completed an online training module that focused on the physiologic monitors including training on the Philips *X*2, MP50 and MP70 monitors. Staff noticed that the cardiac monitor tracings transitioned from the normal ECG tracing to a checkerboard tracing, which would last for 1–2 min, during which time there was no transmission of an ECG tracing, and thus no potential for alarms (Fig. 7.4). Since there was no alarm, the staff only knew it was happening if they happened to be looking at the monitor at the minute it happened. There was also an intermittent issue with transmission of the signals from the *X*2 monitors to the central station once the *X*2 was disconnected from the parent monitor. So if the patient was disconnected and in the bathroom, there might not be a signal transmission. The staff understood that there was an anticipated

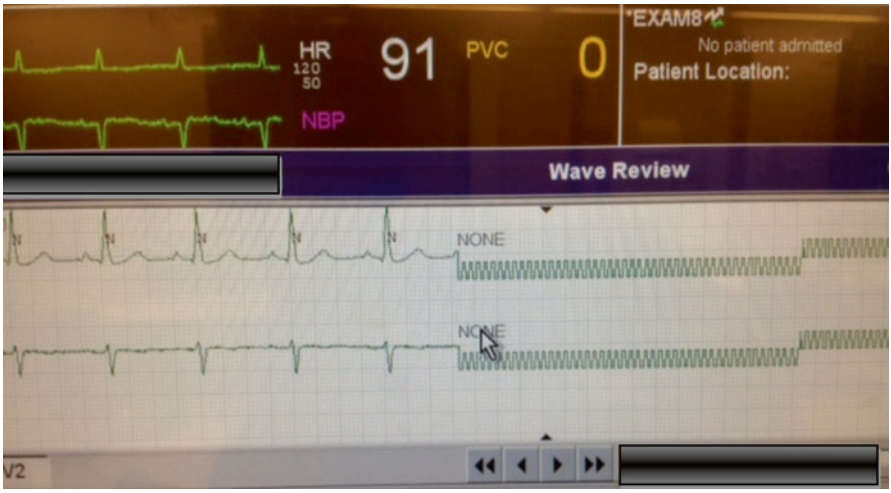


Fig. 7.4 Transition from ECG tracing to checkerboard pattern

crossover time, which was anticipated to be up to 1 min, to allow the transmission of the ECG signal to cross over from transmitting from the wired parent monitor to transmitting from the wireless *X*2 to the central station. Staff was observing longer periods of transition time, and at times the wireless signal did not transmit to the central station.

Identifying the Issue

Over the first month, staff identified several events during which time the ECG tracing transitioned from a normal to a checkerboard pattern. An interdisciplinary team was formed, which included staff from the Emergency Department Observation Unit (EDOU), clinical engineering, nursing technology, hospital administration, and Philips Medical. An action plan was developed to help direct activities to identify the underlying cause of the signal loss.

Investigation

The initial action plan included making simple practice changes to ensure that there was not a simple solution to the signal transmission issue. Key practice changes were immediately implemented to ensure that there was a standardized approach to cardiac monitoring (Table 7.6).

Table 7.6 Nursing practice changes

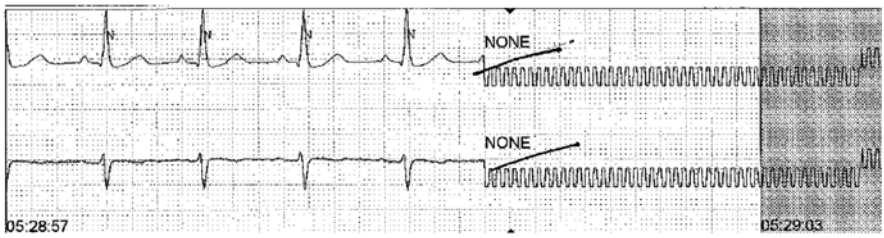
Electrode management
Remove excess hair with clippers
Skin preparation with soap and water
Dry/abrade skin with gauze
Change electrodes every 24 h
Electrodes managed per the manufacturer's recommendation
Management of *X*2 monitors
Monitors are to be disconnected and reconnected by EDOU staff only
Monitors are not to be used for transport off the unit
Once the monitor is disconnected, staffs have been educated to ensure that the wired tracing hands off to the wireless tracing

Table 7.7 Data collection

Time	Monitor display	Alarm review From bedside monitor	Clinical correlation
4:45:00	Checkerboard		
4:46:11		*X*2 monitor Unplugged	Patient was disconnected by the nursing assistant to walk to the bathroom. Nursing assistant checked to ensure that there was a tracing on the monitor
4:46:13		Tele inop	
4:48:58	"No data from bed"		Patient back in room. On *X*2, not connected to parent monitor
5:20:00			RN noted that sector at the central monitor where the EKG signal was displayed said "no signal," went to room, reconnected the *X*2, and the issue was resolved. Data review from the central station from 4:48–5:24
5:28:57	Checkerboard		
5:29: 22		*X*2 monitor Unplugged	Patient disconnected and walked to bathroom
5:29:26		Tele inop	

Data Collection

The first step was to create a timeline with clinical correlation, to understand what was happening with the patient as the displays were changing (Table 7.7). The next step was to capture the transition of the ECG tracing from normal to checkerboard and return to normal (Fig. 7.5). It was also helpful to visualize the presentation at the central station (Fig. 7.6). The final step was to conduct an alarm analysis from the bedside monitor (Fig. 7.7). Each event was summarized and submitted to Philips Medical for analysis.



Return to EKG tracing

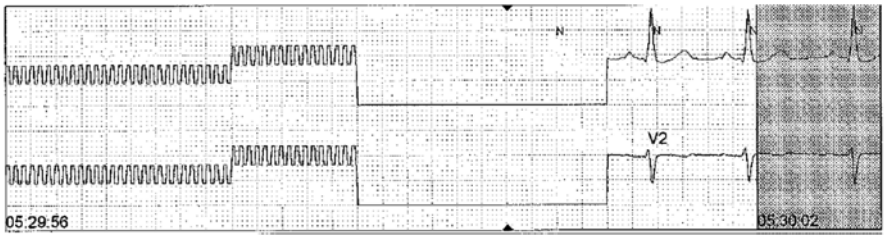


Fig. 7.5 Starting of checkerboard

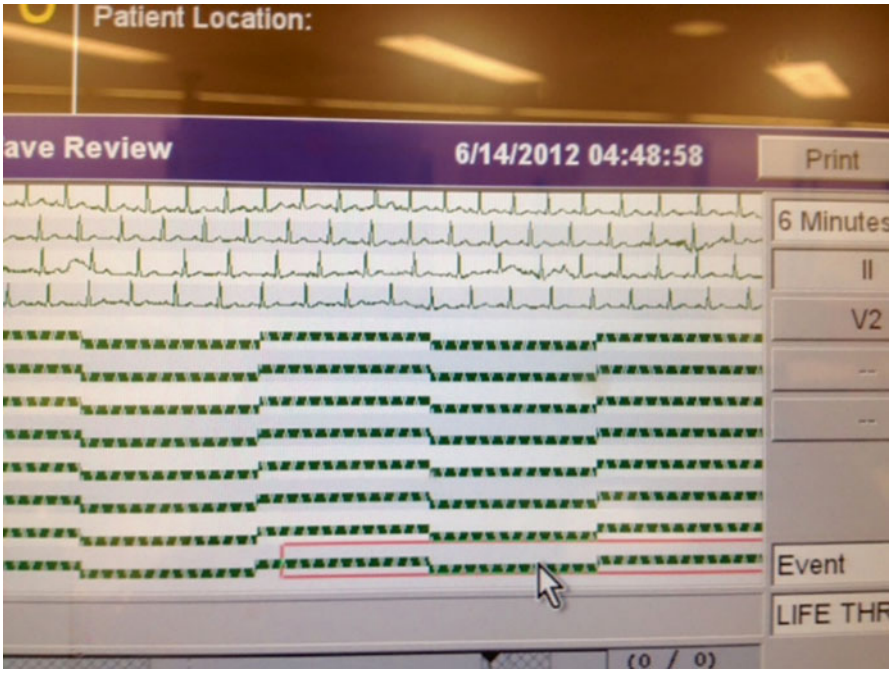


Fig. 7.6 Tracing at central station

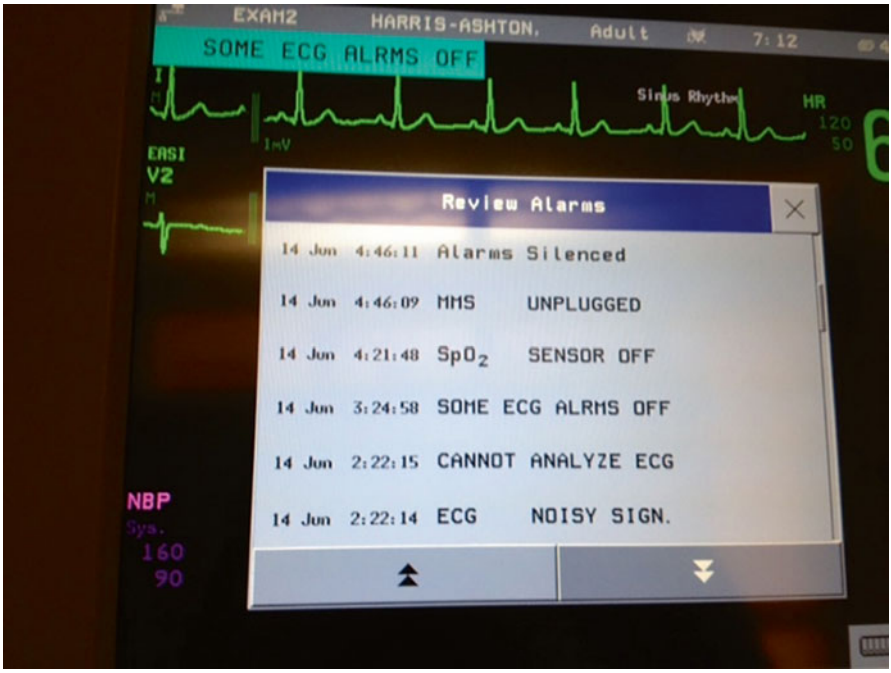


Fig. 7.7 Alarm analysis from bedside monitor

Analysis and Action

After an in-depth analysis of practice and technology, several nursing practice changes initiated to standardize the care of the patient on the monitor and the associated technology (Table 7.6). The nursing staff wanted to ensure that there was no aspect of their practice that contributed to the issues in question. The *X*2 monitors were analyzed by the Philips engineers, and the computer boards replaced. The staff noticed that once the computer boards were replaced, there were no further issues for that monitor. A decision was made to replace the computer boards in the remaining monitors, which resolved the issue.

Case Summary of ECG Signal Failure

Although this was a complex issue, the ongoing collaboration between the EDOU staff, clinical engineering team, and Philips Medical resulted in a better understanding of the technology and a solution that has resulted in safer care for the patients in the EDOU.

Key Lessons

Alarm safety is a complex process that integrates the work of information technology, clinical engineering, and nursing to ensure that the technology safely supports the care of the patient. An increase in the number and complexity of medical devices has resulted in the creation of an environment that may create overwhelming distractions for both patients and staff. Collaboration of all disciplines is essential to ensure that patients feel safe and staff are able to focus on actionable alarms.

References

1. Purbaugh T. Alarm fatigue. Dimens Crit Care Nurs. 2014;33(1):4–7.
2. Sendelbach S. Alarm fatigue. Nurs Clin N Am. 2012;47(3):375–82.
3. ECRI Institute. 2015 Top 10 health technology hazards [Internet]. 2015 https://www.ecri.org/Pages/2015-Hazards.aspx. Accessed 29 Nov 2015.
4. Phillips J. Clinical alarms: complexity and common sense. Crit Care Nurs Clin N Am. 2006;18(2):145–56.
5. Sendelbach S, Funk M. Alarm fatigue. AACN Adv Crit Care. 2013;24(4):378–86.
6. Christensen M, Dodds A, Sauer J, Watts N. Alarm setting for the critically ill patient: a descriptive pilot survey of nurses' perceptions of current practice in an Australian regional critical care unit. Intensive Crit Care Nurs. 2014;30(4):204–10.
7. Cvach M. Monitor alarm fatigue: an integrative review. Biomed Instrum Technol. 2012;46(4):268–77.
8. Cvach M, Frank R, Doyle P, Stevens Z. Use of pagers with an alarm escalation system to reduce cardiac monitor alarm signals. J Nurs Care Qual. 2014;29(1):9–18.
9. Bitan Y, Myer J, Shinar D, Zmora E. Nurses' reactions to alarms in a neonatal intensive care unit. Cogn Tech Work. 2004;6(4):239–46.
10. FDA.gov. Medical Device Reporting (MDR) [Internet]. 2015. http://www.fda.gov/medicaldevices/safety/reportaproblem/default.htm. Accessed 29 Nov 2015.
11. The Joint Commission. Medical device alarm safety in hospitals [Internet]. 2013. http://www.jointcommission.org/sentinel_event.aspx. Accessed 29 Nov 2015.
12. Ryerd E, Okeu S, Ackerman J, Zimring C, Persson K. Noise pollution in hospitals: impacts on staff. J Clin Outcomes Manag. 2012;19(11):301–9.
13. Blake N. The effect of alarm fatigue on the work environment. AACN Adv Crit Care. 2014;25(1):18–9.
14. ECRI Institute. The alarm safety handbook: strategies, tools, and guidance [Internet]. 2015. https://www.ecri.org/components/Pages/Alarm_Safety_Handbook.aspx. Accessed 29 Nov 2015.
15. Graham K, Cvach M. Monitor alarm fatigue: standardizing use of physiological monitors and decreasing nuisance alarms. Am J Crit Care. 2010;19(1):28–34.
16. Gazarian P, Carrier N, Cohen R, Schram H, Shiromani S. A description of nurses' decision-making in managing electrocardiographic monitor alarms. J Clin Nurs. 2014;24(1-2):151–9.
17. Jointcommission.org. National Patient Safety Goals|Joint Commission [Internet]. 2015. http://www.jointcommission.org/standards_information/npsgs.aspx. Accessed 29 Nov 2015.
18. Joint Commission Resources: Quality and Safety Network. Risky business: conducting proactive risk assessments [Internet]. 2015. http://www.jcrqsn.com/VA/2013_jcr3-VA.pdf. Accessed 29 Nov 2015.

Chapter 8
Errors Related to Personal Mobile Technology

Christine Jorm and Lucinda Roper

Introduction

This chapter uses a literature survey and a number of cases to discuss the safety challenges that are arising from the increasing use of mobile devices and technology in healthcare, mainly smartphones. These are pocket-sized devices primarily designed for communication—either voice or text based (messaging and email). Smartphone users can connect to the Internet for greater information access, run specialised programs (applications or apps), and take photographs. Smartphones are changing the way people live—including how they navigate from place to place, and keep in touch with family and friends. Most healthcare workers own smartphones [1–4]. Doctors were early mobile phone adopters; the release of the iPhone 2 (2007), 3G network expansion and rapid medically oriented app development spurred a more widespread uptake of smartphones by healthcare providers. Smartphones are now used by most hospital-based doctors on a daily basis to assist them to do their job and they believe that this technology enables them to provide better patient care [2].

However, these devices are recent arrivals in the workplace and hospital care is still delivered using a model developed in the early years of the twentieth century. Nursing staff are largely fixed in place (undertaking shifts) while medical staff are mobile, with responsibility for patients both inside and outside the institution. Although there are systems, such as rapid response teams, that are designed to flatten hierarchy, the way patient responsibility is generally managed is highly hierarchical. Thus complicated

C. Jorm, M.B.B.S.(Hons.)., M.D., Ph.D., F.A.N.Z.C.A. (✉)
Sydney Medical School, Sydney University, Sydney, NSW 2006, Australia
e-mail: christine.jorm@sydney.edu.au

L. Roper (✉)
UNSW Medicine, University of NSW, Sydney, NSW 2052, Australia
e-mail: roper.lucinda@gmail.com

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_8

communication processes (including between healthcare professions) are required for approval and action. Additionally, medical staff in large institutions undertake patient care while also being trained and training others. Finally, more medical staff now work in shift arrangements established to reduce the incidence of dangerous staff fatigue, but which add new communicative complexity around handover. Communication practices may be designed more to facilitate training processes and maintain boundaries between different health professions, rather than optimising efficient patient care.

Clinical care itself is frequently an uncertain process, being "always about probabilities, about making definite, often irreversible, decisions with incomplete certainty" ([5] p. 211). This adds tension and risk to the complex communication surrounding the care that any patient receives. Furthermore "clinical work today has become increasingly fragmented due to high levels of specialisation and the spatial organisation of medical work" and yet it is also "highly collaborative and consequently requires extensive articulation and coordination of the tasks performed" [6].

A review of clinical communication is well beyond the scope of this chapter, but it provides context to note that the safest communication is at the patient bedside and face to face, allowing for querying, shared decision-making and confirmation of shared understanding. This face-to-face communication is ideally accompanied by contemporaneous recording of this shared understanding into the permanent patient record. There is a grave lack of research on how choice of modes of communication affects patient outcomes.

Problems in designing and interpreting research on smartphones include the rapid pace of technical change and varying local practice norms. Practices relating to staffing, ward rounds, the physical distribution of patients, how orders are given and documented and so on vary substantially inside as well as between institutions. While some institutions may provide smartphones, individuals often bring their own or carry both institutional and personal devices [4].

In Table 8.1 we summarise some of the patient safety advantages and risks of mobile devices.

Leaving aside the advantages mobile devices offer, in this chapter we focus on three types of risks of mobile technology: infection control, patient privacy and interruptions. The first is important as hospital-acquired infections (HAIs) are a major cause of patient harm. For this we provide a discussion of the literature. The second two risks are discussed with the use of case studies. The first case study deals with emerging risks to patient privacy. An important risk associated with use of smartphones is interruption and distraction. This forms the subject of the second case study.

Infection Control Risks

The costs (financial and human) of HAIs are high. As well as providing a possible vector for colonisation and infection of vulnerable inpatients, phones have the potential to carry resistant organisms back out into the community [7]. The risk of personal medical devices forming fomites has been recognised since the 1970s—thus recommendations for regular stethoscope cleaning. Pathogenic bacteria are found on the phones of clinical staff and patients [8]—leading to their description

Table 8.1 Summary of patient safety advantages and risks associated with mobile devices

Smartphone facility	Patient safety advantage	Patient safety disadvantages or risks
Make and take mobile phone calls	Ability to rapidly update decision makers, get help, give orders Time efficient—especially for the person making the call (if it is answered) Enables development of a clear shared understanding Allows senior staff to stay closely involved with unfolding cases when distant Allows senior staff to attend social gatherings, etc.—possibly better work–life balance (certainly better than that of the pre-mobile phone era)	Interruptive—adds risk to other activities being undertaken by receiver May encourage senior staff to undertake activities far away from institution ("you can always get me on my mobile")—if they are far away, they are less likely to review patients Calls not always accompanied by contemporaneous formal notes Assumption of connectivity can be dangerous (flat batteries, unnoticed poor reception) Electromagnetic interference with medical devices possible if faulty but no longer likely (due to better shielding of modern equipment [8]
Send instant messages	Allows for asynchronous communication—less interruptive than phone calls Allows for clear acknowledgment of instructions	May result in overly simplified messages Person requesting information may need to wait—and keeping track of "pending" lines of text communication adds cognitive load Receiver may forget to respond, being distracted again Does not encourage discussion Not always accompanied by contemporaneous formal notes May be insecure
Small, kept in pocket	Convenient. Unlikely to be lost	Possibility of phone contamination spreading infection
Send emails	Modality encourages fully formed summaries, reasoning and plans	Creates patient information source that may be outside the formal record May be insecure
Take photographs	Share patient images with distant experts Store images to share with patients (e.g. operative findings) Chart progress of wound healing	Risk of significant and illegal privacy breaches
Record voice	Record spoken patient consent Can combine convenience of asynchronous messaging with the clarity and detail of spoken communication (voicemail)	Risk of significant and illegal privacy breaches
Access web-based information	Ability to check evidence and provide best practice most up-to-date care Point-of-care decision aids now provide a reputable source of information that is optimised for mobile use	Convenience checking (e.g. use of Google, Wikipedia) may result in poor-quality information and/or information from a single source being used [1, 9] International sources, inappropriate for local practice, may be used
Apps	Convenient Prescribing apps especially helpful and commonly used [1]	Difficult for users to assess credibility, quality and safety [1, 10]

as "mobile bacterial zoos" [9]. Sometimes the "zoo" inhabitants are quite benign [10] and conclusive proof of the relationship between the colonisation of mobile devices and rates of HAI is lacking [8]. However, the relationship between health workers' hands and patient infection is undisputed, and phones are handled by clinicians during and between patient care episodes.

In a recent Irish study, two-thirds of staff were confident that their phones would be contaminated, but when asked if they washed their hands after phone usage 45 % said never, 38 % said occasionally and 17 % said always [10]. In regard to phone decontamination, 63 % of staff reported *never* decontaminating their phone and none did so after every use. Interestingly, this study found low levels of bacterial contamination and hypothesised that this was due to the high level of hand hygiene compliance in the unit studied, and thus simply recommended focus on hand hygiene [10].

Others have found higher levels of contamination, and that a phone decontamination intervention decreased the number of contaminated phones by 79 % [11]. Phones can be decontaminated by wiping the keypad surface several times with wipes containing 70 % isopropyl alcohol [11]. New technologies—such as antibacterial screen protectors—may assist in the future [12].

It has been difficult to obtain compliance with hand hygiene procedures [13] and appropriate hygiene for the use of a personal mobile device care during a visit to a patient is not straightforward. For example, a practitioner performs hand hygiene and then enters a patient room. When their phone rings, they may answer it, reperform hand hygiene and then approach the patient. This seems simple enough; if they have examined the patient and their phone rings while they are in the room talking to the patient, they must touch it whether they answer it or turn it off. They then should perform hand hygiene and phone hygiene, but what of the pocket in which the phone was resting? In one German survey, almost every fifth participant admitted to using their devices *during* contact with patients, for example, for showing information to their patients or as a diagnostic aid [4]. It is difficult for clinicians to focus heedfully on infection control practices (ICPs) during the complex interactions they have with patients, environmental objects and personal objects while also delivering care and often communicating (talking to the patient or other staff).

In the UK, following the protocol of "bare below the elbow", watches are not worn and many staff use their phone clocks to measure pulse and respiratory rate [10]. This adds risk as phones are handled by the fingers which touch patients, whereas a watch would be rarely touched. This is a classic example of an unintended negative consequence of a rule. The complexity of patient and communicative encounters suggests that blanket rules relating to mobile devices and ICPs will not suffice. Rather, what is needed is practitioner sensitivity to ICP and then a heedful and creative approach to creating safety. Videography has been successfully used to provide clinicians and patients with new insights into their work practices [14]. Used for ICP, the technique involves clinicians "in observing everyday ways of working, identifying local infection risks, and making practice safer in situ" [15]. This is not a regulatory technique; provision of a safe (non-punitive) environment for discussion is critical for success.

Emerging Risk: Privacy

This case was submitted by a Sydney medical student as part of an assignment and demonstrates an "ethical dilemma" based on a real case.

A summary of the clinical case study #1 is provided below.

Clinical Summary of Case Study 1 About Privacy Risks

Case 1

You are an intern starting your rotation on a busy medical ward in an Australian suburban hospital. Your registrar (resident) explains to you that the elderly consultant (attending) has embraced the technology of the young. As a busy man running two private practices on top of his public hospital engagement, he likes to do his handover by email from home or his other work places. The consultant uses his private Yahoo account from a private iPhone, whilst the Registrar uses Google Mail from Samsung Galaxy 4G.

Having a Hotmail account yourself, you know that in exchange for a "free" service these private companies, with servers located in the USA, have software scanning through your emails and attachments at all times and, with your upfront consent to the terms and conditions, they perform "data-mining" analyses on your content in order to sell the information on to other companies for a profit.

You are asked to participate in the team communication system, drafting the handover emails for the registrar and emailing them to him. He will then edit and email the handover to the consultant and cc you. (The consultant sometimes forgets to cc you if he emails the registrar back with queries or directions.) You are of course primarily responsible for updating the patient record.

Analysis

The practices utilised in the above case study reflect ignorance about the laws regarding patient information and privacy. These are quite comprehensive in Australia and similar legislation exists in most countries. It is illegal to collect potentially identifiable information without patient consent or to store or share such information in an insecure manner. The privacy risks related to the use of the Internet in clinical care have been described [16]. In this case, "accidental disclosure", by entering the incorrect email address, is possible, and this idiosyncratic communication "system" is highly vulnerable to hacking (or information release triggered by a virus, etc.).

Additionally, the need to remember to cc the junior staff, a step that is easily forgotten, means that important patient care information may not be shared (e.g. tests not acted on or ordered). Options (or lack of forcing functions) create risks. For instance in the case of computerised physician order entry systems (CPOE), having an option to send a result to a doctor's inbox *or* make it available as part of the patient record increases the likelihood of results being missed [17].

In this case, the seductive convenience of the smartphone led the senior doctor to recommend rash actions. The consultant and registrar may have been unaware of the illegality and risks involved, although the junior doctor was aware and anxious. Trainees want to please; in fact, often career success depends on doing so. Doctors are often reluctant to report—adverse events in general [18] but particularly the behaviour of other doctors [19].

An ambitious and busy practitioner may be reluctant to forgo a technology that enables them to manage a heavy workload and may simply choose to ignore risks they are indeed aware of in the absence of a hospital-approved, secure, Internet-based handover system.

In addition to sharing identifiable patient data in a text form, many practitioners currently take and send images using smartphones—e.g. showing the process of a wound healing or a relevant scan. Canadian interns report doing so [2] and a survey of Irish interns revealed that 53 % had done so [1]. Guidelines from the Australian Medical Association [20] suggest that once patient consent has been gained, it is legal to take images on a personal device and send them to another, if it is related to clinical management. The image must be treated as a part of the patient's medical record and in the case of an admitted patient, retained by the hospital. Some hospital record systems are incompatible with photo storage and a hard copy of the photograph should be provided. Secondly, the image must be removed from any personal device or email service immediately after use. However, if an institution doesn't have a secure, *accessible* photo storage system, practitioners will be unlikely to delete the photos taken. If the photo is not in the patient records, they need to keep it on their phones (a typical example would be photographs of a slowly healing ulcer).

Figure 8.1 summarises various contributory factors leading to privacy risks in this case study.

Solutions

Increase Knowledge Around Privacy Requirements

Population literacy around Internet privacy is increasing but more education in clinical schools, as part of specialty training and at conferences, could be provided. However, students aware of the privacy risks still used their phones to transmit identifiable patient information [2]. Therefore, technology solutions are an essential accompaniment to education.

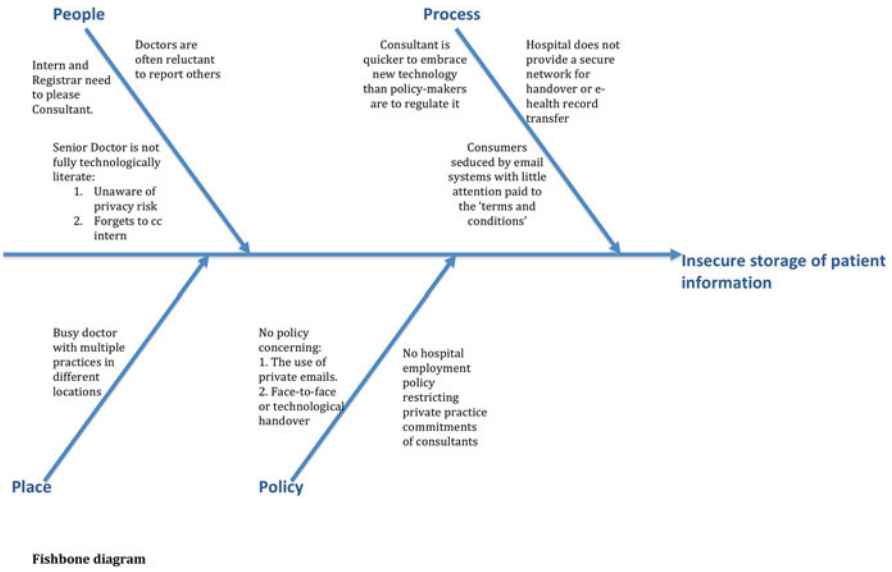


Fig. 8.1 Analysis of case study 1 about privacy risks

Design Technology to Support Clinical Communication Needs

Unsafe "pick and mix" from technologies designed for general use is likely to continue until acceptable systems are available to safely support the communication needs of dispersed clinical teams. Many smartphone workarounds (such as the junior doctor taking a photo of the most significant slice of a CT scan and sending it to their boss) occur because hospital systems are so tightly secured that senior practitioners cannot access their patient's records or results when they are offsite. A secure, remotely accessible portal, in which patient care can be discussed and patient records and images viewed, may be a solution. The technology to create this is readily available [21].

What has been termed "clumsy automation" needs to be avoided [22]. These are systems that do function, but create additional tasks and cognitive load just when staff are most in need of assistance. Busy clinicians will seek convenience—if an official communication system demands too many clicks, difficult login sequences and password changes, a private (albeit insecure) system might be preferred.

Substantial research on e-record and hospital intraweb security has been undertaken in the USA [16]. Creating secure interoperability is a priority to reduce workarounds by doctors between hospitals. However, in the absence of a nuanced system with "contextual access criteria", sharing of patient records often results in irrelevant medical information being shared and workarounds (such as an email) again possibly preferred.

In the absence of institutional solutions, there are some personal measures that could be adopted by clinicians. As a minimum, password protection should be used on smartphones. This is not always the case currently, with 26 % of students in one study admitting to having no security features on their phones [2]. New apps such as

PicSafe Medi (https://picsafe.com/medi) can assist with ensuring privacy. This app allows images taken with a smartphone to be stored, by the app itself, on a password-protected website. The app also records a written or audio consent from the patient.

Consultant with Clearer Limits on Span of Responsibility and Practice Location

From a management point of view, there is a strong argument to make appointments in such a way that medical practitioners work at a more limited number of institutions/locations. High-performing health systems tend to employ full-time medical staff who are necessarily more committed to the institution and engaged in process improvement [23].

Major Risk: Interruption and Distraction

Hospital medical staff are interrupted frequently and interruptions disrupt human cognition [24]. Actions may be interrupted before completion and then are either never completed or completed wrongly. The often-cited case reported where Facebook was the distractor is itself a distractor [25] as most interruptions and distractions do not relate to personal life outside work but are in fact face to face and patient related [26, 27]. The effect of distractions has been especially studied in anaesthesia and while caution around adding discretionary distractions via mobile device use is recommended [28], a recent observational study found that "another anaesthetist was the most common recipient of a distracting event initiated by the anaesthetist" and it was somewhat amusingly suggested that "Anaesthetists need to address themselves as causes of distractions" [29]. Our case introduces some different issues around interruption and distraction.

Below is a clinical case summary that introduces some different issues around interruptions and disruption.

Clinical Summary of Case Study 2 Regarding Distraction Risk

Case 2

Dr. W is an experienced anaesthetist on her third case for the day. The 42-year-old patient is having an elective abdominal hysterectomy for a very large fibroid uterus. The surgeon is very careful but slow. The patient has had previous uneventful anaesthetics, and on no medications except for occasional salbutamol for exercise-induced asthma. The patient has been intubated and paralysed, a large bore IV is in place and a group and hold has been done. Prophylactic antibiotics were given at induction.

(continued)

(continued)
Thirty minutes into the case, Dr. W receives a text on her mobile phone about the next patient on the list. This patient is scheduled for a caesarean section. She is morbidly obese, and has idiopathic thrombocytopenic purpura (ITP) and Dr W has ordered platelets. The laboratory message says "platelets not available". Dr. W texts back "when will they be available?" The laboratory does not respond to this message immediately, so Dr. W makes a call to the laboratory and demands to speak to the director. As she is doing this, the theatre staff ask her if the list order needs to change. Rachel, the scout nurse, is particularly agitated, as she needs to put the steriliser on right now if the order has changed. The surgeon points out that he is worried about fetal well-being and wishes to operate today. Irritated, Doctor W steps outside the theatre to concentrate on her conversation with the laboratory.

Back in the theatre, unnoticed by the team, the patient's airway pressures are creeping up and blood pressure is dropping. The patient is having antibiotic anaphylaxis. Only when the oxygen saturation begins to drop does the team notice and a nurse runs out to find Dr. W.

The anaphylaxis progresses rapidly and although the patient survives she suffers a myocardial infarction and mild hypoxic brain damage. Dr. W and the rest of the theatre team wonder if the outcome would have been different, if she'd been in theatre. The RCA team considers the mobile phone call a contributory factor to the adverse outcome.

Analysis

Figure 8.2 provides a summary of key contributory factors that led to distraction-related error.

Two key distractions occur in this case: the unclear text message conversation, followed by the emotionally charged phone call. Communication tasks that cause emotional arousal (such as a frustrating phone call) result in extra cognitive impairment [30]. However, the second distraction was not dependent on mobile phones, and could have occurred 10 years ago. The information that the anaesthetist receives on the phone is vital and necessary before the next case. Yet processing multiple incoming streams of information is a challenge for human cognition [31, 32]. The anaesthetist lacked the communication skills to restrict these streams by for instance saying:

> *'Could everybody please be quiet while I talk to the laboratory. Then we can make a plan about what to do next.'*

This sentence would have allowed the anaesthetist to remain in theatre whilst dealing with the distraction. Of course, the anaesthetist is not entirely at fault—the

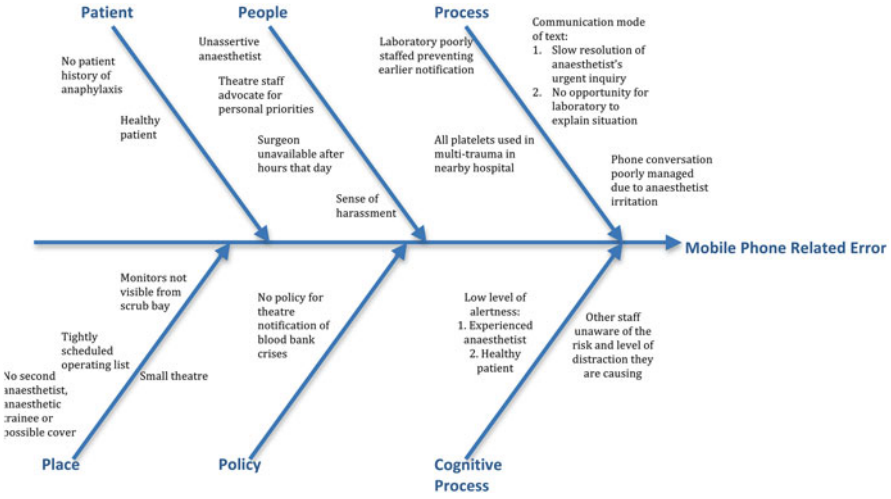


Fig. 8.2 Analysis of case study 2 about privacy risks

other team members did not consider the distracting effects of their attempts to advocate for their own priorities. The mobile phone made the option of stepping out easy.

Text messaging is increasingly popular and less interruptive, allowing asynchronous communication [6], but a large qualitative Canadian study found two major themes [33]. Texting had a negative impact on work relationships between staff and that "de-contextualization of complex issues led to an increase in misinterpretation and an increase in back and forth messaging for clarification". The anaesthetist in this case is distracted by the "back and forth" with just one other party. The Canadian study provides insight into how this distraction can escalate when on the wards:

> 'So if I get a message saying, this is happening on the floor, I will follow up with questions that are not ordered. 'So what are the latest vitals? Here's a suggestion of what to do.' I will not always hear back … I have to remember in my head there was this issue pending. … you have to start keeping track of what was closed and what isn't.'[33]

If we consider the communication perspective of others involved, one wonders how many text messages the laboratory was sending and receiving and whether their failure to reply was a slip.

Below is an interesting variation of the above case where the distracting call is of a personal nature. Views of the anaesthetist's behaviour with this variation would inevitably be harsher (and harsher still if the call had an even more discretionary nature, e.g. a lover at the airport just wanting to say a few more fond words).

… The patient has been intubated and paralysed, a large-bore IV is in place and a group and hold has been done. Prophylactic antibiotics were given at induction.

Thirty minutes into the case, Dr. W receives a call. It is the local Subaru service centre. There has already been a 2-day delay in their car being serviced. It is wreaking havoc on their family logistics—attempting to travel to two workplaces, a school and university with one car.

Reception is bad in this theatre and she realises that she is shouting, so she steps into the scrub bay to avoid distracting the team. The car is finally ready. She tries to ask if one of her kids can pick it up instead of her.

Back in the theatre, unnoticed by the team, the patient's airway pressure is creeping up and blood pressure is dropping …

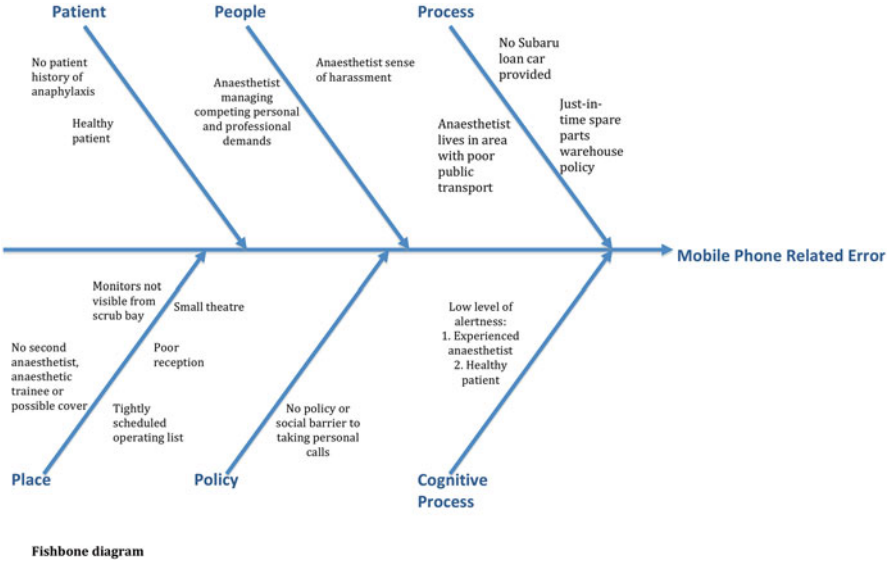


Fig. 8.3 Analysis of the variation of case study 2 about distraction risks

An analysis of this case variation is depicted in Fig. 8.3.

A Variation on Case Study 2 About Distraction Risks

This second case variation could not have happened 10 years ago. It is easy to be critical of the anaesthetist for taking a personal call while she was monitoring an anaesthetised patient. Yet mobile phones are used for a wide variety of personal communications—some of which are important, such as a call from your child's

school, or critical news about a job or home purchase or a sick family member. If these calls can be undertaken safely and quickly and improve the quality of life of all involved, surely they are appropriate.

Given the pervasive nature of mobile phone communications and the expectations that some calls be answered, a blanket ban on personal calls is unrealistic. Personal mobile phone communication can be especially difficult to manage for healthcare workers who do not have many breaks away from direct patient care, such as nurses or anaesthetists. They may attempt to make a call during a break, but it may only be returned later. There is an expectation by others of instant availability and also an increasing acceptance, even within healthcare, of the need for "work–life balance" (for the clinician to look after themselves and have a life outside healthcare). Our mobile devices therefore will frequently result in some blurring of the spatial and temporal boundaries between work and personal life.

Solutions

Technical

A recent paper suggests a number of possible institutional solutions—for enforcement or recommendation to employees [21]. They include the following:

- Individuals or institutions could create a list of "high-alert" or important phone numbers and email addresses. These would be permitted to alert the professional during work, the others being received but no alert given.
- Creation of specific smartphone-use zones with Wi-Fi hotspots to enable staff to manage non-work-related/non-urgent phone calls, messages and emails: These zones could be integrated with cafes or break rooms to ensure that the healthcare professionals are not preoccupied with work-related activities. This should reduce use in other sensitive/restricted areas.
- Restrict access to public social networks to the cellular/smartphone-use zones.

However, the possible negative consequences of such "fixes" are many. For example staff may spend more time in the cafe and less on the ward. It is recommended that any such solution be trialled and studied.

Other simple technical solutions can be adopted by individuals and are likely to be beneficial. Smartphones may persist in showing new text message or email alerts until they receive some attention. For example, a Facebook notification may appear on the home screen, when an intern pulls out their phone to show a patient a Snellen Chart. These annoying features can be customised with a little effort. (Managing an aged relative who persists in calling during working hours may be more difficult.)

Education

Education is justly considered a weak patient safety solution. Its limited value results from the gap between teaching and learning. It is hard to get staff to *remember* something (didactic exercises have to be frequently repeated). However, improved

personal *understanding* is worth seeking. The below narrative (a real case) describes an interaction that was started to achieve this—a reflective awareness of limitations.

An Example of Cognitive Limitations

You are asked to counsel an advanced anaesthesia trainee who has written up ten times the correct dose of paediatric paracetamol. This error is spotted immediately by the nurse who reviews the child's chart on the ward and reported. The young doctor complains that it was a very busy evening shift, that his phone hadn't stopped ringing and that the chart was "shoved under his nose" while he was talking on the phone and that he was just about to rush off to labour ward. He is belligerent about his error and attempts to abdicate any personal responsibility with mention of "system causes". He points out that he hadn't even had a chance to have dinner. You don't have much impact until you tell him that it can always be extremely busy at times after hours in an acute care hospital and probably always will be. In order to have sufficient staff to avoid this ever happening, staff would be painting their nails or similar maybe 50 % of their shift! You both agree that's not likely to happen in our lifetime ….

This capable senior trainee had never before considered the possibility of his own cognitive limitations or that their effects might be more pronounced when he was, for instance, hungry, angry, late or tired. There are a small number of simulator studies where the researchers added distractions in an attempt to force clinicians to make errors [34, 35]. Design of challenging interruptive work simulations (perhaps based in the style of a game) could be pursued to allow all clinicians to understand their own cognitive limitations and those of others. How many patient care tasks did you forget? Were all your prescriptions correct? Education is important for helping individuals make good *choices* regarding whether and when to undertake activities on their smartphone.

Conclusion and Key Lessons Learned

It was suggested in 2012 that we were at the start of a "dangerous decade" and a major issue is the "complexity and heterogeneity of systems and their interfaces, rapid implementation and poor training of users" [36]. Currently health information technology problems form a very small proportion of reports to the FDA [17]. Existing classifications are comprehensive and could extend to incidents associated with personal mobile devices. It would seem likely that personal device use would increase the number of issues in the "human" (e.g. fail to alert, didn't do) and "human–computer interface" (e.g. cognitive load, multitasking and interruption)

categories—if they were reported. However, it is not clear who would have responsibility for reporting or action in regard to personal mobile devices. For instance, if you are an Irish intern and you can't access the British National Formulary (BNF) prescribing information on your phone (poor reception, BNF website problems, flat battery), whose problem is it? Yet the hospital may well have ceased supplying other convenient access because "everyone uses their phones".

While much research on smartphone use is still of poor quality—e.g. self-report—"solutions" such as formal policies regarding resident use during rounds are preferred to anything more extreme [3]. In this instance, mobile devices were mostly used for patient care. The fact that policy restrictions that improved safety for patients being visited could actually add risk for geographically distant patients was not considered.

Implementation of rules is difficult and every change introduces new risks. Proposed changes should be tested prior to implementation. Even when careful testing appears to have been performed, cases such as the CPOE implementation, which resulted in increased deaths in a paediatric ICU by delaying access to emergency drugs do occur [37]. We know that the complexity of a system can mask interactions that could lead to systemic failure [22]. Understanding the impact of system and rule changes in loosely coupled and complex areas such as clinical communication is challenging. Adverse effects resulting from limitations on smartphone use would be hard to predict and measure. It is likely that care processes may be delayed and that less evidence-based care may be practiced.

The phenomenon of "normalisation of deviance" occurs when rules that are either unnecessary or impossible to comply with are created, making it more acceptable to ignore any rules (some of which are important and evidence based) [38]. Rules regulating device use *are* broken; for example, in one study junior doctors admitted to being aware of organisational prohibitions but did not comply as they needed to use their phones to do their job well [10].

There is currently no shared understanding of best practice in overall clinical communication. There is limited evidence available, although more thoughtful analysis is beginning and the work of Wu's group stands out [33]. The research urgently required is observational and patient centred rather than task or doctor centred. It has been suggested that policy makers and electronic health record designers have failed to:

> "understand that transparency of meaning cannot be taken as a given and to … grasp the constitutive role such interactions play in arriving at some shared sense of what the meaning of information actually is." [39]

We know that "clinicians'" organisational competence encompasses negotiating with colleagues how rules work [40]. In the case of the use of mobile devices, this negotiation is situated within developing societal expectations and mores. The etiquette around device use, calls and messaging is still developing. Rather than rules—that will be broken—we argue for education to increase sensitivity to patient safety risks. Thoughtful communication practices using mobile devices, both personal and institutional, should enable improved clinical communication and thus better patient care.

Key Lessons

- Smartphone use in healthcare is still a relatively new phenomenon and the balance of risk and benefit is highly context dependent.
- Smartphones can form vectors for infection transmission.
- Better electronic systems should be provided by institutions to meet the communicative needs of clinicians in dispersed teams to reduce the development of risky workarounds that impose threats to patient privacy.
- Clinicians should be aware of their own cognitive limitations and adopt personal strategies to reduce the risks of distractions on work performance. This includes ensuring that their smartphone use is thoughtful.

References

1. O'Connor P, Byrne D, Butt M, Offiah G, Lydon S, Mc Inerney K, et al. Interns and their smartphones: use for clinical practice. Postgrad Med J. 2014;90(1060):75–9.
2. Tran K, Morra D, Lo V, Quan S, Abrams H, Wu R. Medical students and personal smartphones in the clinical environment: the impact on confidentiality of personal health information and professionalism. J Med Internet Res. 2014;16(5):e132.
3. Katz-Sidlow RJ, Ludwig A, Miller S, Sidlow R. Smartphone use during inpatient attending rounds: prevalence, patterns and potential for distraction. J Hosp Med. 2012;7(8):595–9.
4. Illiger K, Hupka M, von Jan U, Wichelhaus D, Albrecht U-V. Mobile technologies: expectancy, usage, and acceptance of clinical staff and patients at a university medical center. JMIR Mhealth Uhealth. 2014;2(4), e42.
5. Tallis R. Hippocratic oaths. Medicine and its discontents. London, UK: Atlantic Books; 2004. p. 215.
6. Iversen TB, Melby L, Toussaint P. Instant messaging at the hospital: supporting articulation work? Int J Med Inform. 2013;82(9):753–61.
7. Ustun C, Cihangiroglu M. Health care workers' mobile phones: a potential cause of microbial cross-contamination between hospitals and community. J Occup Environ Hyg. 2012;9(9):538–42.
8. Tacconelli E. When did the doctors become fomites? Clin Microbiol Infect. 2011;17(6):794–6.
9. Stein R. When talking and texting get dirty: beware of mobile bacterial zoos. Int J Clin Pract. 2014;68(9):1050–2.
10. Mark D, Leonard C, Breen H, Graydon R, O'Gorman C, Kirk S. Mobile phones in clinical practice: reducing the risk of bacterial contamination. Int J Clin Pract. 2014;68(9):1060–4.
11. Brady RR, Chitnis S, Stewart RW, Graham C, Yalamarthi S, Morris K. NHS connecting for health: healthcare professionals, mobile technology, and infection control. Telemed J E Health. 2012;18(4):289–91.
12. Page K, Correia A, Wilson M, Allan E, Parkin IP. Light-activated antibacterial screen protectors for mobile telephones and tablet computers. J Photochem Photobiol A Chem. 2015;296:19–24.
13. Erasmus V, Daha TJ, Brug H, Richardus JH, Behrendt MD, Vos MC, et al. Systematic review of studies on compliance with hand hygiene guidelines in hospital care. Infect Control Hosp Epidemiol. 2010;31(3):283–94.

14. Iedema R, Mesman J, Carroll K. Visualising health care improvement: innovation from within. Oxford, UK: Radcliffe; 2013.
15. Iedema R, Gilbert G, Hooker C, Jorm C, O'Sullivan M, Wyer M. An innovative approach to strengthening health professionals' infection control and limiting hospital-acquired infection: a video-reflexive ethnography study. BMJ Clin Innovat. (under review).
16. Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. Int J Internet Enterprise Manage. 2010;6(4):279–314.
17. Magrabi F, Ong M-S, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. J Am Med Inform Assoc. 2012;19(1):45–53.
18. Evans SM, Berry JG, Smith BJ, Esterman A, Selim P, O'Shaughnessy J, et al. Attitudes and barriers to incident reporting: a collaborative hospital study. Quality Safety Health Care. 2006;15(1):39–43.
19. Jorm C. Reconstructing medical practice – engagement, professionalism and critical relationships in health care. Hampshire: Ashgate; 2012.
20. Australian Medical Association. Clinical images and the use of personal mobile devices. 2013. https://ama.com.au/article/clinical-images-and-use-personal-mobile-devices. Accessed 26 Apr 2015.
21. Gill PS, Kamath A, Gill TS. Distraction: an assessment of smartphone usage in health care work settings. Risk Manag Healthc Policy. 2012;5:105–14.
22. Committee on Patient Safety and Health Information Technology, Institute of Medicine. Examination of the current state of the art in system safety and its relationship to the safety of health IT–assisted care. Health IT and patient safety: building safer systems for better care. Washington, DC: National Academies Press; 2012. p. 59–76.
23. Baker G, MacIntosh-Murray A, Porcellato C, Dionne L, Stelmacovich K, Born K. High performing healthcare systems – delivering quality by design. Toronto: Longwoods; 2008.
24. Grundeiger T, Sanderson P. Interruptions in healthcare: theoretical views. Int J Med Inform. 2009;78:298–307.
25. Halamka J. Order interrupted by text: multitasking mishap. 2011. http://webmm.ahrq.gov/case.aspx?caseID=257. Last accessed 10 Jan 2015.
26. Coiera EW, Jayasuriya RA, Hardy J, Bannan A, Thorpe ME. Communication loads on clinical staff in the emergency department. Med J Aust. 2002;176:415–8.
27. Alvarez G, Coiera E. Interruptive communication patterns in the intensive care unit ward round. Int J Med Inform. 2005;74(10):791–6.
28. Jorm C, O'Sullivan G. Laptops and smartphones in the operating theatre – how does our knowledge of vigilance, multi-tasking and anaesthetist performance help us in our approach to this new distraction? Anaesth Intensive Care. 2012;40(1):71–8.
29. Jothiraj H, Howland-Harris J, Evley R, Moppett IK. Distractions and the anaesthetist: a qualitative study of context and direction of distraction. Br J Anaesth. 2013;111(3):477–82.
30. Dula C, Martin B, Fox R, Leonard R. Differing types of cellular phone conversations and dangerous driving. Accid Anal Prev. 2010;43(1):187–93.
31. Phillips R, Madhavan P. The effect of distractor modality and processing code on human-automation interaction. Cogn Tech Work. 2011;13:233–44.
32. Finomore V, Matthews G, Shaw T, Warm J. Predicting vigilance: a fresh look at an old problem. Ergonomics. 2008;52(7):791–808.
33. Wu R, Appel L, Morra D, Lo V, Kitto S, Quan S. Short message service or disService: issues with text messaging in a complex medical environment. Int J Med Inform. 2014;83(4):278–84.
34. Dieckmann P, Reddersen S, Wehner T, Rall M. Prospective memory failures as an unexplored threat to patient safety: results from a pilot study using patient simulators to investigate missed execution of intentions. Ergonomics. 2006;49:526–43.
35. Grundeiger T, Liu D, Sanderson P, Jenkins S, Leane T, editors. Effects of interruptions on prospective memory performance in anesthesiology. Human Factors and Ergonomics Society, 52nd Annual Meeting, New York Marriott Marquis Times Square. 2008.

36. Coiera E, Aarts J, Kulikowski C. The dangerous decade. J Am Med Inform Assoc. 2012;19(1):2–5.
37. Han Y, Carcillo JA, Venkataraman ST, Clark RSB, Watson RS, Nguyen TC, et al. Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. Pediatrics. 2005;116(6):1506–12.
38. Rydenfält C, Ek Å, Larsson PA. Safety checklist compliance and a false sense of safety: new directions for research. BMJ Quality Safety. 2014;23(3):183–6.
39. Hartswood M, Procter R, Rouncefield M, Slack R. Making a case for medical work: implications for the electronic medical record. Comput Supported Coop Work. 2003;12:241–66.
40. Iedema R, Jorm C, Braithwaite J. Managing the scope and impact of root cause analysis recommendations. J Health Organ Manag. 2007;22(6):569–85.

Part II
Health Information Technology Implementation Issues

Chapter 9
Improving Clinical Documentation Integrity

Anupam Goel

Introduction

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), part of the American Recovery and Reinvestment Act, was signed into law in February 2009 to promote the adoption and meaningful use of health information technology (health IT) [1]. Economists had seen the positive effects of technology on improving efficiencies in other industries [2]. Billions of taxpayer dollars were spent to incentivize physicians and hospitals to migrate from paper-based medical record systems to electronic medical record systems (EMR) [3]. Since the HITECH's implementation, health IT has been associated with safer medication ordering and automated decision support [4]. Health IT's rapid deployment has also been linked with new error modes [5]. This chapter focuses on documentation errors as a result of health IT.

The primary purpose of physician documentation is to explain the diagnostic and therapeutic decisions made at a given point in time. The documentation can also provide additional information about the patient beyond the patient's discrete data points like vital signs, laboratory values, medications, and coded diagnoses. Free-text documentation allows a clinician to describe findings or circumstances that might explain why one patient's response to treatment is different from another patient with the same diagnoses. The documentation can be used by other members of the health care team to determine next steps or propose other alternatives.

A. Goel, M.D., M.B.A. (✉)
Clinical Information, Advocate Health Care, Clinical Transformation,
3075 Highland Parkway, Suite 600, Downers Grove, IL 60515, USA
e-mail: anupam.goel@advocatehealth.com

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_9

In addition to documenting the patient's condition, the physician's documentation serves other purposes. For inpatient visits, the physician's documentation is the basis for determining the hospital's reimbursement that can vary based on the patient's medical complexity [6]. In all care settings, physician documentation elements are used to determine physician payments [7]. For cases with untoward outcomes, the documentation is a major component of the legal medical record to determine what did or did not happen in a patient's care. In value-based purchasing agreements, physician documentation is used to determine a patient's disease severity to determine per-member per-month payment rates [8]. Most recently, physician documentation is being shared with patients, family members, and caregivers to promote patient understanding and engagement [9].

Given the importance of physician documentation and the increasing EMR penetration [10], medical leadership teams should be particularly interested in documentation errors associated with EMRs.

Clinical Case Studies

Case Study 1: Copy–Paste

A physician admits a patient for a coronary-artery bypass surgery. The patient was intubated for the procedure and remains intubated after leaving the operating room. The first postoperative progress note in the surgical intensive care unit states "Postoperative day #1—patient intubated." The physician copies the note day after day even after a week has passed and the patient has been extubated. Even when the patient is transferred outside the ICU and prepared for discharge, the patient's documentation still states "POD #1—patient intubated."

Health IT allows a user to copy and paste information from day-to-day enabling errors that weren't possible before. An overburdened physician could markedly reduce the time required to document a patient's condition and treatment by cloning information from the previous day and then adjusting a few details to reflect the changes since the last note. Copying documentation without updating any parts of the assessment and plan based on new diagnostic or treatment information could be viewed as lazy at best or fraudulent at worst. Copy-and-paste errors may be the most frequently cited EMR-related physician documentation error [11].

Case Study 2: Inadequate Discharge Summary

Eight hospitalists and three consultants take care of a patient over the course of 5-day hospitalization. The discharge summary includes a list of procedures, laboratory tests, and radiology procedures performed over the course of the patient's stay. The summary does not include how the patient's presentation was translated into a working diagnosis that responded to treatment as expected.

This documentation error highlights the misuse of health IT to meet a documentation requirement (completing a discharge summary) without achieving the actual objective of transmitting meaningful information (e.g., instead of a list of test results, provide the reader with the rationale for why particular diagnostic or therapeutic choices were made). Although more difficult to detect than copy-and-paste errors, these health IT-enabled errors may be responsible for larger lapses in health care quality and safety. Lists of discrete data without the accompanying context can delay a diagnostic evaluation or contribute to unnecessary testing or treatment.

Discussion/Analysis

James Reason has developed a model of error that includes latent conditions and active failures [12]. **Latent conditions** are usually the result of organizational or policy decisions that may inadvertently facilitate active failures. Examples of latent conditions are policies that encourage multiple physicians caring for the patient over a hospital encounter with different documentation styles, hospital credentialing systems that allow for physicians to practice without required EMR refresher training, and regulatory mandates to include specific information within daily physician documentation.

In health care, **active failures** are unsafe acts committed by people in direct contact with patients. Active failures can be further classified into execution failures and planning failures [13]. **Execution failures** refer to those errors where the correct plan was not performed with the desired result. **Planning failures** refer to those errors where the incorrect plan was chosen.

Latent Conditions

Although health IT can be considered the root cause of the errors described in this chapter, the errors occur in the context of non-health IT-contributing factors. Physicians make decisions about what documentation tactics to employ based on environmental conditions. The physician's flexibility in using different approaches based on a given situation can help complete tasks based on shifting priorities or accommodating unplanned events. When physicians choose technology-enabled documentation tactics that adversely affect the team's ability to care for the patient (e.g., note templates, pulling information from other parts of the chart, and cloning other physicians' notes), the tactics contribute to documentation errors. Physicians who use these shortcuts without verifying the accuracy of the document created with technology have traded off a decreased risk of errors due to illegibility with handwritten notes for an increased risk of documentation errors is only possible with health IT.

Latent conditions that could prompt poor documentation include inconsistent handovers between physicians, increased patient volumes and complexity, physicians working with multiple EMRs across different hospital systems, and increasing

documentation requirements from regulatory and billing mandates. See Chap. 11 for additional details about how competing priorities might adversely affect patient–physician communication.

The most significant latent condition may be the low value some doctors place on their documentation. These physicians address documentation after completing their "real" work. A physician might see all of their patients in clinic or in the hospital and then consider documenting on all of those encounters at the end of a session or day. This approach leads to documenting only the highlights of each patient's case without including subtle details that are easily forgotten after seeing a dozen patients. Physicians who do not see documentation as a critical part of their job maximize their documentation time meeting the requirements of external entities rather than describing the patient's condition beyond the medication and problem lists. If billing requirements state that physicians should include four elements of the history of present illness and two "review of systems" components, then that is all that will be documented without regard to what is appropriate for each patient. Physicians faced with a consult list of 30 patients will reuse as much prior physician documentation (from themselves or their colleagues) to get through their day.

Execution Errors

Execution errors are the result of an intention not leading to the desired result. Examples include copying-and-pasting content from other parts of the patient's record, misfiling documentation in the wrong part of the patient's record, and finalizing a document before correcting mistakes within that document. Execution errors can be the result of ignorance of how health IT is intended to work, a lack of appreciation for how specific documentation approaches adversely affect documentation quality, and a doctor's decision to choose a less reliable method of documenting a patient's condition to complete the task to achieve another objective.

Copying-and-pasting is the inappropriate appropriation of information from other parts of the medical record [14]. Copying-and-pasting can apply to a doctor's prior documentation, another physician's documentation, or another clinician's documentation. When used judiciously with a review of what was incorporated into current documentation against the patient's current status, the technique can help pull forward relevant information into a note without re-entering the same information day after day. Without clear policies about what is appropriate to copy, physicians may continue to plagiarize their own work and the work of others without detection.

Another group of health IT documentation errors include improper use of existing electronic documentation tools. Examples include delays in signing notes (preventing users from viewing physician documentation in a timely manner), inadequate note titles (requiring other members of the health care team to manually review each

note rather than utilizing EMR filters to find the appropriate note), and selecting the wrong document type for a particular note. In the last example, if a doctor chooses a history and physical template for a progress note, the document is likely to be filed in the wrong section of the patient's medical record, limiting the ability to subsequently find the note in the future.

A specific health IT execution error is choosing the wrong documentation template [14]. To better capture discrete data elements for billing, quality, or regulatory purposes, some organizations encourage physicians to use documentation templates that specify addressing specific items before completing a note. If the wrong documentation template is selected for the presenting patient, the physician may not be triggered to ask the relevant questions to determine the next most appropriate diagnostic step or complete the associated documentation requirements. A template for altered mental status may not prompt the physician to consider ruling out a cerebrovascular accident. For medical students and residents, these note templates may artificially limit the user's thinking, potentially overlooking important questions to elicit an uncommon diagnosis.

The last group of health IT physician documentation execution errors consist of incorrect information within the physician documentation itself. These errors are usually the result of incomplete review of a document prior to signature. Doctors may type their own notes and overlook errors within the document. Introducing ancillary staff to the documentation process does not always ameliorate the problem. Physicians may not know how to edit transcriptions electronically, perpetuating errors from a transcriptionist or scribe. Historically, any words that the transcriptionist could not understand from a voice recording were identified by long blanks in the report for the dictating doctor to update. The physician would review the transcript, edit the document, and have it included in the patient's medical record. More recently, voice-to-text technology can create physician documentation errors that can be incorporated into a note if the doctor signs the note without a complete review. One group found a 30 % error rate among medical records dictated by physicians without medical transcriptionist review [15]. A physician can now speak into a smartphone to translate voice to text nearly instantaneously. Real-time availability of a doctor's thoughts without a keyboard may represent one of the most significant contributions of health IT toward improving documentation timeliness. In general, voice-to-text software algorithms perform better if the physician speaks in paragraphs instead of individual words by providing the software with additional context to infer the appropriate terms. Some software algorithms use a physician's voice profile to create near-perfect transcriptions without using a human transcriptionist. Physicians may implicitly trust the most current versions of voice-to-text technology given their low error rates. However, unlike telephone transcription with a human transcriptionist, the computer algorithm will make a "best guess" at any verbal utterance that does not clearly map to an existing term. As a result, a transcription error does not appear different than any other text in a document, increasing the vigilance required when using this health IT.

Planning Errors

Physician documentation planning errors are errors in formulating a plan to create a note. An example would be a doctor's decision to list medications, test results, and vital signs without entering information about what the discrete data mean for the patient's treatment course [14]. Health IT, on its own, does not cause physician documentation planning errors. Health IT does allow users to populate a note without significant cognitive input from physicians to explain why the patient is responding or not responding to the current treatment plan. Rather than commenting on why the patient's CT scan might rule out a particular condition on the differential diagnosis, it is faster to copy the entire radiology report in the physician's documentation.

Physician documentation planning errors highlight the physician's missed opportunity to synthesize the patient's symptoms, objective findings, test results, and other information into a coherent narrative. A single positive test result may be a false positive given the patient's other clinical findings. A radiology report documenting an unspecified mass may be evaluated at a later time due to competing priorities during the hospitalization. **Assessments and plans are sections of the document that cannot be outsourced to technology**.

Corrective Actions/Risk Mitigation Strategies

Addressing Latent Conditions

Latent conditions for health IT documentation errors are created in response to other situations. For example, to address low physician productivity, medical leaders implement productivity plans. When payors believe that they are paying too much for medical care, they increase the documentation requirements to receive the same level of payment. Removing all latent conditions from health care, or any other industry, seems impossible.

Latent conditions could be addressed by strategies appealing to physicians' professionalism. Any doctor who has been involved with a peer-review case or malpractice suit understands the importance of accurate documentation. Highlighting good and bad examples of physician documentation in departmental forums with a focus on professional or legal implications could help physicians appreciate the importance of documentation in the context of ever-increasing productivity demands.

On a larger scale, health care systems could apply principles from high-reliability organizations to address documentation errors that are associated with latent conditions. Chassin and Loeb suggest that a strong leadership commitment to the ideal state, a safety culture that support early identification of errors before those errors lead to patient harm, and robust process improvement utilizing techniques like Lean, Six Sigma, and change management could help reduce errors in health care [16]. Many health systems have not examined physician documentation systematically beyond reimbursement opportunities. **The only meaningful feedback a physician might**

receive about documentation quality is from a malpractice claim. Physician documentation would have to be ranked against other medical system quality improvement initiatives for resource allocation to take advantage of this opportunity.

Addressing Execution Failures

Some physician documentation execution errors can be addressed by education [17]. Physicians as a group may be reluctant to admit ignorance when using an EMR. Even if a physician has received extensive EMR training, the absence of early proctored use or feedback may limit self-learning opportunities. Raymond et al. found physicians who used more of the EMR functions to complete their clinical tasks performed at a higher level than their peers [18]. Education should be most effective for developing documentation habits to sign notes in ways consistent with expected clinical workflows, to identify hazards of copy-and-paste behaviors, to label and file notes consistently, and to edit transcriptions, and scribe-generated or voice-to-text documents.

Improving physician copy-and-paste behavior will require audit and feedback. Physicians may copy information from others to align diagnostic and treatment plans. When this behavior masks a lack of independent judgment, medical leadership may need to intervene. Most medical groups do not have the resources to manually review every physician document. Automated analysis of physician documentation is also less likely to be accused of physician targeting. Natural language processing can identify identical text passages across different parts of a patient's medical record. Soon, it will be possible to identify physicians who document the progression of medical conditions over time based on documentation changes from day to day. Physicians who contribute specific diagnostic or treatment information unique from other members of the health care team will be identified as high-performing contributors among medical staffs.

Organizational policies about how best to complete physician documentation could help improve documentation practices among a doctor community. Standards about how incomplete documents are viewed by others, conventions about how physician documents are titled, and educational sessions for users with inconsistent documentation habits can reduce physician documentation errors. Like copy-and-paste errors, health IT could be used to identify doctors who deviate from the organizational standard.

Technology can also be used to reduce the likelihood of entering information in the wrong patient's chart. Some EMRs are designed to limit the number of patient charts that can be open at any one time. A more flexible solution would allow users to open additional charts as "view-only" to allow clinicians to look up another patient's information if interrupted while documenting.

Documentation templates may speed up data entry for novice users. Rather than prompt users at the level of individual data elements, it may be more effective to suggest users enter the relevant information with general headers. Instead of asking for cardiac and pulmonary review of systems, include a paragraph header for any review of systems that the user can use to enter whatever details are most appropriate for the patient.

Any process, human (transcriptionist, scribe) or technology (voice-to-text), translating a physician's voice to printed documentation is susceptible to error. Although each process improves with the next iteration, no process will ever perfectly translate every physician's speech into the intended text. A software with a 0.5 % error rate would imply two to six errors in each operative note, history and physical, consult, and discharge summary. For real-time voice-to-text translation, reviewing each paragraph rather than reviewing the document once it is complete increases the likelihood the author will identify translation errors. For processes without immediate output, document review should occur as soon as possible after the document is available to reduce errors from a lack of recall.

Addressing Planning Failures

Addressing physician documentation planning errors requires understanding what circumstances lead to the error. Some physicians may not be aware of what information is appropriate to include in their documentation. Achar and Wu [19] list three different elements a physician should include in his or her documentation that are not easily cloned from other parts of the medical record:

1. **Thought process**—describe the differential diagnosis and explain why high-risk, low-probability diagnoses are not being pursued. If the initial evaluation does not confirm initial suspicions, then outline a plan to confirm or refute other candidates on the working list of possible diagnoses.
2. **Shared decision making**—describe alternatives discussed with the patient, risks and benefits, and agreement on a plan.
3. **Goals and expectations**—explain what will likely happen next, ask the patient for his or her opinion, and check the patient's understanding as it can help orient the patient to the diagnostic or treatment plan.

Some physicians may not feel that including free-text information about the patient's condition is important or relevant to delivering high-quality patient care. Many doctors receive minimal feedback about their documentation practices from supervisors over the course of their training. Hospital administrators and clinic supervisors may be more concerned with a patient's length of stay or patient satisfaction score than documentation quality. Encouraging changes in physician documentation reviews and physician-specific metrics may be needed before asking doctors to "document better."

A Different Solution

New error types can arise in response to any systematic approach to reduce the risk of an error. Health IT can help identify errors that are specified a priori. As users recognize what behaviors are highlighted by technology, they will adapt their workflows to avoid

detection. **Rather than developing solutions to address specific health IT physician documentation errors, it may be more effective to facilitate document creation and expose documents to stakeholders that doctors value**.

Advances in voice-to-text technology now enable physicians to document patient care in real time. It is possible to see the patient, complete a note, update the patient's summary of care, and complete a bill *before seeing the next patient*. The patient could ask questions while the document was being created. The patient could also see a copy of the note before the doctor left the hospital bed or exam room. Such documentation timeliness could address many health IT physician documentation errors. Some diagnoses and treatment plans may need to be documented separately (e.g., drug-seeking behavior), but the approach of real-time availability of physician documentation should simultaneously reinforce the patient–physician relationship and improve the quality of physician documentation. Doctors would consider maximizing sections of the document that have value for the patient or caregiver and minimize sections of the document that are only important to be reimbursement. Immediate access to physician documentation could become a patient satisfier. Those physicians who are better able to communicate a patient's plan in their documentation are more likely to receive higher patient satisfaction scores. If the patient cannot see evidence of shared decision making or goals and expectations, that may prompt a more detailed conversation with the treating physician at the next encounter.

The most challenging element of this documentation change might be having physicians document in front of patients. Before EMRs, some doctors would dictate their documentation into dictaphones or telephones in front of patients. Early iterations of EMRs required physicians to type their documentation using a keyboard. Since many physicians are not typists, they would often defer their documentation until after leaving the patient's room. With voice recognition, physicians can revert to entering their documentation in front of the patient. Incidentally, this change in documentation can lead to higher quality notes in the same amount of time as writing notes on each patient and then entering all documentation at the end of a shift. This behavior could simultaneously increase patient satisfaction, increase the time physicians spend with patients without significant increases in total time spent in the office or hospital, and decrease physician documentation errors of all types.

Key Lessons

Health IT documentation errors occur within the context of physicians trying to address ever-increasing workloads in limited amounts of time. Even as new processes are developed to reduce specific health IT documentation error modalities, users can be expected to develop new ways to reduce the time spent documenting their work.

Reframing documentation as one of the most important things a physician does may reduce the risk of a physician from making workflow decisions that minimize time spent entering and reviewing physician documentation. Documentation is the most durable communication physicians use to share information with patients and

other members of the health care team. Years after a patient encounter, the physician documentation about that encounter will be considered the "source of truth" about what actually occurred during the encounter.

Health IT can detect specific documentation patterns and possible errors. Voice-to-text technologies can change workflows to be more patient friendly without placing undue burdens on physicians. Physicians, medical leadership, and patients can all support a transition to higher quality physician documentation with full knowledge of the risks and benefits of health IT.

References

1. HITECH Act of 2009. http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf. Accessed 18 Oct 2015.
2. Hesse BW, Ahern BK, Woods SS. Nudging best practice: the HITECH act and behavioral medicine. Transl Behav Med. 2011;1(1):175–81.
3. Searcy T. Majority of physicians used certified EHRs in 2014. http://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/majority-physicians-certified-ehrs-2014/. Accessed 17 Sept 2015.
4. Weigel FK, Switaj TL, Hamilton J. Leveraging health information technology to improve quality in federal healthcare. US Army Dep J. 2015;(4-15):96–100.
5. Magrabi F, Liaw ST, Arachi D, Runciman W, Coiera E, Kidd MR. Identifying patient safety problems associated with information technology in general practice: an analysis of incident reports. BMJ Qual Saf. 2015; (Epub ahead of print).
6. Fetter RB, Freeman JL. Diagnosis related groups: product line management within hospitals. Acad Manag Rev. 1986;11(1):41–54.
7. Medicare. 1997 documentation guidelines for evaluation and management services [Internet]. https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNEdWebGuide/Downloads/97Docguidelines.pdf. Accessed 17 Sept 2015.
8. Chen J, Ellis RP, Toro KH, Ash AS. Mispricing in the Medicare Advantage risk adjustment model. Inquiry. 2015;1:52.
9. OpenNotes. http://www.myopennotes.org/. Accessed 18 Oct 2015.
10. Adler-Milstein J, DesRoches CM, Furukawa MF, Worzala C, Charles D, Kralovec P, et al. More than half of US hospitals have at least a basic EHR, but stage 2 criteria remain challenging for most. Health Aff. 2014;33(9):1664–71.
11. Hirschtick RE. Copy-and-paste. JAMA. 2006;295(20):2335–6.
12. Reason J. Human error. Cambridge, UK: Cambridge University Press; 1990.
13. Reason J. Human error: models and management. BMJ. 2000;320(7237):768–70.
14. Bernat JL. Ethical and quality pitfalls in electronic health records. Neurology. 2013;80:1057–61.
15. David GC, Chand D, Sankaranarayanan B. Error rates in physician dictation: quality assurance and medical record production. Int J Health Care Qual Assur. 2014;27(2):99–110.
16. Chassin MR, Loeb JM. High-reliability health care: getting there from here. Milbank Q. 2013;91(3):459–90.
17. Shachak A, Hadas-Dayagi M, Ziv A, Reis S. Primary care physicians' use of an electronic medical record system: a cognitive task analysis. J Gen Intern Med. 2008;24(3):341–8.
18. Raymond L, Pare G, Ortiz de Guinea A, Poba-Nzaou P, Trudel MC, Marsan J, et al. Improving performance in medical practices through the extended use of electronic medical record systems: a survey of Canadian family physicians. BMC Med Inform Decis Mak. 2015;15:27. doi:10.1186/s12911-015-0152-8.
19. Achar S, Wu W. How to reduce your malpractice risk. Fam Pract Manag. 2012;19(4):21–6.

Chapter 10
EHR and Physician–Patient Communication

Richard M. Frankel

Introduction

> "The patient physician relationship is the *center* of medicine. As described in the patient physician covenant, it should be 'a moral enterprise grounded in a covenant of trust'. This trust is threatened by the lack of empathy and compassion that often accompany an uncritical reliance on technology and pressing economic considerations" [1].

Almost two decades ago, Richard Glass, an associate editor of the Journal of the American Medical Association (JAMA), wrote an editorial, quoted above, in which he introduced a new section of the journal entitled, "The Physician Patient Relationship." Although Glass noted that technology was a potential barrier to trust, he was referring primarily to technological innovations outside of the exam room. The rapid migration of electronic health records (EHRs) from the back room into the exam room has fundamentally changed the role and impact of technology in the doctor–patient relationship and with it the question of where the center of medicine now resides.

In its landmark report, Crossing the Quality Chasm, the Institute of Medicine (IOM) identified patient-centered care (PCC) as one of the six domains that define quality, the others being safety, timeliness, effectiveness, efficiency, and equity. The report defined PCC as "care that is respectful of and responsive to individual patient preferences, needs, and values and [ensures] that patient values guide all clinical decisions" [2]. The primary goal of PCC is for physicians and other health care

R.M. Frankel, Ph. D. (✉)
Indiana University School of Medicine,
Center for Excellence in Healthcare Communication, Cleveland Clinic,
Indianapolis, IN, USA

Center for Healthcare Information and Communication (CHIC), Richard L. Roudebush Veterans Administration Medical Center, Indianapolis, IN 46038, USA
e-mail: rfrankel@iupui.edu

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_10

professionals to be able to collaborate with patients to define problems, set goals, plan care, and communicate information in a safe, supportive atmosphere.

Multiple studies have demonstrated that patient centeredness can improve outcomes of care [3–6]. In addition, patients who are involved in decision making and management of their care experience better outcomes than those who are not [7, 8]. For example, patient self-management for chronic conditions has been shown to be associated with improvements in health status and decreased utilization of services [9]. Patient centeredness has also been shown to enhance clinician satisfaction, reduce malpractice claims, and improve patient loyalty to the clinician [10–14]. It has also been associated with improved provision of preventive services [15]. Additional research demonstrates that six verbal and nonverbal behaviors—empathy and support, trust, tone of voice, eye gaze and posture, physician–patient agreement about the health complaint, and open-ended questioning—are linked to key outcomes that include symptom resolution, patient satisfaction, and adherence to recommended treatment [7, 16–19].

At the same time that an empirical link between patient-centered communication and positive health outcomes was taking shape, technological developments, including EHR use in the exam room, were adding new tasks to the physician's work flow. For example, in the same IOM report that defined PCC as a quality indicator, there is a chapter entitled, "Preparing the Workforce," that outlines new or enhanced skills that will be necessary for medical practice. In addition to being patient centered, physicians will need to be able to effectively use informatics tools, like exam room computers, to communicate, manage knowledge, and support decision making. As aspirational goals, being patient centered and managing informatics tools are laudable. However, the particular kinds of attention and skill that each requires do not necessarily align, and may in fact compete with one another. In essence, exam room computing and its associated tasks add an additional layer of complexity to the traditional model of the doctor–patient relationship as a partnership in which both parties share time and space creating and sustaining therapeutic relationships.

On the technology side, numerous studies of EHRs have been conducted investigating, among other things, data security, time efficiency, and information sharing among providers. One study went so far as to claim that EHR use may be altering the fundamental human reasoning and decision processes involved in health care [20]. Unfortunately, the EHR's impact on patient-centered communication has been largely ignored as a research topic. Nevertheless, integrated health care systems, like Kaiser Permanente and the Veterans Administration, have undertaken large-scale efforts and investments to make computers available in the exam room. The hope and expectation is that this technology can be integrated into clinical care and, once implemented, will be instrumental in improving therapeutic partnerships and the quality of care [2].

EHRs and the Rise of the "iPatient"

The fact that there has been little systematic study of the effects of exam room computing on the doctor–patient relationship hasn't deterred commentary and criticism. For example, Abraham Verghese, an infectious disease physician by

training and a perceptive observer of social trends in modern medicine, coined the term iPatient in a New England Journal of Medicine Perspectives piece in late 2008 [21]. He was referring to the tendency of trainees and attending physicians to focus on the record of care to the detriment of the human being that the record stands for. In the exam room, this translates into a provider interacting more with the computer than the patient. Another high-profile editorial in a 2012 issue of JAMA begins with a drawing by a 7-year-old patient. In it, the patient is seated on the examining table; to her right stands a nurse and the mother holding an infant in her arms. To her left, the doctor is shown at his desk with his back to the patient entering data into the EHR on his computer [22]. The title of the article which appears above the drawing is "The Cost of Technology." From these commentaries, one might be tempted to conclude that exam room computing is the enemy of good medical practice. To be fair, however, there are no national guidelines about computer placement, standards of use, or evidence-based curricula designed to teach trainees and practicing doctors the best ways to be patient centered when using the computer. As such, the conclusion that computers are inherently at odds with good medical practice seems somewhat premature. A more balanced view might be found in Kranzberg's first law of technology that states "Technology is neither good nor bad; nor is it neutral" [23].

Exam Room Computing Through the Lens of Human Factors

Human factors is a branch of engineering that pursues the scientific understanding of interactions between humans and technology in order to optimize well-being and overall system performance. Human factor research has been used extensively in aviation, and other high-reliability industries such as nuclear power, in which precise coordinated actions of humans and technology can mean the difference between life and death [24, 25]. Simulation, cognitive task analysis and micro-analysis of audio and video recordings of actual events are some of the tools that are used in human factor research [26]. In the case of understanding how exam room computing technology affects the doctor–patient relationship, direct observation and recording of the doctor/patient/computer triad in action is an ideal starting place.

The framework depicted in Fig. 10.1 shows units of analyses at the three different levels of organizational structure. Beginning at the bottom of the figure, or the "individual level," situation awareness (SA) theory is used to help describe a provider's level of understanding of his/her environment. The next unit of analysis, moving up Fig. 10.1, is the physician/patient/computer triad and influences on the relationship introduced by ergonomics and the geography of the exam room. At this level the concept of interaction complexity is used to describe communication in the triad. Finally, the organization itself and the demands on workflow are used as the units of analysis to understand their overall influence on work at lower levels of abstraction.

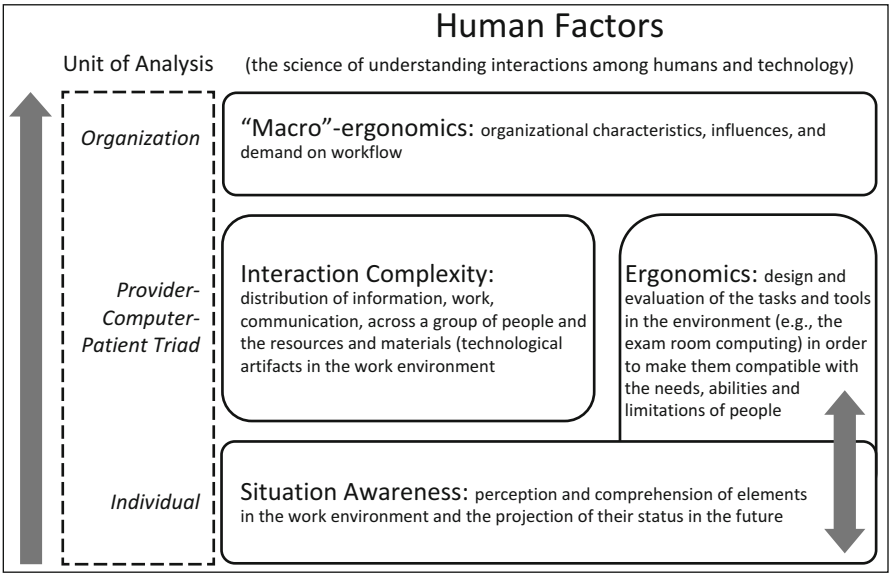


Fig. 10.1 Conceptual framework regarding understanding interactions among humans and technology

Situation Awareness

Situation awareness (SA) is a framework for understanding how humans perceive and comprehend environmental elements and project their status into the future [27]. SA is comprised of the following three levels: (1) perceiving information or cues in one's environment, such as data on the computer screen and patient nonverbal behaviors; (2) comprehending and integrating perceived information; and (3) projecting future events based on the status of current environmental elements. As this description suggests, SA refers to an individual's internal cognitive representation of the environment at a specific point in time. SA is an important framework to draw from when designing a work environment, such as an EHR-enabled exam room. A properly designed work environment will present the necessary information at the appropriate time, without requiring the provider to divert his or her attention away from the patient.

A companion concept to SA is joint focus of visual attention which is achieved either through mutual eye gaze (Fig. 10.2) or simultaneous attention to a third object such as a computer (Fig. 10.3). Joint focus of attention is recognized as an ideal state in which coordinated action is required [28]. Lack of joint focus of attention is associated with diminished performance in technical tasks, and increased risk of errors [29].

Fig. 10.2 Joint focus of attention via (face-to-face) eye contact

Interaction Complexity

Interaction complexity expands the SA framework from the individual to include the interface between the individual and other action systems such as the provider–patient–EHR relationship (Fig. 10.1). Interaction complexity theory helps in understanding the distribution of information, work, and communication across people and technology and the physical environment. As communication and cognitive tasks become more complex, so too does the potential for error [30, 31].

Interaction complexity was first described in a NASA-funded study of errors among commercial airline flight crews engaged in a 3-h full motion simulation [30]. It was defined as situations where multiple, and sometimes competing, interactional demands were placed on crew members and the resulting effects on communication. Figure 10.4 provides an illustration of the phenomenon taken from the transcript of a video recording of crew behavior during one of the simulations.

At line 1 of the transcript, Air Traffic Control (ATC) communicates a request to the captain (P1) to change heading and vector for traffic. P1 responds to the request (line 2) and receives a go ahead, "affirmative," from ATC (line 3). Less than 3 min later (line 10), ATC requests that *another* aircraft ("Cessna 512") contact Phoenix tower on radio

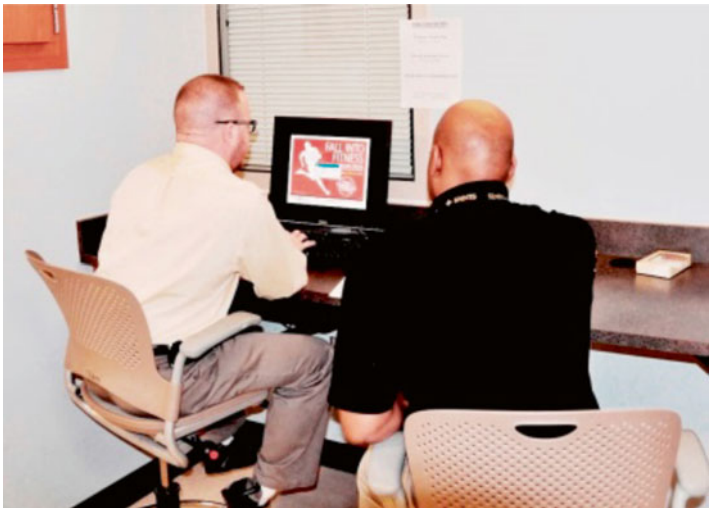


Fig. 10.3 Joint focus via attention to a third object (computer)

		((20 second silence))
→ 1.	ATC:	Flight 343 turn left heading uh 230 vector for traffic
2.	P1:	((transmitting correctly)) Flight 343 left heading uh, 230, 343
3.	ATC:	Affirmative traffic one o'clock five miles uh northeast bound uh
4.		Cessna 172 uh VFR at' four thousand five hundred climbing
5.	P1:	Okay No con- no contact so far.
6.		((173 seconds deleted))
7.	P3:	Flight director and course arrow
8.	P2:	Uh Trim those out about three thousand will y'please John
9.	P1:	Yes sir . Three thousand-fuel flow
→10.	ATC:	This is the 512. Contact the Phoenix tower at one two zero
11.		point niner.
12.	P1:	((transmitting incorrectly)) one two zero niner-
→13.	ATC:	Cessna 512, one twenty point nine.
14.	P1:	Okay one twenty point nine=He was workin' on one twenty four
15.		one, one twenty four one- one twenty point nine. Back to one.
16.	P3:	Joh:n?
17.	P1:	And ((transmitting incorrectly)) Phoenix Tower This is uh
18.		343 on your frequency down wind
19.	ATC:	Oka:y Flight three four three- show you on a downwind you
20.		should still be with Phoenix approach on one two four point one
21.	P1:	((transmitting incorrectly)) They cleared us over to uh one
22.		twenty point nine.
22.	ATC:	Okay Just before you came over here we had a Cessna call I
23.		think you might've taken his call
24.	P3:	Yes: Y'did I was trying t'bring that up

Legend: P1= Captain; P2= Co-Captain; P3=Flight Engineer; ATC=Air Traffic Control

Fig. 10.4 Interaction complexity in aviation

frequency 120.9 which P1 erroneously responds to by changing his own plane's radio frequency. The two requests at lines 1 and 10 are essentially the same linguistically; the only difference between them is the complexity of what's happening in the cockpit when each one is made. Prior to ATC's transmission in line 1, the cockpit has been silent and there are no verbal competing demands on P1. By contrast, the request at line 10 occurs after both the flight engineer (P3) and co-captain (P2) have made requests of P1, the first of which, "flight director and course arrow," P1 has not responded to. In essence P1's error can be attributed to the complex linguistic environment in which ATC's request to another aircraft was made. In general, we found that the greater the interactional complexity the more likely individuals were to make errors [30].

The same principles of interaction complexity can be applied to the exam room and the dual tasks of gathering patient data and documenting it on the computer. Such analyses can help pinpoint opportunities for greater patient centeredness as well as risks to patient safety.

Ergonomics

Ergonomics is a major component of human factor engineering. The principles of ergonomics can be applied at both individual and system levels, as depicted in Fig. 10.1. Organizational design issues and their impact on processes and workflow can be viewed as "macro-ergonomics." In particular, ergonomics evaluates the physical capabilities and limitations of humans; the resulting knowledge is applied during the design process. This framework incorporates the geometry of humans and the surrounding tools (i.e., the "fit" between people, their tasks, and their tools), to design workplace environments. Optimizing workplace design can increase productivity and reduce strain on workers [32].

In aviation, for example, ergonomics is used extensively to design cockpit instrument panels so that pilots are able to synchronize their activities as they interact with the technology (the plane) and the environment (the air space surrounding them) [33]. In medicine, ergonomic design has had minimal application in terms of computer placement in the exam room. The result, as illustrated in the child's drawing in JAMA, is that the physician has his or her back to the patient in order to search for or enter information into the computer, a suboptimal configuration for achieving patient-centered care. A 2005 study of a large multispecialty practice revealed that the most prevalent configuration was for the computer to be placed in a corner of the room where it was easiest to drop the wires totally without regard for the ergonomic strain that might be placed on the physician to engage the patient and the computer simultaneously [34].

EHRs and Communication

Ventres and colleagues found that the positioning of the computer affected communication; this group also found that the very presence of a computer altered the flow of provider–patient encounters [35]. In another study, Margalit et al.

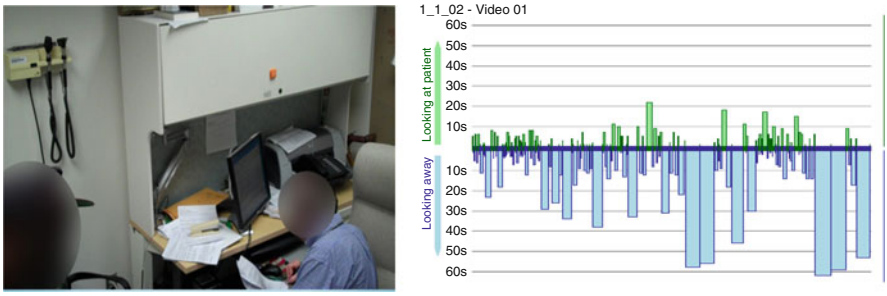


Fig. 10.5 Closed computer configuration and eye gaze patterns when the computer screen is pointing away from the patient

found that patient-centered communication was inversely related to the amount of EHR use during a medical encounter [36]. These effects on verbal and nonverbal communication are particularly concerning given their potentially negative impact on patient-centered communication and ultimately on patient outcomes. Another study by McGrath reported similar variations in spatial computer configurations [37]. The investigators found that exam rooms were configured in one of the three arrangements: open, closed, and blocked. In the open configuration, the computer did not obstruct eye contact between physician and patient and required only a very small adjustment for the physician to turn toward the computer. Also, patients and physicians were physically closest. Several times with the open configuration, patients and physicians viewed the computer together. In the closed configuration, physicians had to turn their backs to patients in order to use the computer, making face-to-face communication difficult. In the blocked configuration, the computer was a physical barrier that "blocked the field of vision between physician and patient."

Figure 10.5 illustrates a computer configuration that is closed with the computer screen pointing away from the patient and the physician's back partially turned away from the patient. In addition to the physical configuration of the computer being a potential barrier to communication this particular physician spent most of his time interacting with the computer screen. The entire visit lasted 19 min and 45 s, of which 12 min and 21 s, or 64 % of the time, was taken up with the physician interacting with the computer and only 7 min and 4 s, or 36 % of the time, during which he was looking at and interacting with the patient. In addition to the ergonomics of the room, and the computer placement, the physician is surrounded by paper documents and is in fact writing on a paper document in his lap. The use of paper represents an additional challenge to work flow and efficiency, not to mention the time it adds to tasks that take the physician's gaze away from the patient. As a habit of practice, we have found that gaze and computer use patterns are relatively stable. For example, in a series of five encounters the amount of time spent on the computer varied from 57 to 64 %.

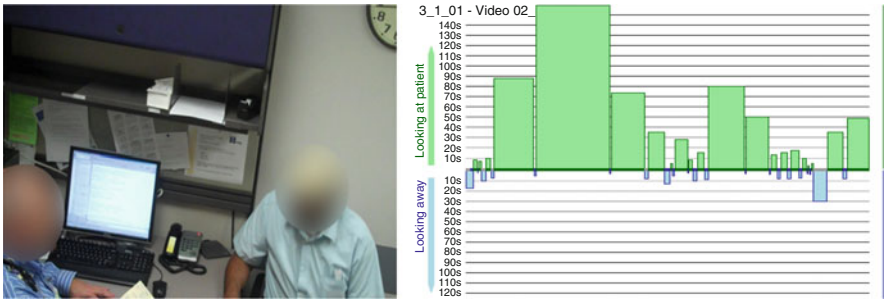


Fig. 10.6 Open computer configuration and eye gaze patterns when the physician and patient are seated facing one another

Figure 10.6 illustrates an open configuration and different gaze patterns from the first physician. The physician and patient are seated facing one another, which is optimal for eye contact. As well, the computer is located in such a way that the physician can rotate it so that he or she and the patient can share a joint focus of attention on the computer screen at any point in the encounter. The gaze pattern of this physician is also quite different in terms of time spent looking at the patient and at the computer. This visit was 14 min and 43 s long. Of that total the physician looked at the patient for 11 min and 57 s, or 81 % of the time, and at the computer for only 2 min and 46 s, or 19 % of the time. Over five recorded encounters this physician's gaze pattern varied from 75 to 81 % of the time spent looking at his patients.

Using mutual eye gaze, which was mentioned earlier as a facilitator of patient-centered care, one can conclude that the physician in Fig. 10.6 is able to use the computer in a more patient-centered way than the physician in Fig. 10.5. At the same time, it is important to point out that the ergonomics of the exam room in Fig. 10.5 and the placement of the computer as a permanent fixture created additional barriers to patient-centered use. These two figures illustrate the wide variation in exam room computer use among practicing physicians and also the distinct differences in ergonomics from exam room to exam room. Compared with the placement of the blood pressure cuff relative to the exam table, which can be calculated in inches, fixed and portable computers can be anywhere in the exam room, from being in a corner, to a desk, to sitting on the physician's lap. Such variation may be necessary given the different tasks physicians use the computer to accomplish during the encounter, but if the ultimate goal of care is to be patient centered it will be important to know which configurations, what behaviors, and the conditions under which physicians and other health professionals are optimally able to realize this goal. Human factor research can help in answering these questions.

Recommendations

Despite the limited systematic research on the effects of exam room computing on delivering patient-centered care, there are some best practices that have been developed mostly by consensus and are worth sharing. Several curricula for teaching medical students and residents have been made available recently. For example, the University of Chicago's Patient Centered EMR Curriculum is available on Meded Portal [https://www.mededportal.org/publication/9953], and Kaiser Permanente hosts a discussion forum for EHR implementation and use in its system [http://www.emrandehr.com/tag/kaiser-permanente/]. In addition, several papers on EHR guidelines have been published that offer helpful advice on EHR exam room use [38–40].

Here I will summarize three of what I believe are the most important guidelines for patient-centered EHR use.

1. Prepare for the visit: In the era of paper records, the idea of reviewing the patient's chart before entering the exam room was treated as a "golden rule." There were, of course, exceptions; charts sometimes were not available to be placed in the door or the clinic schedule was busy. In today's EHR environment it is common to observe physicians entering the exam room without having had the time or opportunity to review the patient's record. Many physicians report that log-on, log-off requirements in many record systems as well as the time it takes to find information in the EHR prevent them from reviewing the record outside of the exam room. While this habit of practice may be functional in the short run, it is both inefficient and limits patient centeredness; for example, searching for the same information in the patient's presence while carrying on a patient-centered conversation is challenging and time consuming and can be frustrating to both parties. Reviewing the patient's EHR prior to the visit is akin to a preflight checklist that pilots go through to make sure that they and their equipment are ready to fly. Doing it in the exam room because you are time pressured and haven't had a chance to do it before is like already being in flight and deciding to do a preflight checklist! It is a threat to patient safety, quality, and the relationship.
2. Introduce the computer and acknowledge that it is now part of the relationship between you and the patient: There is an inherent tension between data gathering and data recording. Research shows that the most accurate rendering of information occurs as soon after an event as possible, suggesting that exam room computing has the advantage of producing highly accurate and complete records [41]. As already noted, accuracy and completeness of note taking compete for attention with patient-centered communication in the encounter. There is no ideal solution to this problem. However, acknowledging and explaining what you are doing on the computer and cueing the patient as to when and why you are doing it can go a long way to engaging the patient as a partner in the process, even if you are busy working on the computer from time to time. Introducing the computer as a third party to the relationship is a type of orienting statement. These types of statements have been associated with lower risk of medical malpractice, another benefit of engaging in this behavior [42].

3. Use the computer as a teaching/instructional aid: The medical record has traditionally been the province of the physician as private "notes to self" [43]. Over time, the role and function of the medical record has shifted and multiple parties (billing, insurance, quality assurance, research) have a direct interest and access to identifiable medical information in the EHR. While a number of others may view the chart when it is completed, it is still the patient who is face to face with the physician and is the primary individual from whom information is gathered. This fact creates enormous opportunities to use the EHR as an educational tool. For example, a patient who has been making good progress in losing weight and keeping their diabetes under control with exercise and diet can be reinforced in their behavior by drawing their attention to the computer screen displaying a histogram of their results over the last 6 months. Jointly focusing on progress toward a goal is a powerful way of continuing to motivate them to maintain healthy behaviors. It also uses time and shared attention efficiently.

Conclusion

In 1816, the French physician Rene Laennec, who was the equivalent of a pulmonary specialist, was asked to see a patient with breathing difficulties. At the time auscultation of the chest was done directly by placing one's ear to the patient's chest. The patient was quite corpulent and he was unable to hear by listening directly. In the moment, he rolled up a piece of paper into a tube, placed it on the patient's chest, and was not only able to hear the lungs but to hear them much more clearly than by direct listening [44]. Laennec's "invention" became the modern-day stethoscope, a technological innovation that has helped generations of physicians evaluate symptoms and make better diagnoses. Although the invention of the stethoscope can be viewed as having placed a technological barrier between physician and patient, its use has been integrated into the medical encounter in a way that supports rather than detracts from the physician patient relationship. In an era of high-tech medicine, the stethoscope and physical auscultation may actually be unnecessary [45]. Nonetheless, both patients and most physicians continue to rely upon it as a means of diagnosis and a reassuring form of communication.

Exam room computers are here to stay. Much still needs to be done to understand how they can be used in a patient-centered environment without detracting from the patient's (and physician's) experience of giving and receiving care. Good science, like good wine, needs time to reach its peak. The science of human factors is one approach that holds potential for finding the sweet spot between data gathering and data recording that is mutually satisfying and produces the most accurate and complete accounts of what happens in the exam room. Until that time comes both the art and science of exam room computing will be tested. Being an optimist, I believe that intelligent, motivated physicians and highly skilled researchers will continue to perfect the doctor/patient/computer relationship and anchor it in the center of medical practice.

References

1. Glass RM. The patient–physician relationship. JAMA focuses on the center of medicine. JAMA. 1996;275(2):147–8.
2. Institute of Medicine. Crossing the quality chasm: a new health system for the 21st century. Washington, DC: National Academies Press; 2001.
3. Rao JK, Anderson LA, Inui TS, et al. Communication interventions make a difference in conversations between physicians and patients: a systematic review of the evidence. Med Care. 2007;45(4):340–9.
4. Roter DL, Larson SM, Beach MC, et al. Interactive and evaluative correlates of dialogue sequence: a simulation study applying the RIAS to turn taking structures. Patient Educ Couns. 2008;71(1):26–33.
5. Lewin SA, Skea ZC, Entwistle V, et al. Interventions for providers to promote a patient-centred approach in clinical consultations. Cochrane Database Syst Rev. 2001;4, CD003267.
6. Stewart M, Brown JB, Boon H, et al. Evidence on patient-doctor communication. Cancer Prev Control. 1999;3(1):25–30.
7. Greenfield S, Kaplan S, Ware Jr JE. Expanding patient involvement in care. Effects on patient outcomes. Ann Intern Med. 1985;102(4):520–8.
8. Wagner EH, Austin BT, Davis C, et al. Improving chronic illness care: translating evidence into action. Health Aff (Millwood). 2001;20(6):64–78.
9. Lorig KR, Ritter P, Stewart AL, et al. Chronic disease self-management program: 2-year health status and health care utilization outcomes. Med Care. 2001;39(11):1217–23.
10. Safran DG, Taira DA, Rogers WH, et al. Linking primary care performance to outcomes of care. J Fam Pract. 1998;47(3):213–20.
11. Levinson W. In context: physician–patient communication and managed care. J Med Pract Manage. 1999;14(5):226–30.
12. Meryn S. Improving doctor–patient communication. Not an option, but a necessity. BMJ. 1998;316(7149):1922.
13. Stewart M, Brown JB, Weston WW, et al. Patient-centered medicine: transforming the clinical method. Thousand Oaks, CA: Sage Publications; 1995.
14. Cuff PA, Vanselow N, Institute of Medicine Committee on Behavioral and Social Sciences in the Medical School Curricula. Improving medical education: enhancing the behavioral and social science content of Medical School Curricula. Washington, DC: National Academies Press; 2004.
15. Flach SD, McCoy KD, Valughn TE, et al. Does patient-centered care improve provision of preventive services? J Gen Intern Med. 2004;19:1019–26.
16. Wasserman RC, Inui TS, Barriatua RD, et al. Pediatric clinicians' support for parents makes a difference: an outcome-based analysis of clinician–parent interaction. Pediatrics. 1984;74(6):1047–53.
17. Lester GW, Smith SG. Listening and talking to patients. A remedy for malpractice suits? West J Med. 1993;158:268–72.
18. DiMatteo MR, Taranta A, Howard S, et al. Predicting patient satisfaction from physicians' nonverbal communication skills. Med Care. 1980;18(4):376–87.
19. Stewart M. Effective physician–patient communication and health outcomes: a review. Can Med Assoc J. 1995;152(9):1423–33.
20. Patel VL, Arocha JF, Kushniruk AW. Patients' and physicians' understanding of health and biomedical concepts: relationship to the design of EMR systems. J Biomed Inform. 2002;35(1):8–16.
21. Verghese A. Culture shock–patient as icon, icon as patient. N Engl J Med. 2008;359(26):2748–51.
22. Toll E. A piece of my mind. The cost of technology. JAMA. 2012;307(23):2497–8.
23. Kranzberg M. Technology and history: “Kranzberg's Laws”. Technol Cult. 1986;27(3): 544–60.

24. Perrow C. Normal accidents. New York: Basic Books; 1984.
25. Vaughan D. The challenger launch decision: risky technology, culture, and deviance at NASA. Chicago: University of Chicago Press; 1996.
26. Russ AL, Fairbanks RJ, Ben Tzion T, et al. The science of human factors: separating fact from fiction. BMJ Qual Saf. 2013;22:1–7.
27. Endsley MR, Garland DJ. Situation awareness analysis and measurement. Mahwah, NJ: Lawrence Erlbaum; 2000.
28. Frankel RM, Flanagan M, Ebright P, et al. Context, culture and (non-verbal) communication affect handover quality. BMJ Qual Saf. 2012;21:121–7.
29. Tallman K, Janisse T, Frankel RM, et al. Communication practices of physicians with high patient-satisfaction ratings. Perm J. 2007;11(1):19–29.
30. Frankel RM. In: Peyton JK, Griffin P, Wolfram W, Fasold R, editors. Captain, I Was Trying Earlier to Tell You That You Made A Mistake": Deference and Demeanor at 30,000 Feet, in Language in Action: New Studies of Language in Society. Kresskill, NJ: Hampton; 2000. p. 289–99.
31. Milanovich D, Driskell JE, Stout RJ, et al. Status and cockpit dynamics: a review and empirical study. Group Dyn. 1998;2:155–67.
32. Salvendy G, editor. Handbook of human factors and ergonomics. 3rd ed. Hoboken: John Wiley and Sons; 2006.
33. Frankel RM, Saleem JJ. “Attention on the flight deck”: what ambulatory care providers can learn from pilots about complex coordinated actions. Patient Educ Couns. 2013;93(3):367–72.
34. Frankel R, Altschuler A, George S, et al. Effects of exam-room computing on clinician-patient communication: a longitudinal qualitative study. J Gen Intern Med. 2005;20(8):677–82.
35. Ventres W, Koojenga S, Vuckovic N, et al. Physicians, patients, and the electronic health record: an ethnographic analysis. Ann Fam Med. 2006;4(2):124–31.
36. Margalit RS, Roter D, Dunevant MA, et al. Electronic medical record use and physician–patient communication: an observational study of Israeli primary care encounters. Patient Educ Couns. 2006;61(1):134–41.
37. McGrath JM, Arar NH, Pugh JA. The influence of electronic medical record usage on nonverbal communication in the medical interview. Health Informatics J. 2007;13(2):105–18.
38. Ventres W, Kooienga S, Marlin R. EHRs in the exam room: tips on patient-centered care. Fam Pract Manag. 2006;13(3):45–7.
39. Duke P, Frankel RM, Reis S. How to integrate the electronic health record and patient-centered communication into the medical visit: a skills-based approach. Teach Learn Med. 2013;25(4):358–65.
40. Shachak A, Reis S, Pearce C. Patient–physician interactions and electronic health records. JAMA. 2013;310(17):1857–8.
41. May JR, Miller PR. Note-taking and information recall: an empirical study. J Med Educ. 1977;52(6):524–5.
42. Levinson W, Debra RL, Mullooly JP, et al. Physician–patient communication. The relationship with malpractice claims among primary care physicians and surgeons. JAMA. 1997;277(7):553–9.
43. Stoeckle JD, Billings JA. A history of history-taking: the medical interview. J Gen Intern Med. 1987;2:119–27.
44. Roguin A. Rene Theophile Hyacinthe Laennec (1781–1826): the man behind the stethoscope. Clin Med Res. 2006;4(3):230–5.
45. Solomon SD, Saldana F. Point-of-care ultrasound in medical education—stop listening and look. N Engl J Med. 2014;370(12):1083–5.

Chapter 11
Patient Identification Errors and HIT: Friend or Foe?

Daniel Hyman and Lynn Voss

Introduction

Problems with patient misidentification resulting in care being provided to the wrong patient have been recognized in healthcare for decades, and are the focus of the Joint Commission's National Patient Safety Goal # 1 [1]. Despite many years of attention, problems of this type continue due to a combination of factors including, but not limited to, inconsistent practices and risk-taking behaviors by staff, language barriers, and other human factors that challenge our ability to eliminate these errors. Risk-taking behaviors include situations where staff members fail to follow policies designed to limit errors in care, for example failing to check two patient identifiers prior to administering a medication. Increasingly, technology is being recognized as both a risk factor for errors and a tool that can offer strategies for potentially preventing them.

In this chapter, we describe examples of how patient identification errors occur in hospital settings, and explore potential strategies to reduce patient identification errors, with an explicit focus on the interface between staff and health information technology (HIT), including the electronic medical record (EMR). Ultimately, the EMR will be one of a number of strategies to reduce the risk of these common, and often under-recognized errors that put patients at risk. Several studies published in the past few years demonstrate that the EMR can be used to reduce risk and are

D. Hyman, M.D., M.M.M. (✉)
Quality & Patient Safety, Children's Hospital Colorado,
13123 East 16th Avenue, Box 400, Aurora, CO 800045, USA
e-mail: Daniel.hyman@childrenscolorado.org

L. Voss, B.S., Six Sigma Black Belt
Quality & Patient Safety, Children's Hospital Colorado, Aurora, CO, USA
e-mail: lynn.voss@childrenscolorado.org

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_11

discussed below. Three proximate causes of HIT-related patient identification errors are profiled, with analysis and potential strategies to address each of these latent safety risks in our systems.

Case Studies

A. Orders Placed on the Wrong Patient

Case 1. A resident physician ordered a lab test on her patient A. The nurse drew blood from the child's central line and sent it to the lab. The resident soon saw that there was a lab test in process on patient A and realized that she had ordered the test on a patient different than who it was intended for. The resident called the lab to cancel the order for patient A and placed it on patient B. Both patients' charts had been open on the resident's computer screen at the time that the order for the lab test, intended for patient B, was mistakenly placed for patient A.

Case 2. A patient was experiencing dystonic symptoms in an inpatient psychiatry ward and the provider placed an order for benztropine 0.5 mg. Unfortunately, the order was placed on patient B instead of the intended patient A. The nurse caring for patient B did not question the order because patient B was on antipsychotic medications and was experiencing some mild adverse reactions. Patient B received medication unintended for him as a result of the error in order entry, and patient A's treatment was delayed for some period because there was no order to give the medication.

In these first two cases, the proximate cause of error was erroneous placement of an order in the wrong patient's EMR. A provider placed an order in the computerized order entry (CPOE) system for either a lab test or a medication for a patient other than whom he/she intended, and in each case the order was acted upon by the patient's nurse. No harm occurred in either of these cases, but the possibility of harm occurring from a future case with similar causation is easy to imagine—either because of an adverse reaction to a medication or a failure to treat the intended patient, leading to a delay in care and a potentially serious adverse outcome.

A research study by Hyman et al. described their hospital's early focused efforts to reduce episodes of care to unintended patients [2]. Surprisingly, one of the commonest causes of patients receiving care not intended for them was the erroneous placement of either orders or clinical information in the wrong patient's chart. This type of error had not been systematically described previously. The authors hypothesized that CPOE systems may introduce a new and unintended source of patient identification errors into the care system, due to both erroneous ordering and documentation. Just as HIT is introducing this risk, it is also recognized as being a source for potential solutions or mitigation strategies.

Figure 11.1 summarizes the distribution of the primary types of identification errors reported at baseline by Hyman's group. While bedside errors related to wrong patients having a medication administered to them or a lab test performed upon

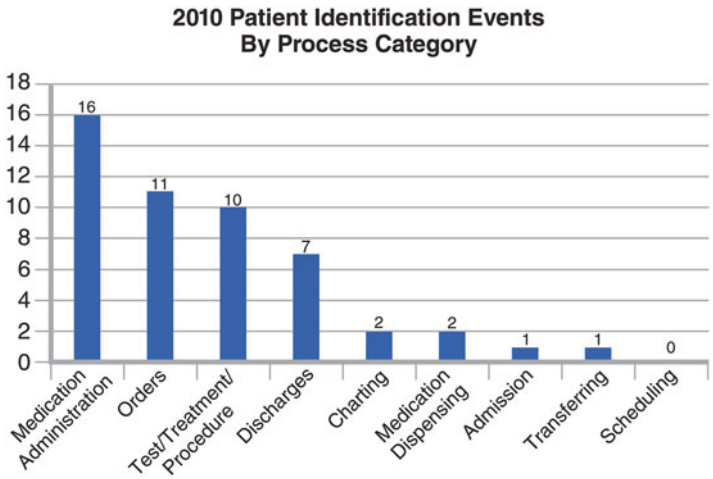


Fig. 11.1 Pareto distribution of patient identification error events during the baseline period (2010) [2]

them were the most common type of error, fully 22 % (11/50) were due to orders being placed in the wrong patient's electronic chart. Furthermore, their near-miss data suggested that at least 75 % of errors related to orders in the incorrect chart were actually being caught by nursing staff or pharmacists upon review of those misplaced orders, and these were then corrected once identified, prior to being executed. During the baseline period in 2010, 33 near misses of this type were voluntarily reported, three times the number of actual events that reached the patient. These errors are most likely to be caught when the medications or tests ordered are not consistent with the patient's care plan, symptoms, or diagnosis, and the nursing or pharmacy staff question the ordering provider.

In the search for solutions to reduce the frequency of ordering errors of this type, the improvement team considered several strategies including placing a restriction on the number of open records (currently four) any provider could keep in his/her workspace. Figure 11.2 illustrates the view a provider had when more than one patient record was open in the user workspace. The team was technically unable to determine whether there was any link between the reported errors and multiple records having been open. In the absence of such evidence and staff concern about workflow if they had to close charts any time they needed to look at another patient's record, the researchers decided to seek an alternate intervention strategy.

Instead, the CPOE workflow was modified, first to include an order verification screen that asked the provider to confirm that he/she was placing orders on the intended patient prior to signing those orders. This strategy did not, itself, impact error rates. Soon thereafter, however, patients' pictures were obtained and placed on the order verification screen (Fig. 11.3). Patient picture-taking equipment and processes were sequentially deployed and implemented across the hospital system over a 1-year period.

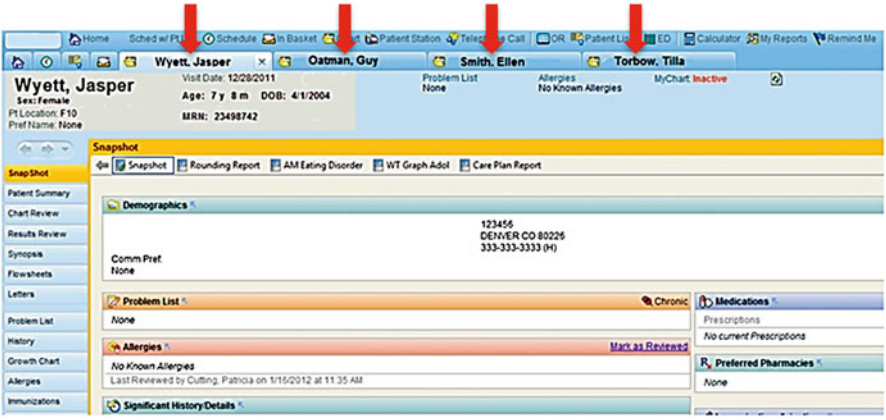


Fig. 11.2 Screenshot of EMR with multiple patient tabs open (before placement of patient photo verification screen)

Fig. 11.3 Screenshot in the EMR with the patient photo on the verification screen (not an actual patient)

Results of the Patient Picture and Order Verification Process

In 2010, hospital staff reported a total of 50 episodes of care being provided to the incorrect patient. In 2011, the total number of reported patient identification errors of any cause decreased by 25–37 %, and the distribution of the types of errors shifted, with two-thirds of them a result of failure to match medications to the patient at the bedside/point of care (Fig. 11.4).

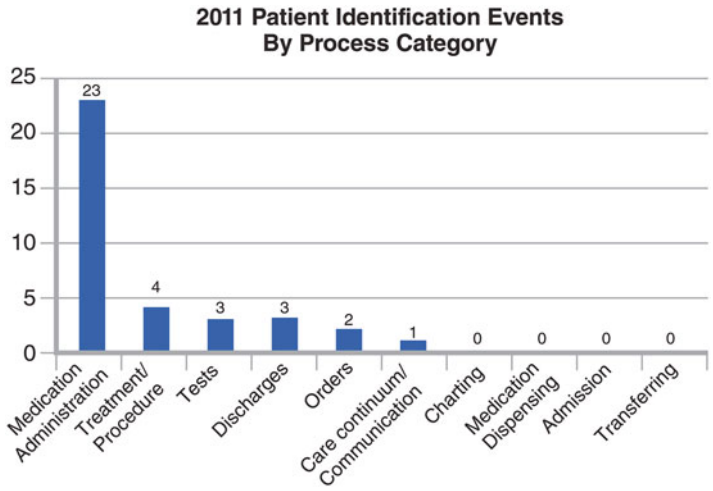


Fig. 11.4 Pareto distribution of patient identification errors after the photo verification screen implementation (2011)

In the first year after the initiation of the order verification screen and the added facial image, reports of errant placement of orders in an unintended patient's chart dramatically decreased. In 2011, only two patients were reported to have received care not intended for them due to misplaced orders, as compared with 11 such events in 2010. Of note, in neither of those two instances was the patient's picture present in the record. Furthermore, ten near-miss events were reported during 2011 in which orders were placed on the wrong patient but interrupted by another staff member who questioned the indication for the order, as compared with 33 similar near-miss reports during 2010. Similarly, only one of those ten patients had his/her picture in the record. The introduction of a patient verification screen with the patient's picture resulted in an immediate reduction of more than 75 % in the number of ordering errors that resulted in unintended care being provided to the wrong patient.

Since the introduction of the order verification screen and the patient photo at the end of 2010, a reduction in errors in placing orders in the wrong patient's EMR has been sustained with each subsequent year reporting between 1 and 3 events per year (Fig. 11.5).

These results suggest a sustainable trend in the decrease in the frequency of providers erroneously completing orders in the incorrect record following these two interventions. Figure 11.6 demonstrates the number of days between reported occurrences of patients receiving care not intended for them due to the placement of an order in the incorrect patient's EMR. This statistical process control chart reflects the significant increase in the number of days between order-related patient identification errors following the introduction of the patient photograph and verification screen in the provider's ordering workflow.

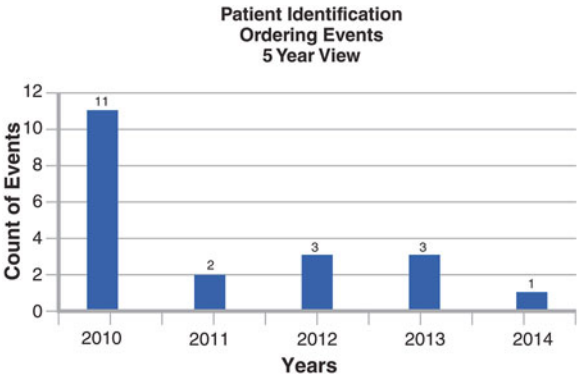


Fig. 11.5 A 5-year view of patient ordering events

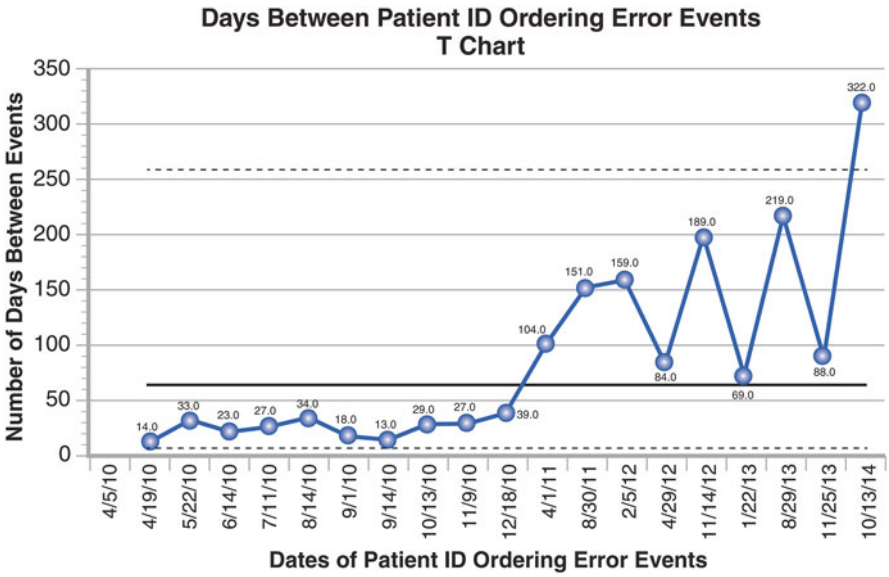


Fig. 11.6 Days between patient identification ordering events for 2010–2014 (including cases both with or without a picture present in the EMR)

One other published study demonstrated that the implementation of a patient verification dialog box at the initiation of the ordering sequence in five emergency departments could also result in sustained improvement over a 2-year period [3]. This study incorporated a 2.5-s delay, after which the provider had to confirm the patient's identity.

The primary interventions in both of these reports were an interruption in the ordering sequence that requires the ordering provider to verify the patient's identity, a step that was strengthened by having the patient's picture on the verification screen. In neither case was the intervention designed so as to be evaluable as an independent variable.

The placement of orders in the wrong patient's chart had not been well documented or analyzed as a cause of error, and is potentially enabled by the implementation of CPOE. Although none of the reported errors in this hospital resulted in significant harm to patients during this time frame, these errors remain a latent systemic risk and require continued evaluation and targeted interventions to reduce the risk of serious harm in the future.

Issues that may be raised by decision makers in organizations considering replicating this type of strategy include both potential HIPAA concerns and the need for updating the picture with changes in the patient's appearance, especially in a pediatric population. HIPPA does not prevent the use of pictures in the course of providing medical care but policies should be in place to ensure that the pictures are handled appropriately, as with any other protected health information in the EMR. Hospital policy on updating pictures has evolved over time; currently the frequency of updates is based on patient age. Patients under one [1] year of age have a new photo taken once every 30 days. For patients over one year of age, a new photo is taken once every 90 days or at any time the staff feels that a change in appearance warrants updating the picture. (Adult hospitals would likely, appropriately, opt for longer intervals between picture retaking.) Workflow at registration where pictures are taken may also be a concern raised by staff, especially in busy outpatient areas. It has been quite feasible to incorporate picture taking into registration processes without significantly impacting efficiency. The scope of work required to implement the order verification screen and patient pictures in the electronic record was extensive and required a range of system interfaces as well as issues with EMR upgrades. Finally, one must also consider the operational expense of placing digital cameras at all entry points to the organization. Even with these considerations, the safety benefits and patient centeredness of placing pictures in the medical record seem to clearly outweigh any time pressure or cost issues.

It is well documented in the literature that providers override between 49 and 96 % of alerts presented to them in the course of entering orders in the EMR [4–7]. Although other alerts in this hospital's system are ignored up to 80 % of the time, providers report that the large, centrally placed patient picture on the verification screen is effective in capturing their attention when the picture is not of the patient they are expecting. This does of course have limitations, especially with newborn babies or when the picture is poorly exposed. The dramatic and sustained reductions in this source of patient identification error over the past 4 years are substantive evidence of the effect of the patient photo verification intervention.

The picture of the patient appears to impact providers differently from a human factor perspective and this would likely benefit from further study. It raises the question of what might health care systems do with other alerts that can be configured to similarly impact providers in the way they are reportedly impacted by seeing a patient picture.

B. Documentation in the Wrong Patient's Chart

A second major proximate cause of patient identification errors due to the interface between health care staff and technology is erroneous placement of information in a patient chart.

Case 3. A clinical assistant (CA) was making patient rounds and obtaining vital signs on the inpatient oncology unit. One of the patients had a temperature of 39.3 °C. The CA informed the patient's nurse directly, but accidentally documented the elevated temperature in the wrong patient's chart. Sometime later, and after shift change, a staff nurse noticed that her patient had a temperature documented in the chart that had not been passed along at shift report. Because the patient was neutropenic, blood cultures were obtained and the patient was started on antibiotics. It was later recognized that the temperature documentation was incorrect and antibiotics were discontinued.

This case reflects a second potential proximate cause of wrong care being provided, due to an error in the use of the EMR. Personal error prevention practices are one strategy for reducing this latent risk of basic human error in everyday workflow. "STAR" (stop, think, act, review) is one such example, but this is certainly not a highly reliable prevention strategy.

Strategies to assess for and use health IT to reduce documentation errors have been limited. Henneman found that providers infrequently identified their own patient identification errors related to documentation in the wrong chart [4]. Wilcox et al. described patient/note mismatches using errors in gender attribution in the medical record, although the linkage to actual care errors was not determined [8]. The Office of the National Coordinator on Healthcare Information Technology released an extensive report on strategies for matching patients with information in their EHR although its focus was less on care workflow and more on dataset reliability [9]. Other strategies will need to be determined in order to minimize the risk of these types of errors. In the interim, personal error prevention practices, like STAR (stop, think, act, review-reference HPI), encourage health care team members to focus on the task at hand, especially when rushed or distracted. This is not an ideal risk mitigation strategy, so other IT solutions will need to be developed.

C. Bedside Errors in Medication Administration

The most common cause of patient identification errors in the Hyman study was bedside administration of medication to (or lab testing on) the wrong patient [2]. HIT has a role in this type of error as well.

Case 4. A nurse caring for four inpatients, one of whom is critically ill, is waiting for the pharmacy to deliver an antibiotic that her patient needs urgently. She

calls the pharmacy to alert them to the urgency and returns to her patient's bedside. Shortly thereafter, another nurse brings the medication that had arrived in the hospital's "tube" distribution system to the patient's room. The nurse spikes the bag of antibiotics and begins infusing it into her patient. Ten minutes later, the patient develops urticaria, wheezing, and worsened hypotension at which time it is recognized that he had been given Penicillin to which he is allergic, instead of the intended quinolone antibiotic. The antibiotic is discontinued, and the patient is treated with diphenhydramine, epinephrine, and albuterol and slowly returns to his baseline.

There are numerous, well-recognized proximate causes for errors in which health care team members give medications, tests, and treatments to incorrect patients. The frequently heard "we know our patients" excuse for not checking two identifiers is a reflection of poor practice and an important issue to address as hospitals seek to advance their patient safety culture. In examples like the above case, staff may be rushing due to real or perceived patient risk, and either do not recognize or minimize their risk of harming their patient by not ensuring that the treatment is intended for them. The primary HIT intervention to reduce this latent patient safety risk is bar code scanning technology. In brief, patient ID bands are typically enhanced with a two-dimensional bar code that is unique to that patient and hospital encounter. Medications and other interventions are similarly labeled with unique patient bar codes and staff can scan both the medication and the ID band (or test vial, etc.) prior to administering the treatment or test. In the event that there is not a match, the scanning device alerts the staff member who then ideally stops what he/she is doing until the situation can be resolved. Although helpful, it is unfortunately the case that these alerts are also too frequently ignored or misinterpreted.

Conclusion

These three common examples of ways in which HIT can either enable or help prevent user errors in ordering, documenting, and managing patient care tasks clearly demonstrate the power of the computer to impact care delivery in both positive and negative ways. Although the user interface, with multiple charts open and numerous patients to pick from on computer lists, may make order placement and/or documentation in the wrong record more likely than with former paper charts, there is also an effective solution with patient pictures in the record and a verification process to reduce these risks. Technology can also reduce the risk of incorrect medication administration within a staff member's task completion workflow. In coming years it is likely that additional tools will be developed that make it harder for providers to err in providing patient care due to new ways of interfacing with each patient's EMR and reduce the likelihood of care being provided to an unintended patient and putting that patient at risk of preventable harm.

References

1. The Joint Commission. National Patient Safety Goals: hospital accreditation program. http://www.jointcommission.org/assets/1/6/2015_HAP_NPSG_ER.pdf. Accessed 4 Oct 2015.
2. Hyman D, Ross M, Redmond D, Kaplan D. The use of patient pictures and verification screens to reduce computerized provider order entry errors. Pediatrics. 2012;130(1):e211–9.
3. Green RA, Hripcsak G, Salmasian H, et al. Intercepting wrong-patient orders in a computerized provider order entry system. Ann Emerg Med. 2015;65(6):679–86.el.
4. Henneman PL, Fisher DL, Henneman EA, et al. Providers do not verify patient identity during computer order entry. Acad Emerg Med. 2008;15(7):641–8.
5. Van Der Sijs H, Aarts J, Vulto A, Berg M. Overriding of drug safety alerts in computerized physician order entry. J Am Med Inform Assoc. 2006;13:138–47.
6. Shah NR, Seger AC, Seger DL, et al. Improving acceptance of computerized prescribing alerts in ambulatory care. J Am Med Inform Assoc. 2006;13:5–11.
7. Weissman IT, Davis RB, Massaali M, et al. Overrides of medication alerts in ambulatory care. Arch Intern Med. 2009;169(3):305–11.
8. Wilcox AB, Chen Y, Hripcsak G. Minimizing electronic health record patient-note mismatches. J Am Med Inform Assoc. 2011;18(4):511–4.
9. Morris G, Farnum G, Afzal G, et al. Patient identfication and matching final report. Prepared for the Office of the National Coordinator for Health Information Technology under contract HHSP233201300029C. https://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf. Accessed 4 Oct 2015.

Chapter 12
Errors Related to Health Information Exchange

Carol J. Parker and Julia Adler-Milstein

Introduction

Health information exchange (HIE) is the process of electronically sharing patient-level health information to support care delivery. The need for HIE arises from the fact that the USA (and other countries) have fragmented healthcare delivery systems in which patients receive care from multiple providers—both during an episode of care and over the course of a lifetime [1, 2]. The clinical information generated during an encounter is captured in the patient's medical record within a given healthcare provider organization, and the process for sharing the relevant pieces of information with other providers has historically relied on manual, error-prone methods of phone, fax, and mail [3]. As paper medical records are increasingly replaced with electronic health records (EHRs), HIE capabilities can be put in place to enable health information to follow patients *electronically* across care delivery settings.

The benefits of HIE are many because, in concept, HIE should enable access to complete patient information at the point of care [3]. This should avoid care that is duplicative and potentially unsafe. The empirical evidence to date suggests reductions in utilization as a result of HIE, primarily related to laboratory and imaging tests [4]. Reducing unnecessary imaging, and the associated exposures known to harm patients, is therefore the domain with the best evidence for how HIE is likely to improve patient safety. However, more complete information enabled by HIE

C.J. Parker, M.P.H. (✉)
College of Human Medicine, Michigan State University, 965 East Fee Road, Room A118, East Lansing, MI 48837, USA
e-mail: parkerca@msu.edu

J. Adler-Milstein, Ph.D.
School of Information and School of Public Health, University of Michigan, 4376 North Quad, Ann Arbor, MI 48109, USA
e-mail: juliaam@umich.edu

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_12

should result in a range of other patient safety benefits, such as more accurate diagnosis and a reduction in potentially harmful drug-drug interactions, drug-allergy interactions, and drug-lab interactions [5–9].

In response, there has been substantial funding and activity at federal, state, and local levels to promote HIE in the USA. Different approaches to HIE have emerged in healthcare markets based on community preferences for how to structure HIE in terms of the types of organizations involved (e.g., hospitals, ambulatory practices, labs), the types of information that can be accessed (e.g., test results), and the form of electronic access (e.g., push, pull). Nonetheless, a common set of terms and definitions to describe key differences between market-driven approaches to HIE have emerged, based on the types of organizations involved: Community HIE Networks, Enterprise HIE Networks, and EHR Vendor HIE Networks.

Community HIE Networks—also referred to as Health Information Organizations (HIOs) or Regional Health Information Organizations (RHIOs)—exist when provider organizations in a given community collaborate to secure the technical infrastructure and negotiate the governance approach to engage in HIE to improve patient care. Typically the only restriction on the types of stakeholders that can participate is geography. A recent survey found 119 of these networks in the USA, operating in 67 % of healthcare delivery markets [10]. Hospitals and ambulatory providers were the most common type of participants in these networks, typically sharing test results and summary of care records [10].

Enterprise HIE Networks exist when one or more provider organization(s) electronically share clinical information to support patient care with some restriction, beyond geography, that dictates which organizations are involved. In contrast to Community HIE Networks, participation restrictions are driven by strategic, proprietary interests [11, 12]. Although broad-based information access across settings would be in the best interest of the patient, provider organizations are sensitive to the competitive implications of sharing data and may pursue HIE in a strategic way [13]. A common scenario is hospitals that choose to affiliate with select ambulatory providers, and invest in HIE capabilities with them, in order to encourage referrals from these providers to the hospital rather than to one of the competing hospitals [14, 15].

EHR Vendor HIE Networks exist when HIE occurs within a community of provider organizations that use an EHR from the same vendor. A subset of EHR vendors have made this capability available; EPIC's CareEverywhere solution [16] is the best known example. Providers with an EPIC EHR are able to query for and retrieve key clinical data from any provider organization with EPIC that has activated this functionality. Little is known about the number of existing enterprise and EHR vendor HIE networks, the number of providers who use them, or the specific types of clinical information that are shared.

While there are important differences between approaches to HIE, regardless of approach, a set of corresponding human processes must be developed and consistently applied in order to translate HIE capabilities into safer and more effective care. When undertaking these processes, weaknesses in provider organizations' internal processes and standards are often exposed, which create opportunities for

errors and unsafe care. In this chapter, we focus on two common types of errors, with implications for patient safety, that can result when provider organizations pursue one or more approaches to HIE. The first is errors related to patient identification and matching. The second is errors related to efforts to protect patient privacy. We use case studies to illustrate the errors, analyze the root causes, and describe potential solutions. Our case studies assume that a community HIE network ("HIO") is the approach to HIE.

Errors Related to Patient Identification and Matching

Because the USA lacks a common identifier that can be used to match patient identity across provider organizations, a key challenge facing any HIE effort is how to enable such identification and matching. This issue is particularly salient because of the potential patient safety implications that could emerge from incorrect identification and matching. Provider organizations typically have developed a set of policies and procedures that dictate patient identification and matching, such as how hospitals name newborn babies and unconscious, unidentified patients. When a provider organization chooses to share patient information electronically with other provider organizations, the naming principles are incorporated into the interface development between the two organizations' clinical information systems. Interfaces allow information to be delivered electronically and securely between separate clinical information systems, such as EHRs and laboratory information systems, which may not be using the same vendor. Even if the two systems are from the same vendor, the organizations that wish to engage in HIE may not be using the same or compatible versions of the software. Patient matching and identification are critical to the development of an interface as they determine how information is sent and received electronically.

Patient identification and matching are particularly challenging in the case of HIOs because HIOs typically facilitate exchange across many provider organizations with many different vendor products and naming principles. Further, there is no standard set of attributes used for patient matching across organizations and not all attributes that an HIO may select for patient matching are collected in all EHRs [17]. Even patient medical record numbers do not offer a robust solution because, within a given provider organization, patients often have more than one number due to the multiple patient and information management systems in use that are not interfaced with each other.

The HIO's role is to accommodate the multiple naming conventions in use across provider organizations by managing the patient identity and matching process for incoming electronic clinical information. By maintaining a master patient index, they can uniquely identify each patient so that clinical information can be shared across provider organizations in a manner that supports successful patient identification and matching at each receiving provider organization. However, when patient identity and matching policies are not applied consistently at the provider organiza-

tion, the logic built in to the interface with the HIO fails to work and the HIO may incorporate a temporary name as a real patient in their master patient index. For example, a given hospital's naming convention may be to use gender (female/male) as the first name and a rotating list of colors as the last name. If an unconscious male patient arrives at the hospital, and he is incorrectly entered into a hospital's electronic health record as "Man Brown" instead of "Male Brown," when the hospital shares the clinical documents associated with this admission with the HIO, the interface would fail to identify "Man Brown" as a temporary name and a new person would be added to the HIO's master patient index as "Man Brown." Clinical information associated with "Man Brown" could then be electronically sent to other provider organizations identified as one of the patient's providers, further propagating this failure in the patient identification and matching process and potentially creating false patients in multiple electronic record systems. Many provider organizations require active consent by their staff or providers to create new patient records when receiving electronic health information from an outside organization through an interface because of this issue. As a result, clinical information necessary for patients to receive safe and effective care may be incorrectly attributed to a false name or rejected by the receiving electronic record system because of intervention by staff or providers.

In addition, if another unconscious male patient is admitted at a later date and the same failure to follow the naming convention occurs at the same point in the color rotation, the records for the most recent patient could be combined with the records of the previous "Man Brown" patient. Once an incorrect match is made and records are merged, it is difficult to go back and appropriately assign each piece of clinical information to the correct patient. Rather than risk propagating incorrect information, the HIO will likely make all the information inaccessible to provider organizations, by tagging the clinical documents so they are not viewable or completely deleting them.

Thus, robust patient identification processes heavily depend on the actions of staff within provider organizations. Since these positions often have relatively high turnover rates, this creates a challenge for provider organizations to consistently apply carefully crafted policies and procedures [17]. Data quality issues such as spelling errors, incomplete patient identifiers, transposition of numbers/letters, and inconsistencies in conventions (such as how to handle hyphenated last names) commonly exist within provider organizations. In the case of HIE, data quality issues are easily spread across the HIO's provider network, posing a risk to patient safety.

Patient matching (ensuring recently created or received health information is added to the correctly identified patient's record) requires constant management within a provider organization and HIO. There is a fine balance between how patient linkages are managed. Too stringent and the result is patients with multiple records and providers potentially missing critical information because they fail to find each of the records. Too flexible and patient records may get inappropriately combined resulting in inaccurate clinical information contained in the patient record.

To illustrate these issues in greater detail, the case study below features a mature HIO that maintains a comprehensive master patient index to uniquely identify

patients and a provider index to uniquely identify providers. The HIO sends and receives electronic clinical information to and from provider organizations through interfaces and provides a community-wide health record (i.e., a clinical data repository) that allows providers to query across provider organizations for clinical information on individual patients.

Case Study

Clinical Summary

William Tell presents to the emergency department at a local hospital with severe pain due to a migraine. During his oral history and physical, he relays that he is taking Metoprolol (a medication to prevent the onset of migraines), 100 mg strength, twice daily. He reports a history of breakthrough migraines requiring Vicodin at least twice a year. As part of the patient's work-up, the physician resident logs in to the HIO's community-wide health record and searches for the patient. He compares demographic information reported to him by the patient to the information available in the community-wide health record—and finds a match with the same first and last name, and date of birth. While William Tell provided additional information, such as his most recent address, this information was missing in the community-wide health record. When the resident looks at the problem list from the matched record in the community-wide health record, he finds migraines along with several other diagnoses associated with severe pain, many different pain medications that have been prescribed previously, and visits to multiple emergency departments. These elements raise the resident's concern about the possibility that William Tell is a drug seeker. The resident reports this information to the attending who decides to decline Mr. Tell's request for Vicodin and instead prescribes Ketorolac. Mr. Tell has a history of kidney dysfunction but this information is not uncovered during the history taking and is not included on the problem list. Ketorolac is contraindicated for persons with kidney dysfunction. Mr. Tell leaves the emergency department and follows the care plan. He returns in several days with signs and symptoms of kidney failure.

Analysis

The resident and physician were provided with clinical information that they believed was appropriately linked to their patient, Mr. Tell, and as a result are concerned that he may be a drug seeker. In reality, the patient in the scenario, William Tell (DOB 11/6/65), was a migraine sufferer and only sought emergency care twice a year. The clinical information that the resident accessed about Mr. Tell was inaccurate due to clinical information shared with the HIO for William Tell (DOB 6/11/65) inappropriately attributed to William Tell (DOB 11/6/65). This misattribution could be due to

data quality issues at the provider organization in patient identifying characteristics, the lack of necessary identifying characteristics included with the clinical information, or a matching algorithm at the HIO that is not sufficiently stringent.

Solutions

Policy: To ensure robust patient identification and matching, multiple and broad infrastructure changes are critical. The Office of the National Coordinator for Health Information Technology with the US Department of Health and Human Services commissioned a project to evaluate current efforts to improve patient identification and matching, and provide recommendations for future efforts. The draft recommendations were reviewed by more than 150 organizations including health systems, HIE organizations, EHR vendors, and vendors of HIE solutions. The final report, released in February 2014, provides recommendations that require action at multiple levels: from federal policy to EHR vendors, HIE organizations, and health care providers. The recommendations include infrastructure improvements, such as standardizing patient identifying attributes and including these attributes when information is electronically exchanged between provider institutions. Increasing and standardizing patient identification attributes would first require enhancements to EHRs. Therefore, the report recommends expanding the list of attributes currently required in EHRs that are federally certified to include elements that would facilitate efforts to improve matching efficiency and accuracy, but are not commonly present, such as a previous last name, middle name, and home/business/cell phone numbers [17].

Provider Organization. Until a more robust policy and certification framework is in place, provider organizations need to focus on improving patient identification and matching procedures in order to prevent errors. As one example, an interventional study conducted at Montefiore Medical Center targeted patient identification errors in newborns [18]. They created a distinct naming convention to replace the common practice of naming newborns with temporary names such as "BabyGirl/Baby Boy MOTHER'S LAST NAME." The study used a pre-validated algorithm to detect "near miss, wrong patient errors" in their computerized provider order entry system by identifying orders placed on one patient, retracted and then placed on another patient. They estimated a 49.9 % reduction in errors for individual orders and a 25.1 % reduction in errors for multiple orders by the same physician for the same patient during the same log-in episode. Implementing technical approaches to improve naming and other key pieces of documentation in provider organizations would not only decrease errors stemming from patient identification and matching in the context of HIE, but also improve patient safety within provider organizations themselves.

A complementary strategy within provider organizations is continuous and regular training for clinicians and other staff to ensure consistent and reliable application of standards, policies and procedures related to patient identification and matching, such as naming protocols and critical patient identifiers. If patient identification and

matching are critical to patient safety, staff training is essential; there must be an expectation in the community of provider organizations that they will train staff on policies and procedures as well as support strategies for accurate and consistent data entry to minimize data quality problems. Provider organizations should be encouraged to reevaluate staff positions that are essential to patient identification and matching in order to ensure they are designed to encourage retention of employees or to ensure consistently high performance.

Errors Related to Efforts to Protect Patient Privacy

HIOs and other HIE efforts prioritize patient privacy protections to comply with state and federal law as well as to meet the expectations of provider organizations that have entrusted HIOs with the protected health information of their patients. If provider organizations question the HIO's ability to protect patients' privacy, they will not share clinical information through the HIO. If patients question the HIO's ability to protect their privacy, they will actively prohibit their information from being shared with the HIO. As a result, HIOs invest in (1) specific and detailed Data Use Agreements (DUAs) with their provider organization participants; (2) policies and procedures for the maintenance and use of protected health information; and (3) privacy and security officers to monitor usage, conduct audits of access and guide response to privacy and security inquiries by patients and provider institutions.

Patient privacy is regulated by state and federal law. States may have privacy laws that are more stringent than federal laws, particularly with regard to mental health. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides a foundation for privacy and security protections of health information in the US HIPAA regulates the electronic sharing of protected health information [19]. Protected health information is defined as clinical information that would identify a person and relay information about a past, current, or future medical condition, treatment, or payment for health care services [20].

Patient consent procedures determine whether patient information is accessible to providers participating in an HIO. As background, HIPAA requires patient consent when a provider queries for or requests information about a patient that resulted from care that the patient received from another provider. (That is, if a provider orders a diagnostic test, the ordering provider is not required to seek patient consent in order to receive the results of the diagnostic test. The patient's consent is assumed, given that they complied with the provider's order to have the test.) For example, a patient arrives indicating they were at an urgent care center or emergency department two nights ago and were told to follow-up with their primary care provider. In order to provide effective follow-up care, the primary care provider must be able to access these records. However, to access the information from the urgent care center or emergency department, the patient's consent is required by HIPAA (whether access is obtained for paper records or electronic access).

In the context of HIE, there are two primary models of patient consent: opt-out and opt-in. The opt-out model assumes inclusion of all patients and their associated health information in the HIO unless a patient opts-out from allowing the HIO to share their information across provider organizations in support of their care. Opt-in requires advance consent from patients to allow their information to be shared. In practice, there are many differences in how each model has been implemented. For example, one hybrid approach to patient consent is to treat patient information for physical health as opt-out while behavioral health information requires a patient to opt-in to allow this information to be shared with other providers. Behavioral health data has additional protections beyond HIPAA (including 42 CFR Part 2 that requires federally funded substance abuse treatment centers to obtain patient consent to disclose patient identifiable information) and state laws that may be more restrictive than either HIPAA or 42 CFR Part 2 [21]. This hybrid consent model requires technology that is capable of managing a sophisticated set of rules related to data type (mental health, substance abuse, or physical health) and level of consent (yes to physical, no to behavioral; yes to both but only specific providers, etc.) that is not routinely available within HIOs. Many HIOs are limited by their technology to an all or nothing strategy in which all information on a patient is available or none is available. As a result, the majority of HIOs work with participating provider organizations to filter out behavioral health data from what is shared. This can lead to patient safety challenges when a patient's behavioral health information influences the safest and most effective course of treatment for physical health concerns.

To illustrate these issues in greater detail, the case studies below feature the same mature HIO as the prior case study. In the first case study, the HIO features an opt-in consent model. In the second case study, the consent model is also opt-in but is further complicated by the patient's substance abuse which is not shared with the HIO or maintained in the community health record (for the reasons cited above).

Case Study

Clinical Summary 1

John Jones, age 14, visits his pediatrician because of diarrhea and abdominal cramps. His pediatrician suspects salmonella and orders a culture for verification. Before the results and diagnosis are provided to the patient, John is in an automobile accident with his mom. His care requires admission to the local community hospital, Better Health Hospital, for an overnight stay. His pediatrician is not associated with Better Health Hospital and the culture is run at Good Care Hospital. Better Health Hospital reviews John's medical record and queries the community-wide health record. Since John's parents have not provided consent to the HIO to allow treating providers to access medical information about John, Better Health Hospital cannot see the culture results shared by Good Care Hospital. As a result, John is not placed in contact isolation, exposing other patients and staff to Salmonella.

Clinical Summary 2

Kendall Smith is a 51-year-old female who has struggled with alcoholism for 20 years. She has received treatment at the local substance abuse treatment center but has had difficulties remaining free from alcohol. She stopped drinking a day and a half ago. Her daughter brought her into the emergency department because she started having seizures. Kendall is deeply ashamed of her alcohol dependency and refuses to acknowledge it. Her daughter is an adult living in another household and believes her mother quit drinking over 10 years ago. During the history and physical, neither the patient nor her daughter provides information on the recent withdrawal from using alcohol. The staff review information about Kendall in the community-wide health record but find no information that could inform them as to the cause of the seizures. As a result, Kendall undergoes several diagnostic tests including a lumbar puncture and cranial CT. Based on the findings, the treating physician rules out other diagnosis and determines that Kendall is suffering from withdrawal. Treatment to control her symptoms and provide supportive care is delayed many hours as a result of the lack of the information, and Kendall is subject to multiple and unnecessary invasive and expensive diagnostic tests.

Analysis

These cases demonstrate the challenges of balancing patient privacy needs with patient care needs. Clinical Scenario 1 describes a situation in which a patient elects to prevent his clinical information from being shared within an HIO and as a result exposes other patients to a disease that is potentially dangerous. Clinical Scenario 2 describes a similar situation in which a patient's decision to restrict access to their behavioral health information results in unnecessary diagnostic testing, causing pain and discomfort to themselves, and inefficient use of resources. In both scenarios, all protocols and procedures were followed and the systems worked as designed. As a result, there is no human, process, procedure, or computer program to hold accountable for this failure. In fact, many would argue that it is not a failure but a limitation of meeting our culture's expectations for information privacy. Regardless, both reveal patient safety challenges associated with HIE.

Solutions

Policy: These cases highlight the limitations of current mechanisms for protecting patient privacy in the context of HIE and the need to update regulations to accommodate new technologies while continuing to protect patient privacy.

The first case demonstrates the limitations to sharing critical health information across provider organizations in order to avoid hospital-acquired infections—a major patient safety issue. Respecting the patient's request to not share their medical records through the HIO's community-wide health record placed other patients

and community members at risk. When the exchange of this information is allowed, there are some important efforts that demonstrate how HIOs can support infection prevention. Kho and colleagues studied patients with Methicillin-resistant *Staphylococcus aureus* (MRSA) who received care from multiple provider institutions to determine whether the second provider institution was aware of the MRSA diagnosis made at the first institution. They found that while less than 3 % of the patients with a history of MRSA infection or colonization ($n = 8895$) sought care at more than one provider institution, those patients who did ($n = 286$) generated more than 4000 inpatient days at hospitals unaware of patients' prior MRSA diagnosis. The researchers tested an intervention that sent a clinical reminder through an HIO to the second provider institution to alert its infection control team when patients with a history of MRSA were admitted to their facilities. The program reported delivering 500 such cross-institutional alerts in the first year of operation [22].

The second case demonstrates the challenge of balancing privacy for patients who have sought mental health or substance abuse services with obtaining clinical information needed to provide these patients safe and cost-effective care. There are ways to explore how technology can facilitate an approach to electronic exchange of behavioral health data that respects patient privacy concerns. The Office of the National Coordinator funded a Behavioral Health Data Exchange Consortium to identify and address challenges to exchanging behavioral health information. The consortium made a number of recommendations. They determined that to comply with more stringent consent requirements for sharing mental health and substance abuse information, the most expeditious route to enabling behavioral health HIE is to center these efforts on directed communications between providers [21]. While this strategy limits the approach to HIE to one-to-one communications between providers, and does not enable the type of query-based access to a community-wide health record that would have allowed providers to better care for Kendall Smith, it does represent a means for sharing patient-specific behavioral health care information.

Provider Organization: While the root causes of these HIE-related patient safety failures require policy changes, provider organizations are in a strong position to shape patient expectations for information privacy while providing the most appropriate, safe, and cost-effective care. In addition, while providers are obligated to protect clinical information shared with them, they can educate their patients about the benefits of allowing their information to be shared and the protections in place to prevent inappropriate access to their personal health information. However, for providers to be effective in this patient education capacity, they must have assurances that systems are in place, followed and monitored to protect their patients' information, both by the HIO and by other providers connected to the HIO. Once reassured, providers can discuss with patients their specific risks when other health care providers lack relevant clinical information, both physical and behavioral health.

Key Lessons Learned

- While there are many ways in which HIE can promote patient safety by making more complete information available to providers across care delivery settings, HIE also introduces opportunities for new types of patient safety failures.
- The two primary opportunities for failures relate to (1) patient identification and matching, and (2) patient consent.
- With patient identification and matching, safety can be compromised when clinical information is attributed to the wrong patient or is unavailable due to failure to match with a patient.
- With patient consent, safety can be compromised when critical health information is unavailable that impacts a patient's diagnosis or course of treatment.
- There are, however, a key set of actions that can be taken by policymakers and by provider organizations to mitigate these potential patient safety failures. They are as follows:

Policy Efforts to Avoid Patient Safety Failures from HIE

- Support implementation of the infrastructure improvements suggested by the Office of the National Coordinator for Health Information Technology in their February 2014 report, such as standardizing patient identifying attributes and including these attributes in messages exchanged between provider institutions.
- Update regulations related to patient consent and privacy to accommodate HIE.
- Encourage innovation for how HIE technologies can facilitate the exchange of behavioral health information while complying with state and federal rules and regulations and meeting patient expectations.

Provider Organization Efforts to Avoid Patient Safety Failures from HIE

- Continuously manage and improve efforts to accurately and consistently identify patients, with a particular focus on unique naming conventions for newborns and unconscious patients.
- Provide sufficient training to clinicians and staff to follow policies and procedures related to patient identification and matching.
- Provide leadership to guide efforts to meet patient expectations for privacy while engaging in HIE to support safe, appropriate, and cost-effective care.
- Continue to serve as patient advocates and protectors while educating patients on the importance of allowing their information to be shared across providers.

References

1. Pham HH, Schrag D, O'Malley AS, Wu B, Bach PB. Care patterns in Medicare and their implications for pay for performance. N Engl J Med. 2007;356(11):1130–9.
2. Finnell JT, Overhage JM, Dexter PR, Perkins SM, Lane KA, McDonald CJ editors. Community clinical data exchange for emergency medicine patients. AMIA Annual Symposium Proceedings. American Medical Informatics Association; 2003.
3. Bodenheimer T. Coordinating care – a perilous journey through the health care system. N Engl J Med. 2008;358(10):1064–71.
4. Rudin RS, Motala A, Goldzweig CL, Shekelle PG. Usage and effect of health information exchange: a systematic review. Ann Intern Med. 2014;161(11):803–11.
5. Smith PC, Araya-Guerra R, Bublitz C, et al. Missing clinical information during primary care visits. JAMA. 2005;293(5):565–71.
6. Bell CM, Schnipper JL, Auerbach AD, Kaboli PJ, Wetterneck TB, Gonzales DV, et al. Association of communication between hospital-based physicians and primary care providers with patient outcomes. J Gen Intern Med. 2009;24(3):381–6.
7. van Walraven C, Taljaard M, Bell CM, Etchells E, Stiell IG, Zarnke K, et al. A prospective cohort study found that provider and information continuity was low after patient discharge from hospital. J Clin Epidemiol. 2010;63(9):1000–10.
8. Franczak MJ, Klein M, Raslau F, Bergholte J, Mark LP, Ulmer JL. In emergency departments, radiologists' access To EHRs may influence interpretations and medical management. Health Aff. 2014;33(5):800–6.
9. Shapiro JS, Kannry J, Kushniruk AW, Kuperman G, The NYCLIX Clinical Advisory Subcommittee. Emergency physicians' perceptions of health information exchange. J Am Med Inform Assoc. 2007;14(6):700–5.
10. Adler-Milstein J, Bates DW, Jha AK. Operational health information exchanges show substantial growth, but long-term funding remains a concern. Health Aff. 2013;32(8):1486–92.
11. Adler-Milstein J, Desroches C, Jha A. Health information exchange among US hospitals. Am J Manag Care. 2011;17(11):761.
12. Vest JR. More than just a question of technology: factors related to hospitals' adoption and implementation of health information exchange. Int J Med Inform. 2010;79(12):797–806.
13. Grossman JM, Kushner KL, November EA. Creating sustainable local health information exchanges: can barriers to stakeholder participation be overcome? Center for Studying Health System Change (HSC). Research brief No. 2. 2008. Accessed 4 Apr 2015 from http://www.hschange.org/CONTENT/970/.
14. Grossman JM, Cohen GR. Despite regulatory changes, hospitals cautious in helping physicians purchase electronic medical records. Issue brief. Center for Studying Health System Change (HSC). Report No. 123. 2008. Accessed 4 Apr 2015 from http://www.hschange.org/CONTENT/1015/.
15. Katz A, Bond AM, Carrier E, Docteur E, Quach CW, Yee T. Cleveland hospital systems expand despite weak economy. Community report. Washington, DC: Center for Studying Health System Change (HSC). Report No.2. 2010. Accessed 4 Apr 2015 from http://www.hschange.org/CONTENT/1154/.
16. Kaelber DC, Waheed R, Einstadter D, Love TE, Cebul RD. Use and perceived value of health information exchange: one public healthcare system's experience. Am J Manag Care. 2013;19(10 Spec No):SP 337–43.
17. Morris G, Farnum G, Afzal S, Robinson C, Greene J, Coughlin C. Patient identification and matching final report. Baltimore, MD: Office of the National Coordinator for Health Information Technology; 2014. Prepared for the Office of the National Coordinator for Health Information Technology.
18. Adelman J, Angert R, Southern W, Schechter C, Aschner J, Ral A, et al. Changing the first name of NICU patients to reduce wrong-patient orders. AAP Experience National Conference and Exhibition, Washington, DC. 2014.

19. US Department of Health and Human Services. Summary of the HIPAA privacy rule. Accessed 6 Apr 2015 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html. Last.
20. Office of the National Coordinator for Health Information Technology. Guide to Privacy and Security of Health Information. 2012.
21. Behavioral Health Data Exchange Consortium. ONC State Health Policy Consortium Project final report. In: Office of the National Coordinator for Health Information Technology, editor. 2014. Accessed 6 Apr 2015 from http://www.healthit.gov/sites/default/files/bhdeconsortiumfinalreport_06182014_508_compliant.pdf.
22. Kho AN, Lemmon L, Commiskey M, Wilson SJ, McDonald CJ. Use of a regional health information exchange to detect crossover of patients with MRSA between urban hospitals. J Am Med Inform Assoc. 2008;15(2):212–6.

Part III
Specialty Considerations

Chapter 13
Safety Considerations in Radiation Therapy

Eric C. Ford and Michael G. Herman

Introduction

Over half of all cancer patients will receive radiation therapy in the course of their disease management, often with curative intent. This care is delivered in a complex environment involving multiple healthcare professionals and utilizing advanced software and hardware systems with associated interfaces. The complexity is also growing quickly with time, a fact that is partially reflected in the large growth rate of healthcare expenditures which has received attention recently [1]. Such a complex and evolving environment presents challenges to delivering safe and effective care and many of the challenges involve information technology (IT) components.

To illustrate the complexity, Fig. 13.1 shows a typical workflow for a cancer patient receiving a course of radiation therapy [2]. This workflow is somewhat unique in healthcare since many of the tasks are accomplished on a "virtual patient" (typically a CT scan), and this work is extended over many days prior to the treatment of the patient (blue sections of Fig. 13.1). The actual patient treatment (red section of Fig. 13.1) typically only lasts several tens of minutes, though it also involves complex software and hardware systems. From Fig. 13.1 it can be appreciated that there are at least four distinct professional groups involved in planning and delivering treatment and there are numerous handoffs between these groups. During this process the electronic medical record (EMR) plays a central role. It is increasingly being used as a communication tool, a purpose that it was often not designed for. It is also true that most hospitals and many free-standing clinics use multiple

E.C. Ford, Ph.D. (✉)
Radiation Oncology, University of Washington, 1959 NE Pacific St,
Box 356043, Seattle, WA 98195, USA
e-mail: eford@uw.edu

M.G. Herman, Ph.D.
Radiation Oncology, Medical Physics, Mayo Clinic, 200 First St. SW,
Rochester, MN 55905, USA
e-mail: herman.michael@mayo.edu

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_13

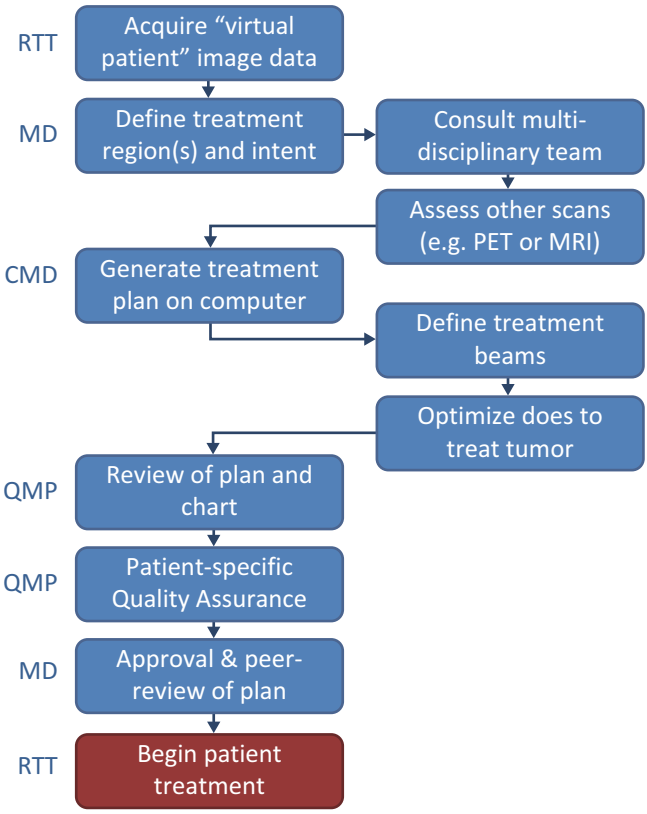


Fig. 13.1 Representative workflow for radiation therapy treatment planning. The radiation oncology professionals primarily responsible for each step are indicated: radiation therapy technologist *RTT*, medical doctor *MD*, certified medical dosimetrist *CMD*, and qualified medical physicist *QMP*. Adapted from reference [2]

EMR systems. A breast cancer patient's chemotherapy, for example, may be scheduled and managed by one system while her radiation therapy is managed by another. Though it may be critical to synchronize the delivery of chemotherapy with radiation therapy, these two IT systems are often not interconnected in any way.

Given this complexity, it is remarkable that radiation oncology is as safe and effective as it is. This is a testament to the concerted efforts on quality control over the years. Reliable data are not available, but estimates of error rates range from 0.2 to 5 % [3, 4]. There is room for improvement to bring it in line with other healthcare disciplines such as anesthesiology or cardiology [5]. The gap in quality is illustrated powerfully by several recent reports on radiation oncology trials and plan quality. In one multi-institutional trial for head-and-neck cancer, it was observed that the quality of the radiation therapy plan was uniquely predictive of the overall survival of patients [6]. This observation is borne out in other radiotherapy trials as well [7].

The explicit link between quality and outcome represents a future direction for research in healthcare and radiation oncology may be in a unique position to contribute, given the wealth of information that is collected during the course of therapy.

The following two cases outline examples of possible error pathways in the coordination and delivery of radiation therapy. These examples are selected on the basis of the specific involvement of IT systems.

Case Studies

Clinical Case #1

Clinical Summary

In 2005 Scott Jerome-Parks, a 41-year-old computer and systems analyst living in New York City, developed an oropharyngeal cancer in the base of his tongue [8, 9]. He had volunteered for cleanup at the site of the World Trade Center and at least one clinician believed that his exposure there may have caused his cancer. A decision was made to treat his disease with radiation therapy with the intent of curing it. On March 8, 2005 he began treatment. In such cases, radiation treatments are typically delivered once per day over the course of approximately 7 weeks. The process followed the steps in Fig. 13.1. Mr. Jerome-Parks' treatments proceeded normally for 4 days, but then in advance of his fifth treatment day, his radiation oncology physician decided to modify the radiation treatment plan in order to further spare his mandible and teeth. This is a relatively common practice and is intended to provide the best care possible. In the course of modifying the plan, however, an error occurred which would prove devastating.

The modification of the treatment plan started on a Monday morning with the goal of having a modified plan ready for his treatment later that day. The computer system used for treatment planning crashed but the planner was able to reboot it and proceed on with the work. Unknown to her, however, the crash had caused the database to revert to a partially saved state in which some pieces of the information were stored correctly but others were not. In particular, there was a file that contained incorrect positions for the multileaf collimator (the device that controls the shape of the radiation beam). The shape of the beam was therefore inaccurate and, because the leaf motion was incorrect, the resulting radiation dose per treatment was drastically different than prescribed. The new plan delivered ~700 % of the intended dose. The flawed treatment continued, unnoticed, that Monday afternoon and for the next 2 days delivering a 700 % overdose each time over 3 days. At this time Mr. Jerome-Parks experienced an acute and toxic reaction with facial swelling and nausea. His reaction was not understood or fully appreciated by his care team. After the third treatment, a quality assurance measurement of the plan was performed. It was this measurement that revealed that there was an error. Treatment was stopped. Mr.

Jerome-Parks, however, had received a toxic overdose of radiation, and there was no effective cure or treatment option available. In February of 2007, after nearly 2 years of pain and deteriorating health, Scott Jerome-Parks died.

Analysis

This case demonstrates the safety risks of nearly complete reliance on IT that now pervades the radiation therapy treatment environment, as well as a limited understanding of the potential problems with a complex, computer-controlled healthcare technology. A single computer crash can produce catastrophic consequences. Furthermore, this software and hardware is not static but develops and changes at a rapid pace. If Mr. Jerome-Parks' disease had developed 5 years earlier, for example, the complex technology would likely not have even existed in the clinic where he was treated.

This case also illustrates the occurrence of an error when extra complexity is introduced. In this case a change was introduced to a plan that was already under treatment. This introduced an extra complexity and created an additional risk point. Data suggests that treatments that occur under complex and stressful circumstances such as an emergent case are significantly more risk prone [10].

One way to view this accident is to focus on the many missed opportunities in which the error could have been identified. Perhaps a medical physicist should have run a measurement of the plan before treatment started. Perhaps a radiation therapist at the treatment console should have noticed the errant pattern of radiation field collimation. Perhaps a member of care team should have recognized clinical symptoms earlier on. This approach to understanding human error, however, is largely counterproductive. This "could have, should have, would have" approach is subject to hindsight bias and ignores the fact that, at the time that events were unfolding, only partial information was available to the people involved. The true patterns of events and "correct" decisions are clear only after the fact. An excellent description of this issue and its drawbacks can be found in work by Sidney Dekker [11]. Instead of focusing on retrospective analysis of what should have happened, it is more productive to study the environment and ask the question: why did these well-meaning people make the decisions that they did?

When viewed in this light, one clear causal factor in the mistreatment of Scott Jerome-Parks was a deficiency in the human–computer interface. At least five people might have recognized that there was a serious error in the plan, but the computer interface and environment were not designed to provide obvious indicators. There were certainly no hard interlocks or explicit signs warning the user of a potential problem. The principles of human factors engineering and usability (UX) have received much attention [12] but healthcare IT systems continue to be designed with interfaces that are not in accordance to best practices.

At another level, the tragic death of Scott Jerome-Parks had other consequences for the discipline of radiation oncology. The high-profile nature of this story gener-

ated a great deal of well-deserved attention that affected change. In 2010 a national "call to action" meeting was organized by one of us (MH) [13] and out of that came the "Target Safely" initiative from the American Society for Radiation Oncology (ASTRO). One component of this is the RO-ILS™: Radiation Oncology Incident Learning System, whose mission is to facilitate safer and higher quality care by providing a mechanism for shared learning in a secure and nonpunitive environment. The RO-ILS system, launched in June 2014, utilizes a Patient Safety Organization or PSO, a federal system which provides protection of incident information. In addition, through the National Electrical Manufacturers Association (NEMA), radiation treatment device manufacturers have formed a consortium in collaboration with users to help develop consistent computer display/interface terminology and critical information to help users understand potentially dangerous situations.

Solutions and Lessons Learned

One reference suggests that the "lessons learned" from this case are to "work with awareness" and to "be alert" [9]. In our view, this is unlikely to be a long-term durable solution for safety improvement since it assumes that the front-line provider is not already "working with awareness" or "being alert." While clinical care teams need to continue due diligence and adherence to standardized protocols and quality assurance, there is also a need for better design in healthcare IT systems. The design should explicitly account for the socio-technical factors that drive the use (and misuse) of technology. Pioneering proof-of-principle work has been conducted in this realm by the human factors engineering group at the University of Toronto [14] who conducted a prototype redesign of an EMR commonly used in radiation oncology (MOSAIQ, Impac Inc.) and demonstrated that their redesign resulted in a substantially reduced error rate. This work and others like it will hopefully one day propagate into a product. The goal is to make the process (and the interface) as simple and transparent as possible. This becomes crucial in the face of increasing complexity.

This case also highlights the importance for clinics to learn from each other in order to limit preventable mistakes. The newly released RO-ILS system will provide a mechanism for accomplishing this.

Clinical Case #2

The second case example illustrates a common potential error scenario in radiation oncology and how it is related to the IT system in use. That is, the potential treatment of a wrong location. Figure 13.2 shows an example where the center of the radiation beam (cross hairs) is misaligned with the intended target by approximately 3 cm, which is considered a major miss in most situations where radiation therapy

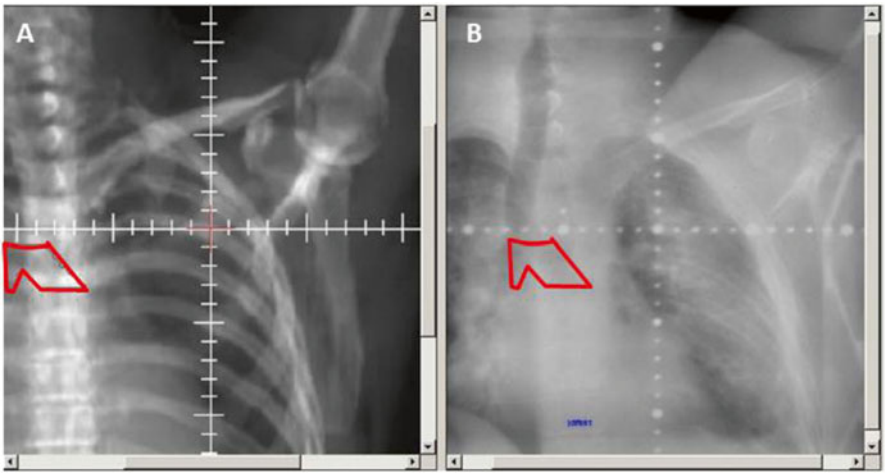


Fig. 13.2 Incorrect treatment location showing the intended treatment location (**a**) and the location that was actually setup for treatment (**b**). For reference the anatomical landmark of the carina is shown in *red*. Each mark on the graticule represents 1 cm

is applied. In this case the error was caught and corrected by means of the films shown in Fig. 13.2, but the cause of the error is interesting to understand and address in order to prevent it in the future.

Figure 13.3 shows the cause of the wrong location error. One of the key procedures is to identify a landmark on the CT scan using the treatment planning computer. The process at work is shown in Fig. 13.3a where a mark is identified (red cross hairs). In this case, however, a surgical drain site was mistakenly identified as the reference mark. The correct landmark should have been the BB that was placed at the time of the CT scan (Fig. 13.3b). The cause of this confusion can be appreciated in Fig. 13.3c. Because the wrong landmark was identified on the planning scan, the wrong location on the patient was ultimately targeted (Fig. 13.2).

Analysis

This case illustrates several valuable learning points. Unlike the first case example, this is not simply a failure of the computer system or a pure software or hardware bug but is a failure of the user to identify the correct information in the computer system. This is partially due to the complex interaction between the user and the computer and the way the information is presented. Such complex failure patterns appear to be much more common than a simple crash or bug [15].

The case also illustrates the importance of standard quality assurance checks. Here the wrong location was identified via a film verification which is considered

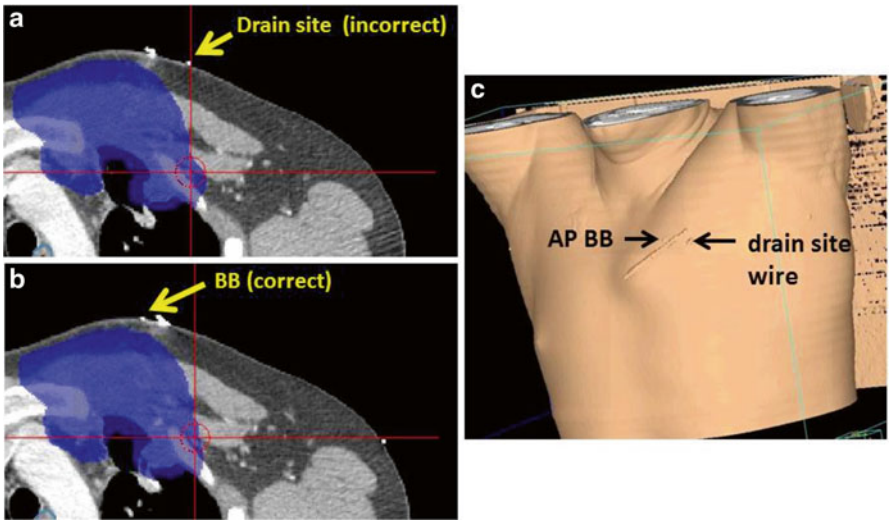


Fig. 13.3 Cause of the incorrect treatment location. A surgical drain site was identified as a landmark on the CT scan during treatment planning (**a**). The correct intended landmark was the *BB* (panel **b**). Because the incorrect reference landmark is selected in the planning computer, the incorrect treatment location is identified on the patient. Multiple markings on the patient (**c**) contribute to this misidentification

standard practice in radiation therapy. It must be recognized, however, that standard quality assurance checks will not identify all errors. Even when all the standard quality assurance checks are employed in their most ideal usage, it appears that some 3 % of errors in radiation therapy may still be undetectable [16].

Solutions

Like the first case example, the error outlined here might be prevented by an improved human–computer interface. Another possible solution is to employ a method to automatically verify the integrity of radiation therapy plans prior to treatment. Currently such verification relies largely on human inspection, but many of the tasks could be more reliably performed by software which evaluates the plan parameters against common error scenarios and/or historical patterns. Prototypes of such software systems have been developed and tested by a handful of academic groups [17–19] but no commercial solutions exist yet. In addition to software solutions, it is possible to measure the radiation doses delivered to a patient during treatment using hardware that exists on most treatment devices. Pioneering work has been done with such an approach by several academic groups [20], but its use is not yet widespread.

Key Lessons Learned

- Radiation oncology is a complex discipline where IT and human factors engineering considerations play a key role in determining the safety and quality of care.
- IT healthcare systems need to be designed with best practices in mind in terms of human factors engineering and the reduction of error.
- Techniques exist to automatically verify the integrity of radiation therapy plans either prior to treatment (via software verification routines) or during the first treatment (via direct measurement of the beam with exiting detectors). Prototype systems exist and should be more widely adopted in the coming years.
- The newly released national incident learning system, RO-ILS™: Radiation Oncology Incident Learning System, should provide valuable information in the coming years as to common error pathways, contribution of IT systems, and methods to prevent and control errors.

References

1. Alhassani A, Chandra A, Chernew ME. The sources of the SGR "hole". N Engl J Med. 2012;366(4):289–91.
2. Ford EC, Fong de Los Santos L, Pawlicki T, Sutlief S, Dunscombe P. Consensus recommendations for incident learning database structures in radiation oncology. Med Phys. 2012;39(12):7272–90.
3. Ford EC, Terezakis S. How safe is safe? Risk in radiotherapy. Int J Radiat Oncol Biol Phys. 2010;78(2):321.
4. Marks LB, Light KL, Hubbs JL, Georgas DL, Jones EL, Wright MC, et al. The impact of advanced technologies on treatment deviations in radiation treatment delivery. Int J Radiat Oncol Biol Phys. 2007;69(5):1579–86.
5. Gaba DM. Anaesthesiology as a model for patient safety in health care. BMJ. 2000;320(7237):785–8. Clinical research ed.
6. Peters LJ, O'Sullivan B, Giralt J, Fitzgerald TJ, Trotti A, Bernier J, et al. Critical impact of radiotherapy protocol compliance and quality in the treatment of advanced head and neck cancer: results from TROG 02.02. J Clin Oncol. 2010;28(18):2996–3001.
7. Ohri N, Shen XL, Dicker AP, Doyle LA, Harrison AS, Showalter TN. Radiotherapy protocol deviations and clinical outcomes: a meta-analysis of cooperative group clinical trials. J Natl Cancer Inst. 2013;105(6):387–93.
8. Bogdanich W. A Lifesaving Tool Turned Deadly. Radiation offers new cures, and ways to do harm. New York Times. 2010. http://www.nytimes.com/2010/01/24/health/24radiation.html?_r=0
9. International Atomic Energy Agency. IAEA training materials: module 2, prevention of accidental exposure in radiotherapy, Vienna. 2009. https://rpop.iaea.org/RPOP/RPoP/Content/AdditionalResources/Training/1_TrainingMaterial/AccidentPreventionRadiotherapy.htm. Accessed 23 Dec 2014.
10. Thomadsen B, Lin SW, Laemmrich P, Waller T, Cheng A, Caldwell B, et al. Analysis of treatment delivery errors in brachytherapy using formal risk analysis techniques. Int J Radiat Oncol Biol Phys. 2003;57(5):1492–508.

11. Dekker S. The field guide to understanding human error. Aldershot, England; Burlington, VT: Ashgate; 2006. p. xv, 236 pp.
12. Norman DA. The design of everyday things. New York: Basic Books; 1988.
13. Hendee WR, Herman MG. Improving patient safety in radiation oncology. Med Phys. 2011;38(1):78–82.
14. Chan AJ, Islam MK, Rosewall T, Jaffray DA, Easty AC, Cafazzo JA. The use of human factors methods to identify and mitigate safety issues in radiation therapy. Radiother Oncol. 2010;97(3):596–600.
15. Terezakis SA, Harris KM, Ford E, Michalski J, DeWeese T, Santanam L, et al. An evaluation of departmental radiation oncology incident reports: anticipating a national reporting system. Int J Radiat Oncol Biol Phys. 2013;85(4):919–23.
16. Ford EC, Terezakis S, Souranis A, Harris K, Gay H, Mutic S. Quality control quantification (QCQ): a tool to measure the value of quality control checks in radiation oncology. Int J Radiat Oncol Biol Phys. 2012;84(3):e263–9.
17. Yang D, Moore KL. Automated radiotherapy treatment plan integrity verification. Med Phys. 2012;39(3):1542–51.
18. Furhang EE, Dolan J, Sillanpaa JK, Harrison LB. Automating the initial physics chart-checking process. J Appl Clin Med Phys. 2009;10(1):129–35.
19. Siochi RA, Pennington EC, Waldron TJ, Bayouth JE. Radiation therapy plan checks in a paperless clinic. J Appl Clin Med Phys. 2009;10(1):43–62.
20. Mans A, Wendling M, McDermott LN, Sonke JJ, Tielenburg R, Vijlbrief R, et al. Catching errors with in vivo EPID dosimetry. Med Phys. 2010;37(6):2638–44.

Chapter 14
Safety Considerations in Pediatric Informatics

S. Andrew Spooner

Introduction

Just as surgical tools designed for adults may not work well in the care of children, health information technology (HIT) designed to document and execute adult care can present risks to a child's health. In child health, there are certain topics that are especially relevant to the kind of care children get [1]: growth tracking (which gives clues to the presence of chronic disease), immunizations (the cornerstone of pediatric preventive care), and medication dosing (usually done per unit of body weight in infants and small children). Furthermore, there are special complexities in identification of children, who regularly undergo name changes near the time of birth and often lack identifiers like social security numbers until later in life. There is added complexity in the interpretation of data whose norms change with age (such as height, weight, vital signs, and laboratory values). Lastly, adolescent health care entails special problems in health information privacy, owing to the sensitive nature of care as children mature into adulthood. In addition, the complexity of managing patients who are dependent on their parents/guardians for health care decision-making makes the use of HIT more complex for clinical users. Greater complexity in any system increases the risk of error, including the new kinds of errors we now see in electronic health record (EHR) systems.

Current literature on HIT-related safety issues in pediatrics tends to focus on medication dosing errors [2–7], although there could be other errors stemming from inadequate handling of variation in body size like radiation dosing in diagnostic radiology [8] or damage from inappropriately sized equipment.

S.A. Spooner, M.D., M.S. (✉)
Department of Pediatrics, Cincinnati Children's Hospital Medical Center, University of Cincinnati College of Medicine, 3333 Burnet Avenue, MLC 9009, Cincinnati, OH 45229, USA
e-mail: andrew.spooner@cchmc.org

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_14

The following three case studies illustrate potential unintended consequences of the use of HIT in pediatric settings due to risks associated with medication management at varying body weights and developmental stages. Practical solutions to mitigate these risks are also presented.

Case Study 1

Clinical Summary

A 3-month-old, former 32-week-gestation infant was admitted to room 320 of the pediatric intensive care unit (PICU) after being evaluated and treated in the emergency department for sepsis. The patient was started on appropriate-for-weight intravenous antibiotics and pressors. Shortly after this, a nurse on another unit opened the patient's chart inadvertently; she had meant to open the chart of a patient on her unit, but accidentally opened the wrong unit census list and ended up opening the chart of the patient in room 320 instead of room 420. The patient picture that appeared in the header was not helpful in alerting her to the error, since both patients were infants and looked substantially similar at the low resolution provided. The patient in room 420 was much older than the one in 320, but his picture had not been updated in several months. The nurse entered the body weight of the patient in 420 for the patient in 320; as a result the weight recorded was approximately double what it should have been. The system did not display an alert for the wrongly entered weight since the weight entered would have been normal for the typical 3-month old. After this data entry, a physician working in the PICU calculated an adjustment to the patient's continuous infusion of pressors, and noticed that it was markedly different from the current rate. Investigating further, she asked the parents at the bedside what the patient's weight is. They told her the baby's weight in pounds, which the doctor entered into her weight-based order in kilograms (units in children's hospitals tend to be in metric units, despite US parents' lack of familiarity with them). Before she could enter the new order, the patient experienced an acute deterioration that must be remedied by the code team by the use of resuscitation drugs. Because no one had had time to print up a weight-based code sheet, standard, adult doses of resuscitative medications were used, causing a significant overdose.

Analysis

Wrong-patient errors have been reported [9, 10], usually in the context of prescribing an incorrect medication after the wrong patient has been selected from a list. EHRs have mechanisms to reduce the likelihood of wrong-patient selection, like highlighting similar names in lists and placing photographs of the patient at the top

of each screen. More sophisticated methods for intercepting wrong medication orders, like comparing medications to medical problems [10], have been developed but are not widely implemented. Perhaps because body weight is not as critical to medication safety in adults, wrong-patient errors for body weight data entry have not been recognized as a common class of error in the EHR safety literature. There are other mechanisms for weight data-entry error besides wrong-patient selection: units confusion (pounds/kilograms/grams), typographical errors (dropped or duplicated digits), transposition (weight entered as height and height as weight when both are being entered), and failure to accommodate the tare weight of medical equipment like wheelchairs. EHRs typically possess mechanisms for validating these data that allow detection of errors, but in current designs most users override most drug alerts and presumably all other types of alerts as well [11–13].

In this case, the mechanisms put in place to reduce the likelihood of wrong-patient errors were ineffective due to characteristics inherent in pediatric populations such as rapid change in body size (which made old patient-identification photographs ineffective) and the lack of applicability of normative weight data in a common growth aberration (prematurity). The root cause (picking a patient based on room number vs. more specific patient identifiers) is not unique to pediatrics, but the system offered no protection against such a common error because the patients were infants.

Solutions

There are supports for decision-making that can mitigate all of the above errors:

- Policies requiring that the identification photographs in rapidly growing infants be updated at reasonable intervals to better discriminate identity.
- Decision support (alerts, flags) in the EHR that compares the entered weight to expected weight for age (based either on age-based norms or, more importantly, previous growth patterns or patterns specific to a diagnosis like prematurity). Preferably, this decision support should be a part of the ordering process, so that medication errors can be intercepted in time. Figure 14.1 illustrates a display that could be used to interrupt ordering. Practitioners could proceed through this alert if no orders were weight sensitive, then correct the weight later.
- Decision support that compares entered weight to expected weight based on previous entries.
- Requirement that units (pounds vs. kilograms) be entered along with weights—possibly with specific detection for errors reflecting a factor of 2.2.
- Preprinted, age- and weight-specific "code" (cardiopulmonary resuscitation) sheets that allow clinicians to correlate what they know (age, weight, stage of prematurity) with drug doses or equipment sizes.

Many of these interventions rely on the use of an alert presented as part of the EHR user interface. The salience of these alerts for the clinician depends on the trust

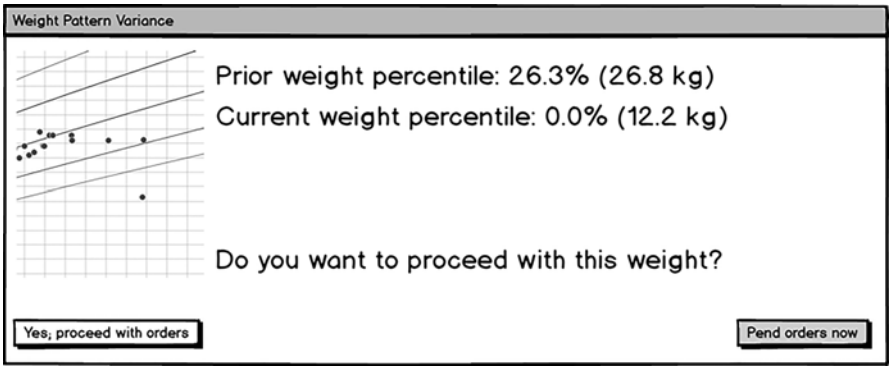


Fig. 14.1 Example of an alert that would present a pediatrician enough context to be able to judge the severity and validity of a weight error during the ordering process. A fragment of the growth chart is shown, since this view illustrates the recent growth pattern and allows comparison to the potentially erroneous entry

that user has in the system and the extent to which the user has become acclimated to alerts. "Alert fatigue," where users ignore most or all alerts, can be a product of alert overload and of failure of trust. This topic is discussed in greater details in Chap. 4 in this book.

Most EHRs used in pediatric settings offer some form of weight-based dosing functionality, where a user can use an actual or estimated body weight to calculate an appropriate dose. Users can use pre-configured, weight-based doses to create orders that meet accepted dose ranges, e.g., 90 mg/kg/day for amoxicillin. These systems can check these doses against the body weight as part of order validation as well. This kind of decision support works well for most prescribing, but it breaks down entirely when the weight is wrong. Systems can implement checks of entered weight against what is expected using age-based norms from the CDC [14] or World Health Organization [15] or against previously entered weights (e.g., whether the current data point is more than a certain percentage above or below the previously entered one). More sophisticated error detection can be employed by incorporating the expected percentile based on previous percentiles, so that the weights of patients who do not fall within the "normal" range (premature infants, patients with chronic disease, obese children) can be monitored for unexpected variation. The growth chart, pictured in Fig. 14.2, is typically what pediatricians use to judge growth patterns or the validity of entered weights. Since weights are usually entered into a form with fields or a spreadsheet-like grid, the EHR may depend on data validation alerts to signal aberrations. Since most users override most alerts [12, 16, 17], and most weighing of patients occurs in a different workflow from the prescribing workflow, it is easy to see how an erroneous weight could exist on the chart. In the case where an erroneous weight has survived in the chart due to multiple alert overrides, the prescriber would not necessarily know the weight was in error. A prescriber could examine the recorded weights every time he or she intended to prescribe, but this is not a sustainable habit. Electronic systems could retain the fact that there was

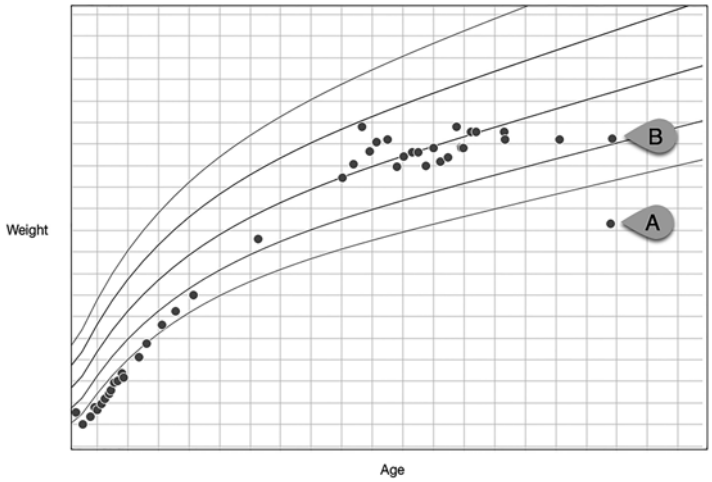


Fig. 14.2 Schematic of a growth chart display in an EHR. *Curved lines* indicate the expected weights at each age based on percentiles taken from normative data published by the Centers for Disease Control [14]. In this case, the growth pattern is irregular, a common finding in children's hospitals where children with prematurity and congenital conditions or chronic disease are treated. The point labeled "*A*" is the aberration that represents a weight data-entry error. The point labeled "*B*" represents a subsequent, correct data entry. While growth charts are generally available in EHRs, weight is typically entered into a grid similar to a spreadsheet, so the context provided by the growth chart is not present at the time of data entry

a recent large weight fluctuation so that a prescriber would be aware that the data may not be trustworthy. This bridging of the patient weighing workflow (performed by a non-prescriber) and the prescribing workflow does not involve any complex functionality, but could improve the reliability of the use of weights in pediatric prescribing.

Even with weight-based dosing support, the lack of agreement as to what those dose ranges ought to be [6] presents a specific challenge to designers of information systems, who cannot provide a universally acceptable standard of functionality in medication dose ranges. Such lack of standardization requires that all systems intended to support pediatric dosing be customized to local practice, which introduces error and unnecessary variation.

Case Study 2

Clinical Summary

An infant is identified through a state newborn screening program as having congenital hypothyroidism. His primary care provider is notified. The primary care provider confirms the diagnosis and starts the patient on an appropriate dose of

thyroxine. The patient is brought to the appropriate appointments in the first 2 months of life, where dose adjustments are made. Because of disarray brought about by family psychosocial circumstances, the patient is not brought in for subsequent well-child encounters. Because the primary care provider lacks the appropriate decision support in his EHR system to identify appointment compliance failures, the lack of follow-up goes unnoticed. The patient is, however, seen in an emergency department (using a separate EHR system) several times for acute illness, where the medication history is confirmed. The parent states that the current dose of thyroxine is the correct one, and is the one that the emergency department physician uses to order the requested refills. One of these encounters involves a bout of viral gastroenteritis with dehydration, during which a creatinine value of 0.9 mg/dL is obtained. Because the clinical laboratory information system in the ED did not support age-based norms, this evidence of acute kidney injury goes unrecognized.

Analysis

Children are dependent on adults for access to care, and, until they reach older childhood, developmentally unable to communicate their own experience as patients. A signal that some aspect of therapy has changed, like a change in symptoms or a change in volume or taste of medication, may remain unknown until problem becomes more obvious to a third party. Therapies and results that are strongly tied to body size, like medication dosing and laboratory norms, require specific features that systems designed for adult care may not possess. In this case, the dependent, rapidly growing patient was not well served by the monitoring functions of the EHR system used. While these deficiencies could have been overcome by a sufficiently trained pediatric provider, even skilled pediatricians can fall victim to placing too much trust in the output of a clinical computing system—one of the ironies of automation [18], made even *less* expected when contrasted with the lack of trust placed in the alerts mentioned in Case 1.

Solutions

- While there is disagreement about what the standard dose ought to be for any given pediatric medication [6], for most common drugs there are local standards and local preferences about drug references. Systems ought to be able to represent typical pediatric doses as default doses and as reference ranges to allow clinicians to tell whether a given dose is reasonable given a patient's weight.

- Norms for laboratory data should be displayed in age-sensitive context, especially in clinical settings where providers see children only rarely.
- EHR systems should provide sufficient registry functionality to allow detection of follow-up failures, especially in cases where poor follow-up has major implications for outcome (congenital endocrinopathies, retinopathy of prematurity, failure to thrive, and developmental dysplasia of the hip to name a few).
- Given the large amount of care that children receive in non-pediatric settings, EHRs in these settings should aim to provide electronic connections to health information exchanges or EHR-based interoperability functions to ensure that care can be integrated across pediatric and non-pediatric settings.

Medication management in pediatric patients has some complexities that are not found to as great a degree in adult medication management [4, 19]. While some research suggests that medication errors are more prevalent in pediatrics than adults [20, 21], it is not yet known whether the specific complexity of prescribing in children is the cause of these increased errors. Nonetheless, children appear to be at increased risk for adverse drug events, and, given the special nature of medication management for these patients, electronic prescribing systems should offer features that help mitigate these risks. Given that children are dependent on their parents or guardians to give medical and medication histories, they are particularly vulnerable to the common phenomenon of discrepancies between reported and prescribed medication [22].

The principal factor that makes prescribing for an infant or child more complex is, of course, the fact that the young are small and their body weight changes more rapidly. But the intricacies of weight-based dosing are not the only issues that can create risk. Neonates can have fundamentally different physiology that can make prescribing and drug monitoring more complex. The difficulty of providing care to adolescent patients, whose care might need to be kept confidential from other members of the family, can create challenges in prescribing. Adolescents pose additional challenges when they take their "pediatric" conditions to adult providers as they age out of pediatric care. Off-label use of medications not approved for use in the young also presents challenges to safe prescribing.

Medications prescribed per body weight early in life require frequent adjustment in dose as the baby gains weight. With the typical infant doubling birth weight by 5 months and tripling birth weight by 12 months, it does not take long for the effective dose to fall below the therapeutic range. Even systems that allow weight-based dosing seldom offer a view of current medications expressed in terms of milligram/kilogram body weight; that information may be visible during the act of prescribing but not after the fact when it comes time to adjust the dose. Prescribers may need to back-calculate the dose per unit of body weight in order to write an equivalent prescription later in life. Electronic systems should offer the ability to maintain patients on an equivalent dose through changes in body weight, to preserve the clinician's intent over time.

Case Study 3

Clinical Summary

An adolescent girl with type-I diabetes wanted to seek reproductive health care from her primary care pediatrician during her health supervision visit, but decided against it when she realized her parents' ability to see EHR online. This access had been set up when she was 11 years old. Because of this perceived lack of privacy, the patient then sought care at women's health center, which prescribed birth control outside the primary care system. The patient reported taking this medication at the next visit to the primary care clinic, after being assured that the presence of the medication will be hidden from the parent on the patient portal and in printouts. Unfortunately, an automated prescription refill message sent from the dispensing pharmacy triggered a phone call to the patient's home that revealed the presence of the prescription to the parent. The ensuing controversy engendered mistrust of the health care system on the part of both the parents and the adolescent, and they canceled the planned encounter meant to coordinate a transition of care to an adult provider who was intending to take over care of the patient's diabetes.

Analysis

Most adolescents state that they would defer care for contraception if they knew their parents could find out about it [23, 24]. In this case, a source of sensitive information was established at an age when concerns about reproductive health were not important to the patient, and there was no mechanism to update the patient's preference as she entered the reproductive years. Despite the recognition of the importance of adolescents' autonomy in matters involving reproductive health, mental health, substance use, and other sensitive matters, parents are still financially responsible for their minor children, so they will have some access to some information, regardless of even the most detailed technical safeguards. The above scenario was less a failure of the technology and more of a failure of clear, proactive policy regarding how the parent should be involved.

Solutions

- While there are many suggestions for how to configure EHRs for adolescent care [25] there is no substitute for clear adolescent privacy policies within the practice, with documented agreement from both the adolescent and the parent. Data access policies (for the EHR, the patient portal, and any printed products of these) should match the agreement, but no restriction on data sharing will help

the adolescent feel trust in the health care system unless everyone agrees to abide by these policies.
- Any policy or feature designed to hide information (like suppression of printing of contraceptive medications) must have a mode where clinicians involved in treating the patient can see all relevant information.
- Systems used in the care of adolescents must support sufficient interoperability to facilitate smooth transition to care by adult providers.

Miscellaneous Factors Affecting Safety of HIT in Pediatrics

There are other features of care in pediatric settings that affect the safety of HIT. For example, pediatric medications often need to be provided in dosage forms that are different from the usual adult dosage, and IT systems may not be configured to manage medications in these forms. For example, one may need to resort to risky workarounds in order to create a liquid preparation of a medication available only in tablet form. Compounded forms, nonstandard concentrations, and off-label medication use can necessitate similar workarounds. Furthermore, in adult care, a standard dose, often packaged by inpatient pharmacies in "unit doses," suffices for a broad range of body weights. Given the large proportion of care for children that is done in general (as opposed to pediatric) environments, electronic systems that make unit dosing very convenient may inadvertently present risk to smaller patients (adults included). Non-pediatric care environments may not be able to expend the resources necessary to build default pediatric doses into the ordering system or to set up age-specific dosing support. In these cases, electronic systems should, at a minimum, provide some crude age- or weight-based cutoffs for changing the display of the ordering system to make it less likely that a unit dose will be ordered.

Not all pediatric patients live in a typical nuclear family. Systems designed to manage pediatric care should therefore accommodate the recording of complex adult relationships (foster parents, uncertain custody arrangements, the presence of a guardian *ad litem*) in order to ensure that care can proceed in accordance with guardians' wishes and applicable law.

Key Lessons Learned

HIT used in the child health setting must take into account the special nature of pediatric care, with particular attention to the wide variation in body size and the changes in those dimensions over time. Not all EHR systems are designed specifically to be used in child health settings. Child health groups have recognized the special features of pediatric health care that affect HIT and have created a significant body of work detailing these special features [1, 25–29]. While it is impractical to build all of these features into every EHR application (for example, breast milk supply tracking

in a system intended for use in a clinic where those supplies are not handled), designers and implementers should consider the scenarios presented here and in the cited literature while planning for the failure modes that such systems will present.

References

1. Spooner SA. Special requirements of electronic health record systems in pediatrics. Pediatrics. 2007;119(3):631–7.
2. Dart RC, Rumack BH. Intravenous acetaminophen in the United States: iatrogenic dosing errors. Pediatrics. 2012;129(2):349–53.
3. Monagle P, Studdert DM, Newall F. Infant deaths due to heparin overdose: time for a concerted action on prevention. J Paediatr Child Health. 2012;48(5):380–1.
4. Johnson KB, Lehmann CU. Council on Clinical Information Technology of the American Academy of Pediatrics. Electronic prescribing in pediatrics: toward safer and more effective medication management. Pediatrics. 2013;131(4):e1350–6.
5. Villamañán E, Larrubia Y, Ruano M, Vélez M, Armada E, Herrero A, et al. Potential medication errors associated with computer prescriber order entry. Int J Clin Pharm. 2013;35(4):577–83.
6. Kirkendall ES, Spooner SA, Logan JR. Evaluating the accuracy of electronic pediatric drug dosing rules. J Am Med Inform Assoc. 2014;21(e1):e43–9.
7. Stultz JS, Nahata MC. Appropriateness of commercially available and partially customized medication dosing alerts among pediatric patients. J Am Med Inform Assoc. 2014;21(e1):e35–42.
8. Goske MJ. Image gently: child-sizing radiation dose for children. JAMA Pediatr. 2013;167(11):1083.
9. Carpenter JD, Gorman PN. Using medication list-problem list mismatches as markers of potential error. Proc AMIA Symp. 2002:106–10. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2244138/
10. Galanter W, Falck S, Burns M, Laragh M, Lambert BL. Indication-based prescribing prevents wrong-patient medication errors in computerized provider order entry (CPOE). J Am Med Inform Assoc. 2013;20(3):477–81.
11. Ahn EK, Cho SY, Shin D, Jang C, Park RW. Differences of reasons for alert overrides on contraindicated co-prescriptions by admitting department. Healthc Inform Res. 2014;20(4):280–7.
12. Isaac T, Weissman J, Davis R, Massagli M, Cyrulik A, Sands D, et al. Overrides of medication alerts in ambulatory care. Arch Intern Med. 2009;169(3):305–11.
13. Slight SP, Nanji KC, Seger DL, Cho I, Volk LA, Bates DW. Overrides of clinical decision support alerts in primary care clinics. Stud Health Technol Inform. 2013;192:923.
14. National Center for Health Statistics, U.S. Centers for Disease Control. Growth Charts (2010). Accessed 5 Jan 2015.
15. WHO Multicentre Growth Reference Study Group. WHO Child Growth Standards based on length/height, weight and age. Acta Paediatr Suppl. 2006;450:76–85.
16. Lin CP, Payne TH, Nichol WP, Hoey PJ, Anderson CL, Gennari JH. Evaluating clinical decision support systems: monitoring CPOE order check override rates in the Department of Veterans Affairs' computerized patient record system. J Am Med Inform Assoc. 2008;15(5):620–6.
17. Nanji KC, Slight SP, Seger DL, Cho I, Fiskio JM, Redden LM, et al. Overrides of medication-related clinical decision support alerts in outpatients. J Am Med Inform Assoc. 2014;21(3):487–91.
18. Bainbridge L. Ironies of automation. Automatica. 1983;19(6):775–9.
19. Jani YH, Ghaleb MA, Marks SD, Cope J, Barber N, Wong IC. Electronic prescribing reduced prescribing errors in a pediatric renal outpatient clinic. J Pediatr. 2008;152(2):214–8.

20. McPhillips HA, Stille CJ, Smith D, Hecht J, Pearson J, Stull J, et al. Potential medication dosing errors in outpatient pediatrics. J Pediatr. 2005;147(6):761–7.
21. Holdsworth MT, Fichtl RE, Behta M, Raisch DW, Mendez-Rico E, Adams A, et al. Incidence and impact of adverse drug events in pediatric inpatients. Arch Pediatr Adolesc Med. 2003;157(1):60–5.
22. Osorio SN, Abramson E, Pfoh ER, Edwards A, Schottel H, Kaushal R. Risk factors for unexplained medication discrepancies during transitions in care. Fam Med. 2014;46(8):587–96.
23. Britto MT, Tivorsak TL, Slap GB. Adolescents' needs for health care privacy. Pediatrics. 2010;126(6):e1469–76.
24. ACOG Committee Opinion No. 599. Committee on Adolescent Health Care: Adolescent Confidentiality and Electronic Health Records. Obstet Gynecol. 2014;123(5):1148–50.
25. Anoshiravani A, Gaskin GL, Groshek MR, Kuelbs C, Longhurst CA. Special requirements for electronic medical records in adolescent medicine. J Adolesc Health. 2012;51(5):409–14.
26. Gerstle RS, Lehmann CU. Electronic prescribing systems in pediatrics: the rationale and functionality requirements. Pediatrics. 2007;119(6):e1413–22.
27. Kim G, Lehmann C. Pediatric aspects of inpatient health information technology systems. Pediatrics. 2008;122(6):e1287–96.
28. Lowry SZ, Quinn MT, Ramaiah M, Brick D, Patterson ES, Zhang J, et al. A human factors guide to enhance EHR usability of critical user interactions when supporting pediatric patient care. National Institute of Standards and Technology (U.S. Department of Commerce); 2012. p. 44.
29. Agency for Healthcare Research and Quality. Children's electronic health record format. 2013. http://healthit.ahrq.gov/health-it-tools-and-resources/childrens-electronic-health-record-ehr--format. Accessed 5 Jan 2015.

Chapter 15
Safety Considerations in Ambulatory Care Informatics

Eric Rose

Introduction

Studies on risks to patient safety in ambulatory health care have identified numerous potential types of hazardous events, including diagnostic error [1], lapses in care coordination [2], failure to perform or correctly interpret the results of diagnostic tests [3, 4], and prescribing errors [5]. However, patient safety in ambulatory care settings remains inadequately understood. One recent review of ambulatory patient safety research concluded that "We still know very little about patient safety in the ambulatory setting, and next to nothing about how to improve it" [6].

Ambulatory care is set apart from other care settings, such as acute and long-term care, by a number of characteristics. These characteristics can reasonably be expected to affect the types of safety hazards likely to occur in ambulatory care and how such hazards may be effectively mitigated. They include:

- *Lower acuity of illness*—While ambulatory patients may be medically complex, and may occasionally be severely ill, in general, they are substantially less sick than hospitalized patients.
- *Temporal discontinuity of care processes*—The defining characteristic of ambulatory care is that the patient is cared for during brief visits, and otherwise remains in his or her usual place of residence. Most ambulatory care is provided over an extended period of time, often years or decades in primary care (though often only a small number of visits over a few weeks or months in specialty care), with the time spent in care interactions occupying a tiny percentage of the time over which the care is provided. This means that a great deal must often be

E. Rose, M.D., F.A.A.F.P. (✉)
Departments of Family Medicine and Biomedical Informatics and Medical Education, University of Washington, Seattle, WA, USA
e-mail: emrdoc@hotmail.com

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_15

achieved within a very brief patient encounter, and it also creates the important challenge of managing patient care during the relatively long gaps between patient encounters.

- *Higher degree of cross-organizational collaboration*—In acute care, with rare exceptions, all care is provided within the physical confines of a single care delivery organization, which sets policies and processes and manages the technology infrastructure. In contrast, in ambulatory care, patients frequently receive care from practitioners who are completely organizationally independent from each other, necessitating cross-organizational coordination to ensure safe care.
- *Higher dependence on patient engagement and adherence*—While patients may decline recommended treatments or services in an acute care environment, in ambulatory settings adherence to such recommendations is much more within the patient's control. Since such adherence may have a dramatic impact on outcomes of care, this amplifies the importance of patient engagement and adherence in ambulatory settings.
- *Greater involvement of non-professionals in patient care*—For vulnerable individuals, including frail elderly and people with special needs, non-professional caregivers such as family and friends play a critical role in health care processes, including administering medications, monitoring the status of a chronic condition, participation in rehabilitation regimens, use of medical devices at home, and transportation to and from health care providers. These caregivers are important links in the chain of patient safety (and risk) for many ambulatory patients.
- *Lower levels of professional training for health care personnel*—Even small US hospitals generally have personnel capable of performing sophisticated clinical assessments and providing appropriate interventions, including nurses, respiratory therapists, physical therapists, and social workers. In contrast, while some ambulatory practices employ nursing and allied health personnel, many more rely on professionals with a lower level of training, sufficient for a subset of tasks that occur at a high frequency within the practice. This may create hazards if such personnel are called upon to perform tasks outside their expertise (e.g., patient triage and interpretation of diagnostic tests), or if providers are required to interweave such tasks among the work of patient visits.

The last decade has seen a dramatic increase in the use of electronic health record systems (EHRs) and other health information technology (HIT) in ambulatory care. Despite the evidence of beneficial impact of some aspects of such technology in clinical processes [7], there is growing attention to the potential of such technology to also pose risks to patient safety. Among the body of published original research regarding HIT hazards, itself a nascent area of study, studies dealing specifically with ambulatory care environments are sparse. Many of the most detailed studies either involved only acute care safety-related events or did not distinguish between ambulatory and acute care events [8–11]. However, studies of EHRs in ambulatory environments have suggested that they have a significant impact on the distribution

of clinician time among various types of work [12], that clinicians perceive them to have problematic effects on clinical workflow [13], and that features designed to enhance patient safety often do not perform as desired [14].

Case 1: Temporal Ambiguity Leading to Inaccurate Plans for Preventive Care

Clinical Summary

A 64-year-old man presents for a routine preventive exam at the 4-physician private primary care practice where he has received care for the last 12 years. The practice has used an EHR system during that entire time. He is seen by a physician who uses a documentation template which the practice's medical director created for routine preventive care, by modifying a "stock" template delivered with the EHR system by its vendor. The template is accessed by the user within the EHR's note creation screen, which resembles a word processing user interface. When the template is selected, certain segments of text are added to the note creation screen, some of which are a fixed part of the template specification itself, and some of which represent data specific to the current patient, retrieved from the database at the time of template selection. The user then adds additional text representing information from the patient encounter, to complete the note. Among the data "pulled into" the note by the template are the patient's current medications, allergies, vital signs from the current visit, recent laboratory results, and the patient's "Past Medical History" (PMH). This particular EHR system maintains PMH as free text that is entered and stored separately from the record of any specific patient encounter. There is a "Past Medical History" screen from which users can enter, view, and edit the PMH.

In the physician's practice, it is common for providers to populate the PMH at a patient's initial visit, and to update it if there is some noteworthy change in their health status that merits mention as part of the PMH. This patient's PMH included the statement "Screening colonoscopy: 1 year ago, results normal." This had been documented in the EHR at the patient's first visit, over 10 years prior to the current visit, and the text of the PMH had not been updated since. The physician performing the routine preventive exam, when reviewing the on-screen information after selecting the documentation template, viewed this information in the PMH (which was inserted into the note without any indication that it had been recorded many years earlier) and concluded that the colonoscopy had been performed the year prior to the visit. When discussing screening recommendations with the patient, the physician told the patient that based on the information in his record, he would not be due for routine screening for colorectal cancer for some years. The patient, having unpleasant memories of the procedure, was relieved and voiced his ready assent. It

was only in the ensuing conversation regarding the patient's experience with the procedure that it became apparent to the physician that the colonoscopy had been done more than 10 years earlier, and that colorectal cancer screening was indeed indicated for this patient.

Case Analysis

This case illustrates the critical importance of the time course of events in managing patient care, and the potential for ambiguity and misunderstanding when temporal information is reused in a context different from that in which it was recorded.

The myriad ways that data can be entered and then viewed in an EHR system are not often apparent to its users, particularly those who use the system infrequently or have been using it only for a short time. Describing the timing of an event in relative terms (e.g., "10 years ago," "next week") is common for patients when relaying history, and often duplicated by clinicians who are documenting that history. This is generally a low-risk approach if such documentation will only be used as part of the record of a single visit, where the temporal context will never be in question. However, if the documentation is intended to serve as a non-encounter-specific record to be reused over time, then such relativistic temporal references quickly become inaccurate. If the EHR system stores the date when the documentation was recorded and makes that visible to end-users when the documentation is viewed or used in other contexts (like being inserted into a visit note as part of a documentation template), then users have the opportunity to consider that date "stamp" and infer the meaning of the documentation in that context, but such a date stamp may not be shown by the EHR system (it was not in the case described above) or even if shown, may be overlooked by end-users.

Sittig and Singh have established an eight-dimensional "socio-technical model" for studying HIT [15]. Examining this case within this framework can help elucidate the contribution of multiple factors to this potentially hazardous event. Although not all eight of Sittig and Singh's "dimensions" of HIT can reasonably be deemed applicable, the following do seem to be at play:

- *Human–computer interface (HCI)*—The HCI issues here might at first glance seem noncontributory to the event described in the case. In contrast to many EHR systems, the note creation screen of this particular EHR system is quite simple and straightforward, resembling the user interface of a word processing application and providing to the end-user, as he or she composes a note, a display of exactly how the note will appear in the patient's record once finalized. However, the simple fact of the date stamp not being displayed along with the PMH text could be considered a contributory factor to the potentially hazardous misinterpretation of the PMH content.
- *Internal organization policies, procedures, and culture*—The practice, like many, invested significant effort in configuring their EHR system at the time it

was first adopted. However, over time, they neither maintained that level of effort, nor extensively analyzed various information flows through the system and their effects. Moreover, while the practice had policies to ensure accuracy of the patient record (e.g., ensuring that the PMH was completed for each patient), over time, the practice's physicians developed slightly different habits in using the system, including one physician's tendency to make use of the relative temporal statements mentioned above in areas of the record like the PMH. Because the physicians tended to see patients primarily from their own panels, these differences in EHR system usage were not always evident, nor were there any processes in place to proactively analyze and address them.

- *People*—In this case, a highly trained, diligent practitioner came close to making a preventable error with potentially serious consequences for a patient's health. While the contributions of the aforementioned HIT dimensions must not be minimized, it is important to acknowledge the role of the two users in this case: The physician who originally documented "Screening colonoscopy: 1 year ago, results normal" in the patient's record, and the physician who, seeing that documentation many years later, took it to be referring to the present time. If both of them had a better understanding of how their practice's EHR system might reuse and re-present this data in contexts other than those of its original entry, the former might have thought instead to document: "Screening colonoscopy: 2002, results normal," and the latter might have thought to consider whether textual data "pulled into" the note might have a temporal point of reference in the remote past.
- *Clinical content*—The case could not have occurred without two clinical content artifacts: the PMH, which described an event's temporality in relative terms, and a documentation template, which inserted the PMH into a note without any indication that the text which comprised it might have been entered years earlier.
- *Workflow and communication*—At the crux of this case is a piece of information recorded by one health care professional and subsequently viewed and used for decision-making by another. While this is the very essence of "workflow," the practice had not intentionally conceived and planned out the workflow implemented in the above case. It was, in effect, a "stealth" workflow uncovered by capabilities of the software which had likely never been considered by anyone using the software at the practice.

Proposed Solutions

As in the section above, Sittig and Singh's eight-dimensional socio-technical model provide a useful framework for considering solutions to this HIT hazard:

- *Human–computer interface (HCI)*—A simple HCI change to the EHR system used in this case—displaying a date stamp indicating the original date of entry or last-updated date, along with the PMH text—could have helped contextualize the PMH contents and avoid the error that occurred in this case. This might even be

worth consideration as an industry safety standard for free-text data that is added to an encounter note through a documentation template in an EHR. At the same time, if the PMH text could be updated at various points in time (as is the case in many EHR systems), there could be relative-time statements in the PMH whose meaning could be misinterpreted even with the availability of a displayed time stamp.

- *Internal organization policies, procedures, and culture*—Alongside changes in application functionality, changes in organizational behavior around HIT could help avoid a recurrence of the type of event described in this case. By establishing clear guidelines about how data is to be recorded in the EHR, and providing sufficient orientation to the providers, practices can reduce the risk that critical information will be inaccessible, overlooked, or misinterpreted. In this case, providers could have been educated about the way data flows between sections in the EHR and conventions for expressing temporal data in unstructured notes in absolute, not relative, terms, and to always consider the date of data entry when interpreting statements involving relative time intervals. Moreover, if the EHR offered the ability to record events (like colonoscopies) as structured data with a discrete field to represent the date of the event, as this practice's EHR in fact does, the practice could have established a convention to utilize that capability for recording such data, rather than the free text PMH section. While the process of establishing and disseminating these guidelines of EHR use might be burdensome, particularly within a small practice, it does not need to be particularly elaborate or time-consuming. It could be made easier if some of these issues were covered in a basic informatics curriculum as part of health care provider training.
- *People*—Common wisdom eschews putting the onus purely on individuals to simply be more careful, focusing rather on systemic factors that make error more likely. This is reasonable, since the cognitive and attentional capacities of humans are finite and it is likely that the vast majority of clinicians try their utmost to avoid mistakes. At the same time, had either provider in this case been more familiar with the information flows in their EHR, and acted accordingly, the error could have been avoided without necessarily requiring greater cognitive or attentional resources during the patient encounter. If HIT is to support rich functionality involving complex data, it behooves those who use it to become familiar enough with it to use it safely.
- *Clinical content*—In most EHRs that allow customized documentation templates, the end-user who creates a template may include any text they wish. It has become common to add advisory text to some templates, intended to provide advice or cautions to clinicians who uses the template when documenting patient encounters. The clinician generally deletes this text before finalizing the note (so that it does not become part of the patient record). In this case, had the template included advisory text preceding the PMH such as "Note-The following text was added to the patient record in the past," this could have helped contextualize the PMH text including the reference to the past colonoscopy.

- *Workflow and communication*—In the case analysis, it was pointed out that the case centered around a workflow whereby a piece of information recorded by one health care professional was subsequently viewed by another and used for decision-making. This workflow provides significant benefit, by allowing a provider to leverage highly relevant information collected in previous patient encounters. Rather than dismantle this workflow, e.g., by redesigning the template to not include the previously recorded PMH, it would seem more appropriate to retain the workflow but, through the approaches described above, ensure that it is presented, and users are prepared to interpret it, with the correct context.

Case 2: Terminology Idiosyncrasies Leading to Population Management Failure

Clinical Summary

A mid-sized multispecialty practice decides to initiate a disease-management effort for its patients with diabetes mellitus. The practice has, for several years, utilized the EHR's capability to record problems using SNOMED-CT (SCT), an extensive and detailed terminology designed for capture and processing of clinical data [16]. The Medical Director of Quality, who is leading the disease-management effort, has taken an introductory course on clinical informatics. In that course, she learned of SCT's hierarchical structure and the technique of testing whether an SCT code falls into a particular branch of the SCT hierarchy ("subsumption testing"). She decides to utilize this approach as a means to identify patients who have been noted to have diabetes mellitus. She directs her database analyst to generate reports that identify patients who have a problem list entry with an SCT code of 73211009 ("diabetes mellitus") or any of its 109 SCT descendants, along with information about their disease status or potential gaps in care. These reports are used by a team of "patient coaches" who work collaboratively with the patients' primary care providers to engage and educate patients and help coordinate their care.

Ten months after the initiation of the program, the Medical Director of Quality has an office visit with one of her more complex diabetic patients. This patient, whose diabetes has been difficult to control and fraught with complications, has had inconsistent adherence to and engagement with his care, and rarely comes in to be seen. He is the exact type of patient she had in mind when she designed the disease management program. She asks what he thinks of his patient coach, and is surprised to hear that he has not been contacted. She confirms that his problem list contains references to his diabetes, including entries with the following SCT codes:

- Type II diabetes mellitus uncontrolled (SCT 443694000)
- Proliferative diabetic retinopathy (SCT 59276001)

- Macroalbuminuric diabetic nephropathy (SCT 445170001)
- Neuropathic diabetic ulcer—foot (SCT 201251005)
- Necrobiosis lipoidica diabeticorum (SCT 56391002)

The next day, she confirms that this patient does not appear on any of the SCT-based reports created for the disease management program. She contacts her database analyst and asks him to check into why this is the case. The database analyst confirms that the 5 SCT codes above are not in the "diabetes mellitus" (SCT 73211009) hierarchy.

Case Analysis

SCT is a well-established clinical ontology maintained by a nonprofit, international standards development organization. It is widely used in many countries around the world, and is among the health care standards required for certified EHR technology in the USA [17]. SCT includes coded concepts with textual descriptions, and specifies hierarchical relationships, known as "Is a" maps, that link concepts to their conceptual parents. For instance, "type 2 diabetes mellitus" (SCT 44054006) has an "Is a" link to "diabetes mellitus" (SCT 73211009), and "insulin treated type 2 diabetes mellitus" (SCT 237599002), in turn, has an "Is a" link to "type 2 diabetes mellitus"(Fig. 15.1). The conceptual "ancestors" (the targets of an "Is a" relationship or a chain of "Is a" relationships) are said to "subsume" their narrower conceptual "descendants." By testing SCT codes for subsumption, automated processes such as database queries can identify codes that are a particular branch of the SCT hierarchy and thus, patients who have a particular category of disease (provided the patients' problems are coded in SCT).

In defining relationships among concepts, SCT takes a formalistic approach that may not be anticipated by health care professionals attempting to utilize it for clinical purposes like population management. The case above illustrates one example of this: in addition to over 100 SCT codes subsumed under "diabetes mellitus" (SCT 73211009), SCT provides a set of over 200 codes subsumed under a different SCT code, "diabetic complication" (SCT 74627003) (Fig. 15.2). Although SCT allows for a single code to have "Is a" relationships to more than one parent, the codes in the "diabetic complication" hierarchy do not have "Is a" links to codes in the "diabetes mellitus" hierarchy. From the perspective of a formal ontology, this is actually appropriate, since, for example, "diabetic retinopathy" is not, strictly speaking, a type of "diabetes mellitus." The SCT codes in the "diabetic complication" hierarchy do, in fact, have links in SCT to "diabetes mellitus," but those links are tagged with the relationship type "associated with" rather than "Is a." In any event, any attempt to use subsumption testing to SCT 73211009 to identify diabetic patients will fail to identify diabetics whose diabetic problems are coded only with SCT codes in the "diabetic complication" hierarchy.

SCT is also a living terminology that has evolved over decades and is continually updated, and as such, has imperfections. In the case described above, four of the five

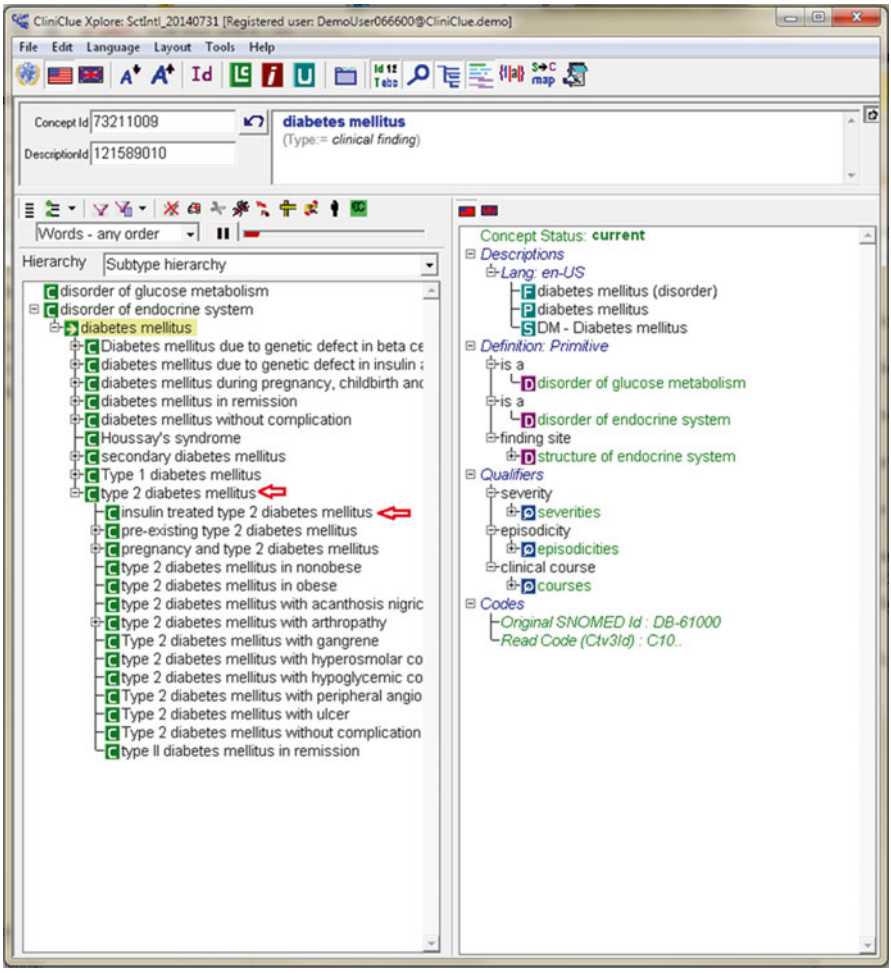


Fig. 15.1 SNOMED CT diabetes mellitus subhierarchy (partial)

SCT codes on the patient's record represented complications of diabetes, and as such, would, by SCT's own conventions, not be properly subsumed under "diabetes mellitus." In contrast, the first, "Type II diabetes mellitus uncontrolled" (SCT 443694000), does semantically belong in the "diabetes mellitus" hierarchy," as it describes a particular type of diabetes mellitus. However, SCT does not include this code in the "diabetes mellitus" hierarchy. Instead, it is a child of the SCT code "diabetic—poor control" (SCT 268519009) which falls into the SCT "evaluation finding" hierarchy, separate from the "diabetes mellitus" hierarchy (Fig. 15.3). While there may be a justification of this within the context of SCT formalisms, it is unlikely that even fairly sophisticated users of SCT would be able to anticipate

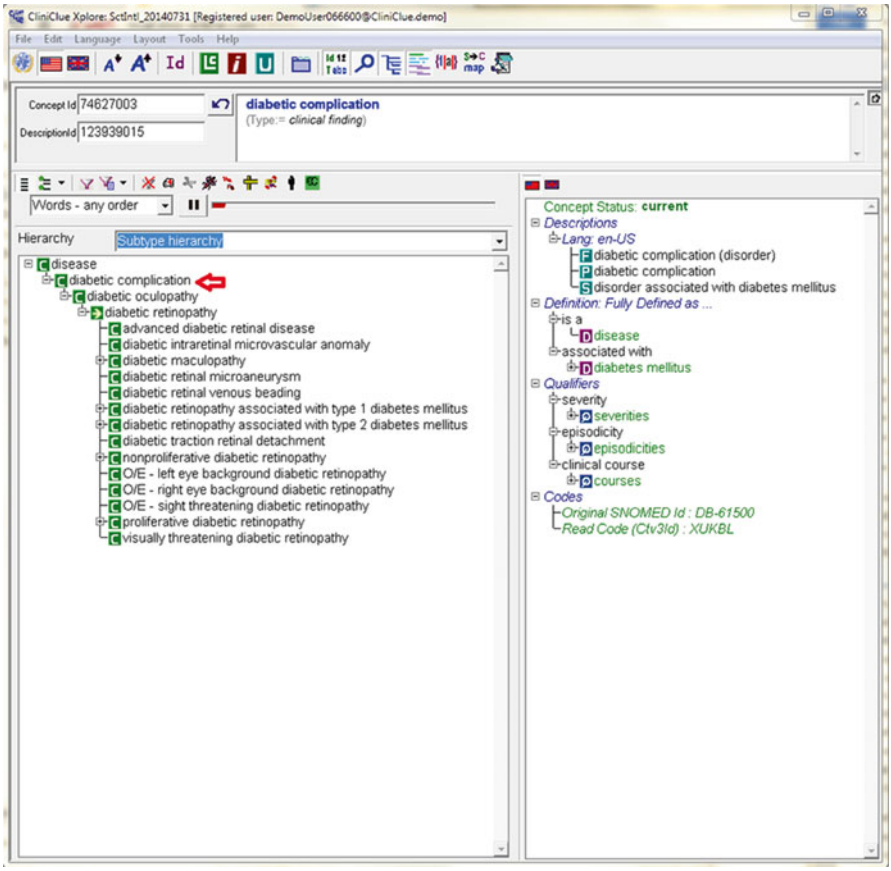


Fig. 15.2 SNOMED CT diabetic complication subhierarchy (partial)

that a patient with a documented problem associated with this SCT code would not be included in a SCT-based subsumption test for diabetes mellitus.

As with the prior case, Sittig and Singh's model helps to frame the factors behind the potentially hazardous situation of a high-risk patient being inappropriately excluded from a disease management program:

- *Hardware and software computing infrastructure*—In this case, the hardware and software functioned precisely as designed. Point-of-care systems allowed capture of patient problems with correct SCT codes, and the systems and queries used to generate reports on the practice's diabetic population correctly identified those with SCT codes that fell into the "diabetes mellitus" SCT hierarchy. In fact, one might be tempted to lay all the blame at the feet of the terminology itself and the unfamiliarity of the disease management team with its particular nuances. At the same time, it should be noted that had the organization had access to a list of

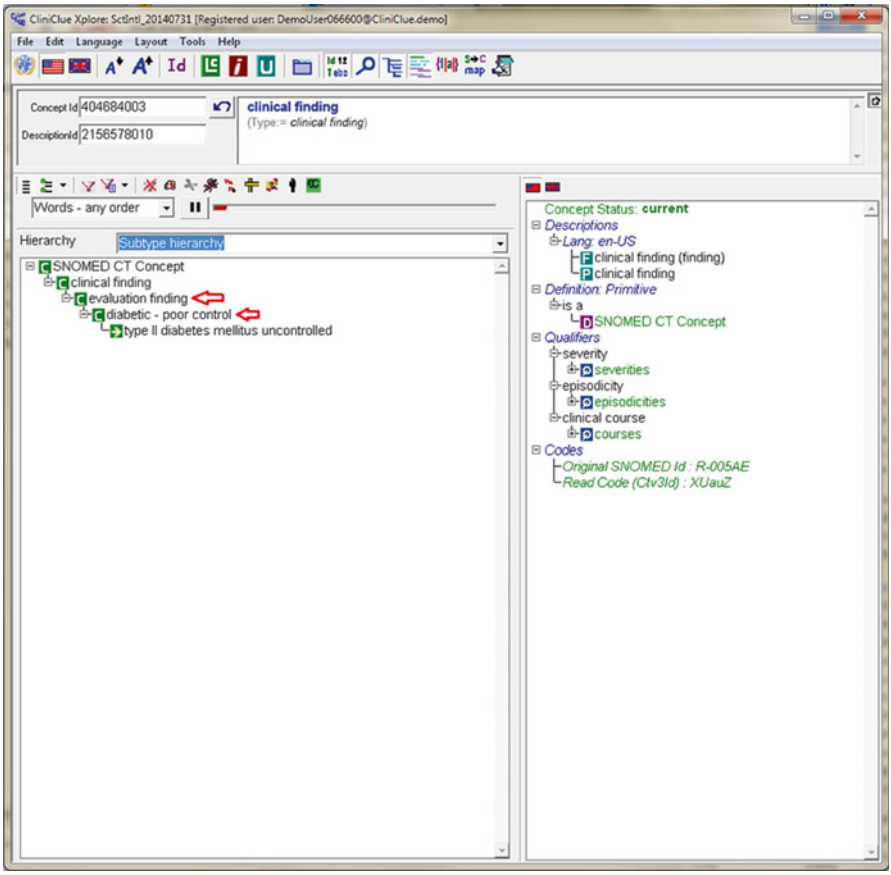


Fig. 15.3 SNOMED CT subhierarchy showing concept "type II diabetes mellitus uncontrolled" outside of diabetes mellitus hierarchies

SCT codes that imply that a patient has diabetes mellitus (regardless of place within the SCT hierarchy), the outcome could have been averted.

- *Clinical content*—The clinical content on patient records (i.e., the SCT codes associated with problem list entries) is at the root of this case. Because these codes did not fall within the SCT "diabetes mellitus" hierarchy for the patient in question, he was excluded from an important clinical intervention. However, it would seem unreasonable to expect that an organization to attempt to refrain from using such codes, given that they represent important information about patient status (like the presence of severe diabetic retinopathy), which in fact the organization might be using to drive other important data-dependent processes like disease management or automated clinical decision support.

- *People*—The individuals involved in this case should not be regarded as primary contributors to the outcome in question. The Medical Director of Quality acted based on what would seem to be reasonable assumptions about SCT, and the database analyst simply created reports to the specifications he was given. At the same time, deeper training in SCT, or simply having had experiences like the one illustrated in the case, might have led the Medical Director of Quality to take a closer look at SCT to ensure that all the hierarchies implying the presence of diabetes mellitus were covered in the reports she was using for the disease management effort.
- *Internal organization policies, procedures, and culture*—The organization in which this case occurred was a mid-sized practice with an entrepreneurial culture that allowed for energetic individuals to undertake innovative projects such as the disease management project discussed above, and without a large staff of highly trained informatics professionals that a larger organization might have. As the adoption of HIT and the use of structured vocabularies like SCT increase, more and more projects like this will be undertaken to leverage this coded data. While many successes can be anticipated, this case illustrates that missteps may also occur, particularly in small to mid-sized organizations with limited access to informatics expertise.
- *System measurement and monitoring*—The organization launched a disease management project based on a set of database queries that was intended to identify the organization's diabetic patients. However, no attempt was made at the outset to validate that all members of the diabetic population were captured in the queries used. Had such validation been attempted, the flaw in the queries might have been identified much earlier.

Proposed Solutions

As with the prior case, proposed solutions can be categorized according to Sittig and Singh's socio-technical model:

- *Hardware and software computing infrastructure*—As noted above, there are no frank hardware or software defects whose repair would have avoided the events described in this case. However, one potential solution would be a curated list of all SCT codes that indicate that a patient has diabetes mellitus. Such lists are commonly referred to as "value sets" and have come into common usage as components of clinical quality measure specifications. Value sets must be very carefully constructed in order to be complete and accurate, and may rapidly become out of date as the underlying terminology is updated, unless they are diligently maintained. Nonetheless, curated value sets are likely to become increasingly important as more organizations need to make secondary use of coded clinical data without the benefit of expert informaticists.

- *Clinical content*—While clinical content is central to this case, the clinical content itself was valid. It does not seem reasonable to try to address the problem by requiring clinicians to, for instance, ensure that patients have a "diabetes" SNOMED code in addition to any "diabetes complication" SNOMED codes on their problem lists. That approach would in effect make the clinician responsible for addressing the limitations of the terminology and information technology infrastructure. Such non-user-centric approaches have rarely had success in health care environments.
- *People*—This case illustrates the need for highly experienced and trained clinical informatics professionals in health care delivery organizations. The need to make use of health care data for secondary purposes will only increase over time, and a skilled informatics workforce is needed to accomplish this work. The growth of formal clinical informatics training programs and the recent emergence of clinical informatics as an accredited medical specialty may help address these needs [18].
- *Internal organization policies, procedures, and culture*—In this case, an important clinical project did not completely fulfill its mission because of an informatics-based error. In order for health care delivery organizations to successfully increase the scale of such undertakings, they will need to adopt governance policies that reduce the risk of such errors while avoiding excessive bureaucracy that stifles ground-up innovation from those closest to the realities of patient care. While there are no recognized "best practices" in such governance approaches, discussions of this topic with proposed approaches have been published [19].
- *System measurement and monitoring*—This case illustrates the importance of validating any automated process before using it as the basis of a major undertaking involving large numbers of people. Such validation would not need to be comprehensive; simple spot-checking can often identify major gaps in identifying a patient cohort. In this case, approaches that could have been undertaken include automated searches of problem list descriptions (rather than codes), or medication or laboratory records, manual or automated scanning of appointment schedule records or paper records, or even recollection by providers and staff of frequently seen diabetic patients.

Conclusion

The cases discussed in this chapter are based on real events, though minor details have been modified for purposes of brevity and clarity. On the surface, the cases seem quite distinct. The first case involved information viewed by a clinician in the EHR during a patient visit and the second involved the results of an automated database query. Nonetheless, a common theme connects them. In both cases, there was no outright

"bug" in the sense of software behaving inconsistently with its design. Rather, there was a gap between the design of the software (and in the second case, an associated data artifact, the SNOMED ontology) and the understanding or assumptions of the humans interacting with it. Ultimately, this reflects a gap between the mindset of the humans designing technology and the humans using it.

It is possible to close such gaps either on the design side, by modifying the technology made available to health care delivery organizations, or on the implementation side, by changing how the technology is configured or how users operate it. The manner in which HIT is configured and used can have a dramatic impact on its potential to improve (or worsen) patient outcomes, as illustrated in several examples in the published literature. In one study, performed in a local Veterans Administration health system, the incidence of lack of timely follow up for positive fecal occult blood test (FOBT) results dropped from 29.9 to 5.4 % with resolution of a configuration issue that was preventing FOBT results from being transmitted to primary care providers [20]. Correspondingly, many producers of HIT maintain contact with those who use their products and introduce design modifications over time based on user feedback. Application of traditional technology usability evaluation approaches has been shown to be capable of identifying usability issues in HIT, though the impact on patient safety of redesign based on such evaluation remains to be demonstrated [21].

Clinician training in HIT is a matter of some controversy. While there is evidence that many clinicians who use EHRs do not feel they are adequately trained [22], some might consider the very need for training to be *prima facie* evidence of inadequate system design and implementation. The cases presented in this chapter do illustrate the potential for training to mitigate HIT-related hazards. In the first case, had the end-user been more familiar with the EHR (or with EHRs in general), he might not have taken the text displayed to him at face value. In the second case, if the physician coordinating the disease management program had a deeper understanding of SCT, she would likely have designed her database query in a way that captured her practice's diabetic patients more thoroughly. If the hazards of HIT are to be minimized, it would seem reasonable to expect all clinicians to be armed with basic informatics knowledge and for clinicians with significant responsibility for managing the use of HIT to have specialized informatics training.

When radically new ways of managing information are introduced into a complex environment where mistakes can have very serious consequences, it is to be expected that both beneficial and deleterious effects may result. The interactions between patient, clinician, and information technology during even a 1–1 office encounter are highly complex and nuanced, and factors as subtle as the physical placement of display screens in the exam room may have an impact on these interactions and, indirectly, on patient safety [23]. However, despite the magnitude of the potential risk from introduction of HIT into ambulatory care, published data on the associated hazards is extremely limited. The cases discussed in this chapter, while useful in their ability to illustrate some of the factors at play with ambulatory HIT use, are anecdotal and not a substitute for systematically

collected and rigorously analyzed data. It is hoped that future research will elucidate how to gain the greatest benefit from HIT in ambulatory care with the least risk to patient safety.

References

1. Gandhi TK, Lee TH. Patient safety beyond the hospital. NEJM. 2010;363:1001–3.
2. Singh H, Esquivel A, Sittig DF, Murphy D, Kadiyala H, Schiesser R, Espadas D, Petersen LA. Follow-up actions on electronic referral communication in a multispecialty outpatient setting. J Gen Intern Med. 2011;26:64–9.
3. Giardina TD, King BJ, Ignaczak AP, Paull DE, Hoeksema L, Mills PD, Neily J, Hemphill RR, Singh H. Root cause analysis reports help identify common factors in delayed diagnosis and treatment of outpatients. Health Aff. 2013;32(8):1368–75.
4. Singh H, Thomas EJ, Mani S, Sittig D, Arora H, Espadas D, Khan MM, Petersen LA. Timely follow-up of abnormal diagnostic imaging test results in an outpatient setting: are electronic medical records achieving their potential? Arch Intern Med. 2009;169:1578–86.
5. Singh H, Mani S, Espadas D, Petersen N, Franklin V, Petersen LA. Prescription errors and outcomes related to inconsistent information transmitted through computerized order entry: a prospective study. Arch Intern Med. 2009;169:982–9.
6. Lorincz CY, Drazen E, Sokol PE, Neerukonda KV, Metzger J, Toepp MC, Maul L, Classen DC, Wynia MK. Research in ambulatory patient safety 2000–2010: a 10-year review. Chicago, IL: American Medical Association; 2011.
7. Karsh B. Clinical practice improvement and redesign: how change in workflow can be supported by clinical decision support. AHRQ Publication No. 09-0054-EF, 2009. http://www.nachc.com/client/Clinical%20Practice%20Improvement%20and%20Redesign_How%20Workflow%20can%20Support%20CDS.pdf. Accessed 28 June 2014.
8. Myers RB, Jones SL, Sittig DF. Review of reported clinical information system adverse events in US Food and Drug Administration databases. Appl Clin Inform. 2011;2:63–74.
9. Magrabi F, Mei-Sing O, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. J Am Med Inform Assoc. 2012;19:45–53.
10. Warm D, Edwards P. Classifying health information technology patient safety related incidents — an approach used in Wales. Appl Clin Inform. 2012;3:248–57.
11. Harrington L, Kennerly D, Johnson C. Safety issues related to the electronic medical record (EMR): synthesis of the literature from the last decade, 2000–2009. J Healthc Manag. 2011;56:31–43.
12. Pizziferri L, Kittler AF, Volk LA, Shulman LN, Kessler J, Carlson G, Michaelidis T, Bates DW. Impact of an electronic health record on oncologists' clinic time. AMIA Annu Symp Proc. 2005;2005:1083.
13. NIST 2014. Integrating electronic health records into clinical workflow: an application of human factors modeling methods to ambulatory care. http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7988.pdf, Accessed 28 June 2014.
14. Can der Sijs H, Aarts J, Vulto A, Berg M. Overriding of drug safety alerts in computerized physician order entry. J Am Med Infom Assoc. 2006;113(2):138–47.
15. Sittig DF, Singh H. A new socio-technical model for studying health information technology in complex adaptive healthcare systems. Qual Saf Health Care. 2010;19 Suppl 3:i68–74.
16. International Health Terminology Standards Development Organization. SNOMED CT. http://ihtsdo.org/snomed-ct/, Accessed 9 Nov 2014.
17. 2014 Edition Release 2 Electronic Health Record (EHR) Certification Criteria and the ONC HIT Certification Program; Regulatory Flexibilities, Improvements, and Enhanced Health Information Exchange; Final Rule. Federal Register 79 (11 Sept 2014): 54330–54480.

18. AMIA. History of the clinical informatics subspecialty. http://www.amia.org/clinical-informatics-board-review-course/history. Accessed 9 Nov 2014.
19. Wright A, Sittig DF, Ash JS, Bates DW, Feblowitz J, Fraser G, Maviglia SM, McMullen C, Nichol WP, Pang JE, Starmer J, Middleton B. Governance for clinical decision support: case studies and recommended practices from leading institutions. J Am Med Inform Assoc. 2011;18(2):187–94.
20. Singh H, Wilson L, Peterson LA, Sawhney MK, Reis B, Espadas D, Sittig DF. Improving follow-up of abnormal cancer screens using electronic health records: trust but verify test result communication. BMC Med Inform Decis Mak. 2009;9:49.
21. Kushniruk AW, Triola MM, Borycki EM, Stein B, Kannry JL. Technology induced error and usability: the relationship between usability problems and prescription errors when using a handheld application. Int J Med Inform. 2005;74(7–8):519–26.
22. Singh H, Spitzmueller C, Petersen NJ, Sawhney MK, Smith MW, Murphy DR, Espadas D, Laxmisan A, Sittig DF. Primary care practitioners' views on test result management in EHR-enabled health systems a national survey. J Am Med Inform Assoc. 2012;20(4):727–35. doi:10.1136/amiajnl-2012-001267.
23. Frankel RM, Saleem JJ. "Attention on the flight deck": What ambulatory care providers can learn from pilots about complex coordinated actions. Patient Educ Couns. 2013;93:367–72.

Part IV
Organizational Considerations

Chapter 16
HIT and Medical Liability Risks

Sandeep S. Mangalmurti

Introduction

As the use of electronic health records (EHRs) becomes more widespread, we will all be forced to confront more complex legal issues involving privacy, confidentiality, and ownership of electronic records. One less discussed implication is the potential impact on the medical liability landscape [1–3]. As a key point of contact between the physician and patient, it is clear that as EHRs evolve, so will the manner in which physicians approach potential malpractice lawsuits. These changes will likely ripple through the multiple functionalities of EHRs, from basic functions such as transmission of clinical information to more advanced features such as computerized provider order entry and electronic messaging [4].

One initial issue will be the increased volume of data that will now be easily accessible by providers. Intuitively, increased information is a net positive, allowing providers to make medical decisions with more available facts. However, the liability implications are unclear. One key aspect of effective medical care is the ability to focus on important pieces of information in a sea of data. EHRs make that sea much larger, and can make it easier to miss those key pieces, particularly as clinical volumes continue to increase. Unfortunately, the liability standard is likely to be unforgiving. Quite the contrary, the presence of accessible information may create an obligation to actually access it. Practitioners may be trapped between a more stringent liability standard on one hand, and a more demanding clinical environment on the other [5].

Another possible sources of liability exposure are errors in the use of EHRs. Some of these possible errors are straightforward and predictable. Incomplete or incorrect transmission of information will clearly carry significant liability implications [6]. Irresponsible copying and pasting may result in documentation

S.S. Mangalmurti, M.D., J.D. (✉)
Section of Cardiology, Bassett Heart Care Institute, 1 Atwell Road,
Cooperstown, NY 13326, USA
e-mail: sandeep.mangalmurti@bassett.org

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_16

errors that would be viewed poorly by judges and juries [7, 8]. Increased use of electronic messages between patients and providers will create increasing obligations for physicians to be regularly connected and respond promptly [9].

Use of more sophisticated systems with advanced clinical decision support features may have even greater medical liability implications. These systems have built in clinical recommendations to help guide a provider as she/he interfaces with an EHR. The recommendations might be as simple as warnings that the patient has evinced an allergy to a particular class of medications; any attempt to order medications from that class will result in warnings. More sophisticated systems may make medical recommendations based upon provider orders, including identifying an increased risk of bleeding or renal/hepatic failure from certain combinations of medications. Even more advanced systems may, after identification of a potential diagnosis, produce sets of orders from which the provider can choose.

The liability implications of these clinical decision support systems are yet to be determined. There are at least two potential malpractice pitfalls. First, the decision support system must be medically accurate. Obviously, this is less of a problem when the issue is a simple one, such as identification of patient allergies. In more complicated systems that are making actual medical recommendations, it is imperative that these systems remain up-to-date with the most recent guidelines and medical standard of care. Physicians should be involved in shaping the content of these systems, and, equally importantly, continue to be regularly consulted to keep them current. Failure to do so will clearly expose providers to liability risk when they attempt to follow any recommendations that these decision support systems might offer.

The second liability pitfall will develop when providers choose to ignore the recommendations of a clinical decision system. Clearly, mere compliance with EHR recommendations will not serve as inherent protection in a malpractice lawsuit. The question will be always be whether the provider met the "standard of care," which is an objective standard that is independent of any electronic systems that attempt to duplicate it. Providers should and will overrule EHR recommendations when necessary. However, it is not yet clear how this action will be viewed by juries. A poorly designed (or poorly updated) clinical decision support system might force a provider to frequently overrule incorrect recommendations. Despite the ultimate merit of the physician's decision, the appearance of impropriety may create liability problems [5].

A less commonly known, but of even greater potential liability impact, is likely to be the increasing impact of metadata in malpractice lawsuits [10]. Metadata is the electronic footprint that records the details of every provider interaction with an EHR. Metadata will reveal when a record was accessed, how long it was examined, and when and what was documented. It can reveal that a provider looked at a plaintiff's lab work only for a brief period of time, or not at all. Alternatively, it might reveal that a thorough examination of a record was performed, even if the plaintiff alleges otherwise. Though not easily accessible by the user, metadata can be uncovered by those with technical expertise. More importantly, metadata is generally discoverable and admissible in malpractice lawsuits [11].

A further complicating factor is changing liability risks as providers and health care systems transition from paper to electronic systems [12, 13]. Despite the incentives to adopt EHRs, transition to a completely paperless system can be a slow process, particularly as it needs to be done without significant interruptions in patient care. This transition can be fraught with liability pitfalls, particular when providers are caught, either temporarily or permanently, in a "hybrid" paper–electronic model. There are numerous potential problems with hybrid systems, the most significant of which are potential gaps in the EHR that may be incompletely or inefficiently filled with paper backup systems [14].

In the remainder of this chapter, we discuss case studies that will explore, in detail, some of the issues mentioned above. In the first case, the plaintiff was a patient injured secondary to an operative complication. Investigation of the metadata revealed discrepancies in the anesthesia monitoring record that eventually led to problems with mounting an effective defense. In the second case, the patient underwent a routine mammogram which was found to be abnormal. However, diagnosis was delayed because the treating hospital was transitioning from paper to electronic records; her results were misplaced in this shuffle.

Clinical Case Studies

Case Study 1: Clinical Summary

In this case, a 58-year-old male with a history of brain neoplasm was scheduled to undergo craniotomy [15]. The procedure began with anesthesia induction that occurred without incident, and the patient was placed on an electronic monitoring system that measures the patient's blood pressure and heart rate through an arterial and central venous catheter. After several hours, there was a routine shift change in anesthesia support personnel, including the nurse anesthetist and resident. After the change, it was noted that the monitoring system recording the patient's vital signs was no longer transmitting data. Eventually, the system was repaired and data transmission was restored; however, the absent data was never captured or entered manually.

Upon the patient's emergence from anesthesia, a severe complication was noted. Though the patient was spontaneously breathing, he had not yet had a return of motor function. Initially, this was felt to be due to the residual effects of anesthesia, but eventually it became clear that the patient had become quadriplegic. Initial investigation showed multiple gaps in the electronic record, resulting in significant periods where the patient's vital signs remained unmonitored and unrecorded. In fact, one gap was more than 90 min long, ample time for an undetected complication to cause injury. However, both the electronic system software and monitor were confirmed to be functioning correctly. Eventually, it was discovered that a cable

connecting the patient to the monitoring system had become accidentally disconnected.

Unsurprisingly, the injured patient and his family pursued an investigation and ultimately pursued a liability claim against multiple physicians involved in the patient's care, including the surgeon and the anesthesiologist. Attention ultimately turned to the latter, and he was accused of failing to meet the standard of care due to these gaps in monitoring. Per the plaintiff, standard of care demanded that the patient have his blood pressure and pulse monitored at least every 5 min; clearly, this did not occur. The plaintiff further alleged that, as a result of these monitoring gaps and improper patient positioning, the anesthesiologist failed to observe periods of significant hypotension that resulted in spinal cord ischemia and permanent neurological damage.

The defense in this case was, initially at least, difficult but not impossible to mount. Of course, the defendant had to acknowledge that there was likely an excessive reliance on the electronic monitoring system. Ultimately, when technology fails, the provider has a responsibility to turn to available manual backup systems. Clearly, there was a communication breakdown between the members of the anesthesia team. As the resident and nurse anesthetist signed off to each other, they should have discussed the absence of incoming vital signs with the attending physician; ideally, this data should have been entered manually to prevent any monitoring documentation gaps.

Other potential problems with the electronic monitoring system were identified and acknowledged by the defendant. Ideally, the monitoring system should revert to a "home" screen and alert the user if there is a break in data; this system failed to do so in an effective manner. Poor placement of monitoring screens may have contributed to the poor outcome, as they made it difficult for the anesthesiologist to simultaneously watch the patient and monitors. In this case, more attention was paid to the latter.

Despite these errors, the defendant was initially able to develop a plausible defense strategy based on previous experience with these types of surgical cases. He identified multiple previous cases in which the patient underwent similar physical positioning for similar surgeries. In many of these cases, the patient developed arterial blood pressures lower than the lowest recorded blood pressure sustained by the injured plaintiff. However, in these other cases, spinal cord ischemia did not develop.

Despite a reasonable strong potential defense on the medical facts of this case, ultimately the defendant physician had to settle due to problems with the documentation in the EHR. A key element in both the plaintiff and defendant case was presenting an accurate record of the timing of important events in the patient's care. The first problem was a discrepancy regarding the precise time that patient was placed into an upright position. The time stamp on the note the anesthesiologist filed did not appear to correspond to any changes in the patient's blood pressure. There was no independent documentation of the exact time of patient movement which created a suspicion that this note was inaccurate. An inaccuracy of this kind could potentially call into question much of the anesthesiologist's defense, which depended on persuading others of his version of the timing of events. Eventually,

the defense was able to rebut this discrepancy by turning to a unique characteristic of the EHR. Unlike paper anesthesia documentation, which records vital signs and other events in 5 min intervals, the electronic monitor recorded events in 1 min intervals. Close inspection of these intervals showed a blood pressure change that could likely be attributed to patient positioning near to the time documented by the attending anesthesiologist.

Ultimately, however, another aspect of the EHR dealt a blow to the defense from which it could not recover. As part of pretrial discovery, plaintiff's counsel demanded and received the metadata associated with electronic monitoring record. This data showed the electronic footprint left by all of the physicians that interacted with the record, including the time at which vital signs and other documentation were entered. Examination of the metadata uncovered a curious and troubling fact. Soon after the surgery had started, the anesthesiologist entered a note stating that he was present at the patient's emergence from anesthesia; this is a practice known as "prospective documentation." Clearly, this was not technically true, since the patient had not even started to awaken when this documentation was filed. As the note was untimed, cursory examination of the note would be unrevealing. However, this discrepancy could not be hidden from the metadata.

This discrepancy was devastating to the defense strategy. The plaintiff was able to undermine the anesthesiologist's general credibility, and specifically question the defendant's assertions regarding the timing of clinical events. The plaintiff was able to question whether the defendant was even participating in the case in any meaningful was, to say nothing of the actual quality of the care given. Eventually, the defendant settled this case for an undisclosed sum.

Analysis

This case captures the potential double edged nature of EHRs in liability suits. More specifically, the accessibility and admissibility of metadata has the potential to both protect and injure physician-defendants. In this case, examination of the metadata revealed clinical events that would have remained undiscovered if only paper records had been used. One of these events, the detailed, minute by minute recording of vital signs helped support the defendant physician's claim regarding the timing of patient positioning. However, the metadata also undermined the credibility of the defendant by revealing that he was willing to take shortcuts with documentation, which suggests that he might be willing to take shortcuts with patient care.

One interesting aspect of this case is that it is unlikely that errors were made in actual medical decision making. In many cases, the admissibility of metadata may damage a physician's case simply by creating the appearance of impropriety. In this particular instance, the damage to the defendant's case was due to questions regarding the documentation of the patient's emergence from anesthesia. However, there is no credible allegation that the actual management of this clinical event was faulty. This reflects a rather unique potential liability pitfall of EHRs. As the use of meta-

data becomes more common, every aspect of a physician's interaction with an electronic interface will be subject to legal scrutiny. There is no place to hide, and even clinically irrelevant details can be damaging when exposed.

The admissibility of metadata may also have consequences when the accusations are actually clinically relevant. Analysis of a physician's electronic footprint through a health record allows the plaintiff and defendant to recreate each step of the clinical care provided to the patient. Metadata will confirm whether a physician actually looked at a patient's previous notes, and for how long. It will confirm which labs and radiology reports were examined, and for how long. It will time stamp every order that is entered, and allow an examiner to determine the order in which these orders were entered. The legal consequences of this level of transparency are obvious. Clearly, in some cases the metadata might be used to support a physician's assertions. However, one can easily imagine even more scenarios where it can be used to directly impeach a provider's testimony. For example, if a physician asserts that he saw no evidence of a mass on a patient's chest radiograph, a jury would likely look very poorly on his clinical judgment if metadata revealed that this film was examined only briefly.

Solutions

There are several potential solutions to minimize the liability exposure of metadata. Obviously, the easiest is increased awareness. Behave and document as if someone is always (electronically) looking over your shoulder, because they might be. Clearly, clinical decisions should be made based entirely on patient needs, but documentation may involve more than simply conveying information. The metadata always tells a story above and beyond progress notes and history; physicians need to take control of this narrative. One way to do this is to maintain a consistent protocol when using an EHR. If possible, develop patterns that govern the sequence in which you access information, in order to ensure that nothing is missed. Not only will this enhance patient safety, but may help provide an intelligible narrative for physician behavior if there is a lawsuit.

Prospective charting must be completely avoided. This type of charting occurs when providers chart events in advance, as they anticipate that they will not have time to effectively do so as the event is occurring. The aforementioned case is one example of the practice. A more common example is the practice of writing "skeleton" inpatient or outpatient notes prior to the encounter, sometimes the day before. These practice is designed to increase the efficiency of documentation during busy periods of patient care. However, as this case demonstrates, if managed poorly, these notes can be a source of liability exposure. If you document histories or physical exams before they occur, your credibility may be shattered even if the documentation had no impact on patient care.

Case Study 2: Clinical Summary

In this case, the patient was a middle aged woman who underwent a mammogram ordered by her primary care physician [16]. This study was completely routine; the patient had no complaints and ordering physician had no increased suspicion of a positive finding. The patient reported that she was told that she would be contacted within a week or two after the study if it was abnormal; if she did not hear from the physician, she should assume that the mammogram was normal. Months passed, and while doing a routine breast self-examination, the patient palpated a mass. She eventually contacted her primary care physician, and saw him in consultation. He confirmed the presence of the mass, and mentioned that he had never received the results of the mammogram ordered earlier that year. He finally tracked down these previous results, and was shocked to discover that the reviewing radiologist had documented a suspicious breast mass and recommended biopsy. The patient became distraught and hysterical upon hearing this information. The patient's primary provider immediately ordered another mammogram, which found a lesion with "irregular borders and measures approximately 2 cm in greatest diameter and is highly suspicious for carcinoma." Biopsy was again recommended, and when performed, confirmed the presence of infiltrating ductal carcinoma. The patient underwent lumpectomy, chemotherapy and radiation. Axillary lymph node dissection showed metastases to multiple nodes; there was no evidence of spread to other organs, and at the time of the lawsuit, the patient appeared to be in remission.

Obviously, a significant error had been made, and the patient filed a lawsuit on multiple grounds. The primary focus of this lawsuit was whether the hospital breached its duty by failing to implement an adequate process for the dissemination of test results. This question was the fundamental issue of the lawsuit, and is the primary learning point of this case. Specifically, this particular hospital had recently implemented an EHR system, and clearly had not worked out its potential problems. Prior to this event, this hospital had an entirely paper-based system of delivering lab results. When a physician wished to order a radiological examination, he would write his request on a multilayer, multipart form. This form was taken to the Radiology department; the reading radiologist would personally write the results of the study directly onto this requisition. Carbon copies of this form were then divided among the interested parties. One copy would remain in the Radiology department, for comparison in case future studies were ordered. One copy would be placed in the patient's permanent medical record. A final copy would be reserved for the ordering physician; personnel from the ordering clinic would physically pick up the results from the Radiology department and hand carry them back to the ordering department, and sign a logbook confirming receipt. In the case of an abnormal result, the radiologist was expected to telephone the ordering physician. One limitation of this system was that the Radiology Department had no method of verifying that the ordering physician actually received the written report.

In spring of the year of the incident, the hospital began implementation of an EHR system that would report all results by computer. Once a radiology result was

available, the requesting physician would be notified that a result was pending, every time he logged into the computer. It would continue to flag this result until the ordering provider electronically signed the result. In addition, if the radiology result had been flagged as "abnormal," the system would also generate an email warning to the provider. However, because all physicians could not be immediately trained to use this system, a transition period of several months was required. During this transition period, a backup paper system was put in place; this backup system was to be discontinued once the EHR was fully completed. In addition to the electronic result, once a radiology result became available, a transmission would automatically be sent to a preselected printer in the department of the ordering physician. The result would be automatically printed, and it would be that department's responsibility to then transfer this printed result to the appropriate provider. A third backup was verbal communication between the reading radiologist and the ordering physician; in the case of abnormal results, the radiologist would retain the option to inform the provider verbally by phone, and document this conversation.

The incident that resulted in the lawsuit and missed diagnosis occurred during the transition period between paper and electronic recording keeping. The ordering physician had not yet been trained on use of the EHR, and was likely anticipating receiving results by the familiar method of personal delivery of paper results, or at least through a printout on his departmental printer. Neither of this occurred, for unclear reasons. Review of the record revealed that the initial abnormal mammogram result had never been printed at the appropriate printer, a clear failure in the system. Prior to this time, the hospital had a generally favorable experience with automatic printing of results; during the transition, there were only a handful of "failures to print" because the printer was out of paper or was in the middle of a software upgrade. These failures were promptly repaired without incident. The ordering physician was clearly expecting the paper system to serve as an effective backup, which it did not, nor did he or any member of his staff follow up on the ordered test to check the results.

On the other end of the care sequence, the reading radiologist fell prey to incorrect assumptions regarding the transition from paper to electronic records. By his own admission, he was not very adept at use of electronic records, and assumed that his electronic reports were accessible to the ordering physician. Unfortunately, he did not realize that during the transition period, there were physicians that lacked such access. He also assumed that the backup paper system was functioning properly, and depended on his staff to ensure that paper copies of his report made it back to the appropriate physicians. These incorrect assumptions likely made him think it was unnecessary to personally call to convey these abnormal results.

Eventually, the court found that neither the hospital nor physicians breached their standard of care; judgment was rendered for the defendant. Interestingly, however, the court did find that hospitals and providers had a legal obligation to ensure that an appropriate reporting system was set up during periods of transition from paper to electronic record keeping.

Analysis

It is vitally important to appreciate the liability dangers associated with transitioning from paper to EHRs. The advantages of the latter are well known and well documented. However, as this case illustrates, paper records have certain advantages as well. The previous system used by this hospital, though unwieldy and labor intensive, was still effective. It was a simple, uniform system with minimal moving parts and no significant ambiguities. Its primary weakness was that the Radiology department was unable to routinely verify that a final report actually reached the ordering physician. Nevertheless, the system was reliable enough that direct verbal contact between radiologist and ordering physician was not felt to be routinely necessary. Alternatively, once the EHR was fully implemented, and all providers were included, it too would likely serve as an effective method of disseminating results, with less effort and cost than paper records. In fact, it could likely be programmed to avoid the weakness of paper records, by building in mechanisms to confirm that results reached an ordering physician, and that he reviewed them.

Unfortunately, during the transitional period, the whole was less than the sum of the parts. The presence of the electronic system created the expectation that everyone would be using the system, though this was not true. This likely created a false sense of security, perhaps even complacency. Though there was a backup paper system, it was not a simple continuation of the previous (and effective) paper system, but an entirely new system with new variables such as automatic printing of results on distant printers. As with many new systems, the reality did not match the expectations.

Solutions

Obviously, there were technical glitches in this scenario that led to poor outcomes, such as printer failure. However, the systemic error is failure to ensure a more deliberate and careful transition period between electronic and paper records. The key characteristic of a successful transition is ensuring that all involved providers have accurate expectations. Transition periods should avoid piecemeal approaches that cover only certain providers. Furthermore, a transition period is generally not a good time to initiate a new system, such as in this scenario, where an entirely new method of disseminating through remote printers was implemented. Ideally, if a transition period is necessary, the previous system should be continued until the new one is fully operational.

Key Lessons Learned

- Every moment of every interaction with an EHR is likely discoverable.
- Avoid prospective documentation, particularly regarding variables such as physical examination.

- Metadata can be used to undermine a physician's credibility, even if no medical errors are made.
- The transition from paper to EHRs can be fraught with liability pitfalls. Avoid new or complicated new systems during this transition period. Health care providers and systems have a legal obligation to ensure that an effective system for this transition is in place.

References

1. Mangalmurti S, Murtagh L, Mello M. Medical malpractice in the age of electronic health records. N Engl J Med. 2010;363:2060–7.
2. Hodge Jr JG, Gostin LO, Jacobson PD. Legal issues concerning electronic health information: privacy, quality, and liability. JAMA. 1999;282:1466–71.
3. Woodward B. The computer-based record and confidentiality. N Engl J Med. 1995;333: 1419–22.
4. Blumenthal D, Glaser JP. Information technology comes to medicine. N Engl J Med. 2007; 356:2527–34.
5. Hoffman S, Podgurski A. E-health hazards: provider liability and electronic health record systems. Berkeley Tech Law J. 2009;24:1523–81 (Available at http://www.btlj.org/data/articles/24_4/1523_Hoffman.pdf. Last accessed Dec. 14, 2014).
6. Walsh KE, Adams WG, Bauchner H, Vinci RJ, Chessare JB, Cooper MR, et al. Medication errors related to computerized order entry for children. Pediatrics. 2006;118:1872–9.
7. Thielke S, Hammond K, Helbig S. Copying and pasting of examinations within the electronic medical record. Int J Med Inform. 2007;76 Suppl 1:S122–8.
8. Hammond KW, Helbig ST, Benson CC, Brathwaite-Sketoe BM. Are electronic medical records trustworthy? Observations on copying, pasting and duplications. AMIA Annu Symp Proc. 2003;2003:269–73.
9. Hickson GB, Federspiel CF, Pichert JW, Miller CS, Gauld-Jaeger J, Bost P. Patient complaints and malpractice risk. JAMA. 2002;287:2951–7.
10. Miller AR, Tucker CE. Electronic discovery and electronic medical records: does the threat of litigation affect firm decisions to adopt technology? Washington, DC: Federal Trade Commission; 2009 (Available at http://hdl.handle.net/1721.1/75884. Last accessed 14 Dec 2014).
11. Williams v. Sprint/United Mgmt. Co., 2005 WL 2401626 (D.Kan. Sept. 29, 2005).
12. Lorenzi NM, Novak LL, Weiss JB, Gadd CS, Unertl KM. Crossing the implementation chasm: a proposal for bold action. J Am Med Inform Assoc. 2008;15:290–6.
13. Han YY, Carcillo JA, Venkataraman ST, Clark RSB, Watson RS, Nguyen TC, et al. Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. Pediatrics. 2005;116:1506–12 [Erratum, Pediatrics 2006;117:594].
14. Casalino LP, Dunham D, Chin MH, Bielang R, Kistner EO, Ong MK, et al. Frequency of failure to inform patients of clinically significant outpatient test results. Arch Intern Med. 2009;169:1123–9 [Erratum, Arch Intern Med 2009;169:1626].
15. Vigoda MM, Lubarsky DA. Failure to recognize loss of incoming data in an anesthesia record-keeping system may have increased medical liability. Anesth Analg. 2006;102:1798–802.
16. SMITH v. U.S., 119 F.Supp.2d 561; 2000.

Chapter 17
Improving HIT Safety Through Enterprise Risk Management

Elizabeth M. Borycki and Andre Kushniruk

Introduction

Risk management is an important aspect of health information technology (HIT) implementation and maintenance for health care organizations (e.g., regional health authorities, hospitals, and long-term care facilities) [1]. At an enterprise level, chief medical information officers, chief nursing information officers, chief information officers, and other HIT managers all play a role in ensuring that patients are not harmed and that the safety and quality of the HIT used by frontline clinicians (e.g., physicians, nurses, and pharmacists) is high [2]. Key to the role of enterprise risk management is providing the safest HIT systems possible given the current state of technology advances and using evidence to inform decision making through employing an enterprise level risk management strategy.

Today, research and media reports are increasingly documenting the presence of safety issues involving technology [3]. It is expected that the number of these types of reports will grow as we become more reliant on HIT to support health professionals' work in delivery of care [4]. That said, research has also documented the critical role that HIT has had in the past two decades in improving patient safety; for example, eliminating errors arising from illegible or difficult to read hand writing [5], eliminating transcribing errors [6], and providing clinicians with real-time decision support where there is a drug–drug and drug–allergy interaction present [7]. These advances in safety have their origins in HIT developed and studied by biomedical and health informatics researchers [2, 8].

E.M. Borycki, R.N., Ph.D. (✉) • A. Kushniruk, M.Sc., Ph.D.
School of Health Information Science, University of Victoria,
Human & Social Development Building A202, 3800 Finnerty Road (Ring Road),
Victoria, BC, Canada, V8P 5C2
e-mail: emb@uvic.ca; andrek@uvic.ca

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_17

Technology-Induced Errors: A Concern for Health Care Organizations

It has been recognized that HIT can both improve patient safety as well as introduce new types of technology-induced errors [9–11]. As many of these errors arise from human factors [9, 10], socio-technical [2], contextual [3], and technology based sources [4, 10, 11], HIT managers need to be conscious of these issues and institute organizational practices and processes that can support use of safe HIT while at the same time preventing the introduction of new types of errors. These new types of errors arise from interactions between the technology and the context of work, organizational practices and processes, and local country health care system practices and processes [9–19]. Key to this is the development of an enterprise level strategy that can prevent the introduction of new types of HIT related errors as well as address those near misses and errors identified by health professionals. Before discussing enterprise risk management, we will first provide some background to the issue of technology-induced errors.

Understanding the Origins and Contributing Factors to Technology-Induced Errors

Technology-induced errors "arise from: (a) the design and development of technology, (b) the implementation and customization of a technology, and (c) the interactions between the operation of a technology and the new work processes that arise from a technology's use" ([11], p.154). These also include errors that have their origins in messaging between different health information systems (e.g., pharmacy and clinician order entry systems), and medical devices (e.g., an electronic health record (EHR) and wireless intravenous pump). These errors involve actual and potential medical errors that may arise from and manifest during the complex human and/or technical interactions that take place between HIT, health professionals, patients, organizations, and other HIT [9, 11, 12, 20]. They include "slips" and "mistakes." Slips are errors that are caught by health professionals before they occur. Mistakes are not caught by end users of systems or HIT professionals before being documented [9].

Managing the Risk of Technology-Induced Errors

To illustrate, we consider the work of Borycki and colleagues [20] who adapted the work of Reason [21] to technology-induced errors involving HIT (Fig. 17.1). On the far right of Fig. 17.1 (called the "sharp end" of the model), an error has occurred.

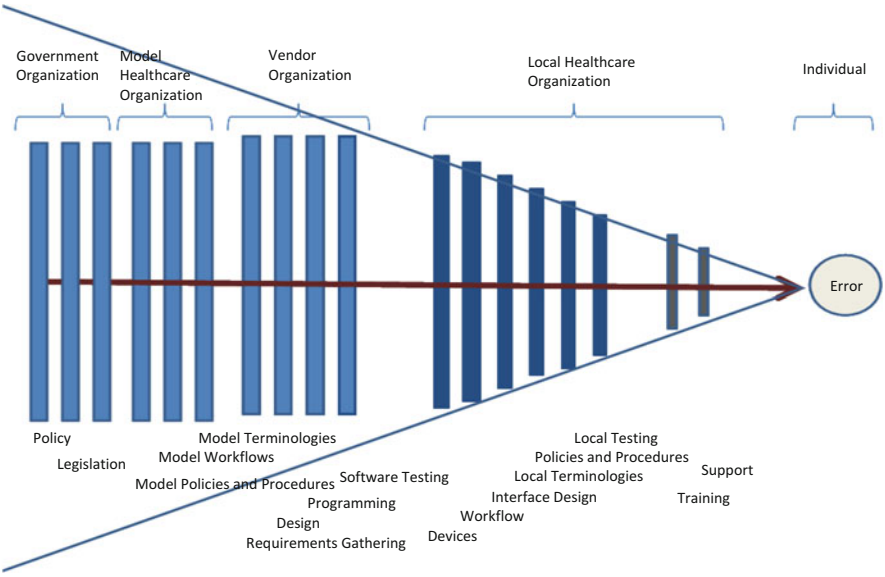


Fig. 17.1 A framework for diagnosing technology-induced errors in health care. Permission to reprint granted by IOS Press

The path that leads to that error (see the arrow in Fig. 17.1) may have causes that may involve problems introduced at multiple layers (indicated by the vertical bars in Fig. 17.1).

As illustrated in Fig. 17.1, technology-induced errors can be introduced at different points in time by different organizations such as governments, model health care delivery organizations used as a foundation for technology design, HIT vendors, and local health care organizations that have implemented or are currently using HIT to support patient care processes. For example, when a government introduces new laws, regulations or policies that differ from those embedded in the HIT we may introduce a technology-induced error. If a vendor organization designs their HIT on a "model health care organization" that has safety issues, those "safety" issues may become embedded in the HIT by the technology designers, developers, and programmers (and become part of the software product) thereby leading to technology-induced errors. As well, vendor organizations themselves can be a source of technology-induced errors. If there is poor requirements gathering, design, programming, implementation, and maintenance of HIT technology-induced errors may be introduced. Lastly, local organizations can introduce technology-induced errors if HIT is poorly customized (in terms of health care terminologies, workflows, procedures, and policies) to local health care processes and practices, system training is inadequate or local software testing, usability testing or workflow testing has not taken place. Either in isolation or in combination, these potential "technology system" issues may lead to the introduction of "technology-induced errors."

Managers need to be aware of these sources of technology-induced errors and develop enterprise risk management strategies to address them. There are a number of opportunities for enterprise risk management at the regional health authority as well as hospital level. Risk management begins with understanding how a technology affects clinical practice after it is implemented [20–26]. Clinical simulations represent a methodology that can be used to learn about the potential implications of software and/or hardware upon clinician work prior to wide-spread deployments [22, 23].

Clinical Simulations

Clinical simulations have appeared as a key methodology aimed at detecting technology-induced errors [22]. Clinical simulations represent an extension of usability testing to include consideration of the complex environmental and contextual factors that will affect safe use of a new system [23]. In such simulations, representative users (e.g., physicians or nurses) are observed as they use the HIT under study to carry out representative tasks. This typically involves recording all interactions (e.g., computer screens and audio of user interaction) [22–26]. In addition, such studies are typically conducted either in realistic simulation laboratories, or ideally in the actual setting and context where a system is to be deployed (i.e., "in situ"), for example in a hospital room off hours [9, 22, 23, 26–31]. The information about the impact of a new HIT on user workflow and safety can be invaluable and can provide detailed information about where to improve and modify the HIT prior to wide spread implementation [9, 22, 24, 26]. In the next section, we will discuss how clinical simulation can be used as a risk management strategy within the context of a case study.

Case Study

The following case study is based on a risk management approach undertaken by a large hospital that was planning to implement an electronic medication administration system to be used by physicians and nurses hospital wide. Initial comments from clinicians suggested that the system was not seamlessly fitting in with clinical workflow. In response, the head of the information management and technology department worked with human factors experts to conduct clinical simulations and understand how the technology would affect clinician work prior to wide spread implementation as the costs of reimplementation and retraining of clinicians would be greater after the system was implemented than if potential issues were addressed prior to wide spread release [22–25, 27–31].

Clinical Summary

An empty hospital room was used to test the software. In the hospital room there was a typical hospital bed, bedside table, IV poles, oxygen equipment, and suction equipment. A mannequin (that acted as the patient) was put in a hospital bed and a bar-coded bracelet was placed around the mannequin's wrist [28–30]. A laptop was placed on a wireless cart, and bar code scanning equipment was integrated with the laptop's medication administration system. The laptop was also loaded with the local hospital EHR system. A patient case was developed by a team of health informatics professionals and clinicians. The case was representative of the types of patients clinicians typically care for at this hospital. Also, the medications that were prescribed to the patient represented commonly given medications in that hospital that had different routes of delivery (e.g., oral, intramuscular, and intravenous) [28, 29]. The data from the patient case was uploaded to the EHR and the medication administration systems.

The test patient was prescribed 10 different medications to be given at 10 AM by different routes of delivery including orally, intramuscularly, and intravenously. Instructions were given to the nurses and physicians who would test out the system for its usability and impact on clinical workflow and patient safety [28, 29].

To capture participants' interactions with the software, hardware, and objects in the hospital room (e.g., hospital bed and bedside table) as well as the "patient," two types of recording equipment were used: (1) on the computer where the medication administration system was deployed, screen recording software was installed (which also allowed for audio recording) (2) a video camera was set up on a tripod to obtain a record of health professional interactions with physical objects in the room, e.g., the computer and the "patient" [28, 29].

Participants were instructed to verify the patient, review the medication list, and verify the medication that was to be taken by the patient. Following this, participants were asked to administer the medications and document the administration of the medication in the medication administration record. Participants were asked to "think aloud" during the entire process. In "thinking aloud" the health informatics professionals were able to learn about what the health professionals were attending to in the process of administering the medications, whether it be the patient, the medication administration system or the medications themselves. The computer screen recording software was activated and the video recorder was turned on for the duration of each participant's interactions with the technology and the patient. After, each participant completed the medication administration tasks, the health informatics professionals would ask questions to clarify any activities that the participant performed that were not understood fully by the observers to obtain further information and to provide additional comments and insights into the medication administration system [28, 29].

Analysis

Computer screen and video data were collected by the health informatics professionals for review. In total, 16 participants (doctors and nurses) administered medications to the patient. The participants were from a hospital that was highly automated and had worked extensively with an EHR system in that hospital. The computer screen recordings and the external recordings of participant activities were integrated using Transana® video coding software so that one could view what was being done by the participant on the computer screen, in the context of the hospital room as they used the laptop and the barcode scanning equipment to administer patient medications [28, 29].

The video data, i.e., computer screen recordings and video data of the participants interacting with the computer hardware and the equipment in the hospital room was viewed by health informatics professionals. Along with this, the audio data that was captured as part of the clinical simulation were reviewed in the context of the video data. The audio was transcribed and the transcripts were annotated with the participants' activities [26]. In this process usability and clinical workflow problems were identified [26, 28, 29].

Clinical workflows associated with the newly tested medication administration process were more complicated than that those present in the clinical setting (before the introduction of the new medication administration system). More steps had to be taken to administer the same number of medications. These workflows became particularly complex when administering intramuscular medication and intravenous medications as the participants attempted to balance the software work, bar coding scanning and verification work on the laptop and the hospital equipment (e.g., IV poles) [28, 29].

The serial and rigid nature of the sequence imposed by the computer system would lead to safer medication administration under some circumstances and contexts of use (i.e., a small number of oral medications to be administered with no interruptions for the nurse or physician). However, if the nurse or physician administering the medication was under intense time pressures, the rigid nature of the sequence of medication administration activities (i.e., where all steps of the process had to be completed on the computer) actually made the interaction with the patient less safe as precious time could be lost. In testing the system with multiple nurses and physicians, it was found that the system locked the data for an individual patient at the wrong level; the entire medication administration record for the patient being accessed by one health provider was found to be completely inaccessible to other health providers who needed to look at that record [28, 29].

Solutions

This case shows how clinical simulations can be used to identify potential technology-induced errors arising from user interface and clinical workflow issues. After reviewing the data from the clinical simulations the health informatics

professionals and clinicians developed a number of potential solutions. The solutions were implemented prior to wide spread release of the medication administration system in the health care organization. These solutions included the following: (a) streamlining of the steps required to administer multiple medications, (b) introduction of an emergency override (in conjunction with an audit trail that could be reviewed later) that would allow for steps in the process to be overridden during emergencies when there was not enough time to follow the computer sequence completely, (c) modification of the locking of records to allow other health professionals to access and see key parts of a patient record while another health professional was accessing the record to administer medication. After these solutions were put in place, the system was implemented widely in the hospital with few subsequent reported problems and with a high level of adoption [28, 29].

The case demonstrates how risk management by an organization can effectively reduce the likelihood of a technology-induced error after the implementation of the medication administration system. More specifically, this study demonstrates how a provider organization effectively used clinical simulation, a risk management approach, to identify potential technology-induced errors. These potential errors were addressed prior to wide spread release—leading provider organizations to achieve cost savings that included avoiding: (a) the costs of litigation, (b) the cost of treating a patient that has been harmed, and (c) the cost of modifying the system and retraining health care providers across an organization if these errors are found after a system had been implemented [22, 28, 29]. Physicians and nurses who participated in the clinical simulations enjoyed providing their input to this risk management process. The findings were used to provide feedback into local organizational plans for implementing a medication administration system (Fig. 17.1) [28, 29].

The case also highlights the value of clinician reports (e.g., physician, nurse) and insights into the effects of technology upon clinical processes [26, 28–31]. In this case physicians and nurses were asked to participate in clinical simulations to identify potential technology-induced errors prior to the implementation of a medication administration system [26, 28, 29]. Physicians and nurses were asked to identify potential issues associated with using the technology and interpreting the impact of the new technology upon clinical workflow [26, 28, 31]. Clinician reports are important in the context of clinical simulation to assess technology from a risk management perspective. Clinician reports are also important from a risk management perspective after a HIT system has been implemented [22, 28, 29].

Newly implemented HITs as well as those that are being used daily to provide patient care are being used to support ever increasingly complex health care activities as well as patients with new or emerging diseases, frequently encountered medical conditions and rare diseases. Technology-induced errors may arise, be observed by clinicians, and reported in the form of organizational incident or error reports [10, 22]. Such reports can provide insights into near misses and actual technology-induced errors [9]. Clinical simulations can be used to understand how the technology-induced error occurred and to provide meaningful insights as to how the technology and organizational policies and procedures can be modified / changed

to prevent similar errors from occurring [22, 26, 28–31]. Incident reports can be used to drive clinical simulations and thereby identify sources of technology-induced errors. Here, there is an opportunity to prevent future technology-induced errors in implemented systems through a better understanding of the technology and its interactions with clinical processes. In addition to this, information from clinical simulations can also be used to train health professionals about safe use of the technology system [32].

Key Lessons Learned

- Risk management is important when implementing an HIT system.
- Clinical simulations can be used to identify potential technology-induced errors arising from user interface designs and clinical workflows prior to wide-spread systems release.
- Health professionals (e.g., physicians and nurses) can be asked to participate in clinical simulations to obtain their perspectives on potential technology-induced errors prior to systems release.
- Clinical simulations result in significant cost savings as they can prevent potential future technology-induced errors from occurring after wide spread release of an information system.
- Health professional reports can be used as inputs to clinical simulations in order to identify ways in which near misses and actual technology-induced errors can be prevented.

References

1. Van Merode GG, Groothuis S, Hasman A. Enterprise resource planning for hospitals. Int J Med Inform. 2004;73:493–501.
2. Institute of Medicine. Health IT, and patient safety: building safer systems for better care. Washington: National Academy of Science; 2011.
3. Medical Economics. EHRs pose potential threat to patient safety. Available at http://medicaleconomics.modernmedicine.com/medical-economics/content/tags/ehrs/ehrs-pose-potential-threat-patient-safety?page=full. Accessed 6 Sept 2015.
4. Borycki EM. Technology-induced errors: where do they come from and what can we do about them? Stud Health Technol Inform. 2013;194:20–6.
5. Edwards M, Moczygemba J. Reducing medical errors through better documentation. Health Care Manag. 2004;23(4):329–33.
6. Mekhijian HS, Kumar RR, Kuehn L, Bentley TD, Teater P, Thomas A, et al. Immediate benefits realized following implementation of physician order entry at an academic medical centre. J Am Med Inform Assoc. 2002;9(5):529–39.
7. Wolfstadt JI, Gurwitz JH, Field TS, Lee M, Kalker S, Wei W, et al. The effect of computerized physician order entry with clinical decision support on the rates of adverse drug events: a systematic review. J Gen Intern Med. 2008;23(4):451–8.

8. Bates DW, Teich JM, Lee J, Seger D, Kuperman GJ, Ma'Luf N, et al. The impact of computerized physician order entry on medication error prevention. J Am Med Inform Assoc. 1999;6(4):313–21.
9. Kushniruk AW, Triola MM, Borycki EM, Stein B, Kannry JL. Technology induced error and usability: the relationship between usability problems and prescription errors when using a handheld application. Int J Med Inform. 2005;74(7):519–26.
10. Magrabi F, Ong MS, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. J Am Med Inform Assoc. 2012;19(1):45–53.
11. Borycki EM, Kushniruk AW. Where do technology-induced errors come from? Towards a model for conceptualizing and diagnosing errors caused by technology. Human, Social and Organizational Aspects of Health Information Systems. 2008;148–165.
12. Borycki EM, Kushniruk AW. Towards an integrative cognitive-socio-technical approach in health informatics: analyzing technology-induced error involving health information systems to improve patient safety. Open Med Inform J. 2010;4:181–7.
13. Settergren T. Is health information technology safe? 2014. Available at http://socal.himsschapter.org/News/content.aspx?ItemNumber=33692. Accessed 6 Sept 2015.
14. Terry K. EHRs linked to errors, harm, AMA says. 2012. Available at http://www.informationweek.com/healthcare/electronic-health-records/ehrs-linked-to-errors-harm-ama-says/d/d-id/1102259. Accessed 6 Sept 2015.
15. California nurses' association. Sutter's new electronic system causes serious disruptions to safe patient care at E. Bay hospitals. 2012. Available at http://www.nationalnursesunited.org/press/entry/rns-say-sutters-new-electronic-system-causing-serious-disruptions-to-safe-p/. Accessed 6 Sept 2015.
16. 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):104–12.
17. Ash JS, Sittig DF, Poon EG, Guappone K, Campbell E, Dykstra RH. The extent and importance of unintended consequences related to computerized provider order entry. J Am Med Inform Assoc. 2007;14(4):415–23.
18. 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):387–8.
19. Koppel R, Metlay JP, Cohen A, Abaluck B, Localio AR, Kimmel SE, et al. Role of computerized physician order entry systems in facilitating medication errors. J Am Med Assoc. 2005;293(10):1197–203.
20. Borycki EM, Kushniruk AW, Keay L, Kuo A. A framework for diagnosing and identifying where technology-induced errors come from. Stud Health Technol Inform. 2008;148:181–7.
21. Reason J. Human error. New York: Cambridge University Press; 1990.
22. Borycki E, Keay E. Methods to assess the safety of health information systems. Healthc Q. 2009;13:47–52.
23. Kushniruk A, Nohr C, Jensen S, Borycki EM. From usability testing to clinical simulations: bringing context into the design and evaluation of usable and safe health information technologies. Contribution of the IMIA human factors engineering for healthcare informatics working group. Yearb Med Inform. 2012;8(1):78–85.
24. Kushniruk A, Beuscart-Zephir MC, Grzes A, Borycki E, Watbled L, Kannry J. Increasing the safety of healthcare information systems through improved procurement: toward a framework for selection of safe healthcare systems. Healthc Q. 2009;13:53–8.
25. Koppel R, Wetterneck T, Telles JL, Karsh BT. Workarounds to barcode medication administration systems: their occurrences, causes, and threats to patient safety. J Am Med Inform Assoc. 2008;15(4):408–23.
26. Borycki EM, Kushniruk AW, Kuwata S, Kannry J. Engineering the electronic health record for safety: a multi-level video-based approach to diagnosing and preventing technology-induced error arising from usability problems. Stud Health Technol Inform. 2011;166:197–205.

27. Kushniruk AW, Patel VL. Cognitive and usability engineering methods for the evaluation of clinical information systems. J Biomed Inform. 2004;37(1):56–76.
28. Kushniruk A, Borycki E, Kuwata S, Kannry J. Predicting changes in workflow resulting from healthcare information systems: ensuring the safety of healthcare. Healthc Q. 2006;9:114–8.
29. Borycki EM, Kushniruk AW, Kuwata S, Watanabe H. (2009). Simulations to assess medication administration systems. In: Bettina S, Victoria H, Herwig O (Eds). Nursing and clinical informatics: socio-technical approaches. Hershey, Pennsylvania: IGI Global, 2009. p. 144–159.
30. Kushniruk A, Nohr C, Jensen S, Borycki EM. From usability testing to clinical simulations: bringing context into the design and evaluation of usable and safe health information technologies. Yearb Med Inform. 2012;8(1):78–85.
31. Baylis TB, Kushniruk AW, Borycki EM. Low-cost rapid usability testing for health information systems: is it worth the effort? Stud Health Technol Inform. 2011;180:363–7.
32. Kushniruk AW, Myers K, Borycki EM, Kannry J. Exploring the relationship between training and usability: a study of the impact of usability testing on improving training and system deployment. Stud Health Technol Inform. 2009;143:277–83.

Chapter 18
Managing HIT Contract Process for Patient Safety

Marilyn Lamar

Introduction

Health information technology (HIT) is often selected based on price and a non-binding demonstration of functionality without determining whether the vendor is in fact obligated under the contract to (1) provide the features and functions demonstrated, (2) address ongoing safety issues, and (3) be responsible for errors caused by its own product. Failing to address these elements in the contract may increase the risk of errors that may jeopardize patient safety.

Customers may inadvertently contribute to this risk by rushing to finalize a contract without adequate review and negotiation. There may be pressure to implement quickly in order to obtain a vendor's discount (although such discounts are often extended) or to meet federal meaningful use requirements. In addition, customers often fail to tell the vendor that the contract terms will also be an important element of the selection process. Giving the vendor notice up front should help preserve the customer's leverage in negotiations.

It may take significant time and effort to figure out whether what was promised by the vendor is in fact reflected in the contract. It is also important to determine whether the customer itself has unstated assumptions about how the technology will work, either on a stand-alone basis or with other technology. These assumptions need to be identified and tested as part of the selection process.

The contract review and negotiation process, therefore, plays an important role in assuring patient safety and avoiding unintended consequences of HIT. The goal of understanding what the product does and does not do—and

M. Lamar, B.S., J.D. (✉)
Liss & Lamar, P.C., 1301 West 22nd Street, Suite 709, Oak Brook, IL 60523, USA
e-mail: mlamar@lisslamar.com

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_18

the limitations of the vendor's support and other obligations—is key because it can provide the opportunity to select a safer product. Even if a different product is not chosen, knowing some of the risks in advance should allow the customer to implement procedures or apply extra resources to reduce the risks before they occur.

Some examples of patient safety issues that could have been avoided or minimized through the contract process include the following:

- Physicians were unable to access patient data for a day from their "cloud" based electronic health record (EHR) system when the EHR vendor experienced a lack of capacity similar to an electric utility "brown-out." This risk of unavailability could have been reduced by uptime guarantees in the agreement. Patient charts also could have been printed in advance if prior notice of anticipated problems was contractually required.
- Corrupted patient information was received from a business associate under an agreement that did not include a warranty that the information submitted could later be retrieved with no loss of accuracy.
- Patient drug allergies were not identified in time because the customer misunderstood the scope of the vendor's clinical support tool. The customer assumed that the technology would check drug allergies but it only checked for drug–drug interactions. The vendor had not represented that it would provide alerts for drug allergies and the customer failed to ask the vendor about this unstated assumption.
- Patient information was unavailable from the previous system when the customer transitioned to a new system. The contract for the old system did not require the vendor to provide transition assistance such as providing data in a generally accepted format.

This chapter is limited to a few key provisions that may impact on patient safety, but it does not address all of the terms that may be important for patient safety or numerous other important provisions. **It is not legal advice**, which depends on the customer's specific circumstances and state law. It is advisable to consult with an experienced attorney for legal advice that can help a customer with its specific contract.

Additional resources that should be helpful in addressing these issues include:

- The Joint Commission's Sentinel Event Alert 42, *Safely implementing health information and converging technologies* and The Joint Commission's Sentinel Event Alert 54, *Safe use of health information technology* [1].
- The SAFER Guides issued by the Office of the National Coordinator of the Department of Health and Human Services [2].

Key HIT Contract Provisions that Impact Patient Safety

"Entire Agreement" Clause Excludes Anything Not in the Agreement

Almost every vendor contract includes a statement that it is the "entire agreement" between the parties regarding the technology. It may look like this:

> *Entire Agreement. This Agreement is the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior or contemporaneous representations, proposals, understandings or agreements, whether written or oral.*

This language may be very favorable to the vendor because it generally means that none of the vendor's proposals, product descriptions, demonstrations, letters, e-mails, prior agreements, oral statements, or other communications are binding on the vendor unless they are expressly included. As a result, what the salesperson said orally and what has been demonstrated or stated in a proposal is not binding unless it is set forth in the contract.

Therefore a critical part of contract negotiation is to reconstruct what has been promised by the vendor and make sure it is actually in the contract in a way that adequately protects the customer. It is possible to include some documents by expressly referring to them if they are very long, although the customer should be sure to keep a copy (This approach is sometimes referred to as incorporating the document by reference.). If the document is posted on the vendor's website, the exact language referring to the document should be carefully reviewed to make sure that the vendor cannot change it by posting a revised version on the website without the customer's consent. The customer should also keep a copy of terms posted on a website.

An equally important part of this process is to identify what assumptions the customer has made regarding the technology and try to have them included in the agreement. For example, has the customer assumed that the product will be updated to address patient safety issues if any arise? The vendor may be unaware of these assumptions, so it is especially important for the customer to find out whether the vendor will include them as contractual obligations.

Disclaimer of Warranties

Warranties are promises that may be stated in the contract ("express" warranties) or warranties that are not in the contract because they are "implied by law." It is very important to make sure that the express warranties are sufficient to cover what the customer expects the technology to do because most contracts include a disclaimer of warranties that might be implied by law. The following is an example of warranty disclaimer language (favorable to the vendor):

No Other Warranties. VENDOR DISCLAIMS AND EXCLUDES ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, OTHER THAN THOSE EXPRESSLY SET FORTH IN THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, SATISFACTORY QUALITY, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SOFTWARE, FIXES, RELATED MATERIALS AND SERVICES.

Terms like "merchantability" in the disclaimer originate in the Uniform Commercial Code (the "UCC") which governs the sale of goods in all states. Although the UCC does not always apply to software or services, vendors often disclaim these implied warranties in case the UCC does apply. The UCC requires that a disclaimer be "conspicuous" which is why the disclaimer language is often in all capital letters.

Even if not disclaimed, the UCC implied warranties may be difficult to interpret in a technology contract, so it is best to include appropriate express warranties. Promises to perform certain obligations should also be included (sometimes referred to as covenants).

Ideally the vendor would warrant that the technology would operate in accordance with:

1. The proposal and other materials that were the basis of the customer's decision;
2. Documentation from the vendor which the customer has had the opportunity to review in advance;
3. Any oral statements made by the vendor and features demonstrated (all of which should be put in writing); and
4. The assumptions upon which the customer is relying (the customer must identify its own assumptions).

Although the following are certainly not every warranty and covenant that should be negotiated, these should help reduce the risk of patient safety issues:

- Accuracy and integrity of data (for example, that the data retrieved from the system is identical to the data stored by the customer);
- Accuracy of any computations made using the software (for example, a failure to convert the patient's weight from pounds to kilograms [3];
- Functionality of clinical decision support embedded in the technology;
- Ability to adjust alerts in order to minimize "alert fatigue" [4];
- The vendor's ongoing efforts to receive and address reports of safety issues from its customers and that such information will be made available to all customers [5];
- Details of back up and disaster recovery services provided by vendor;
- An "uptime" guarantee if the software or service is provided on the vendor's hardware (for example, in a "Software as a Service" arrangement or technology provided "in the cloud");
- Support response times depending on severity of problem with financial consequences for failure to meet stated response times (typically credits against future charges);
- Interfaces to other software and the obligation to revise the vendor's technology;

- No litigation or other disputes concerning quality, operation, patent infringement or other intellectual property issues.

Another point to consider is that many types of HIT require the use of software or services developed by third parties that are sold as part of one vendor's bundled product. Even though the vendor has selected the third party technology, the vendor's standard contract often will state that the vendor is not responsible for the third party services or software. Customers should try to negotiate to have the vendor (or the third party) be responsible for this technology.

Term of Support and Transition Services After Termination

One of the first questions to ask regarding support is whether the vendor has committed to support the product for a period at least as long as the customer expects to use it. If not, the customer may face the operational and financial risks of transition to different technology sooner than it would like. The customer may need to negotiate a longer term than is initially offered by the vendor. Knowing how long the software will be supported or the service will be provided is an important element in vendor selection.

For example, even if the technology contract grants a "perpetual" license to use the software, the related maintenance agreement usually limits the time during which support will be provided for a particular version of the software. The time period for support effectively limits how long most customers will use the technology because a customer will not continue to use it if the vendor no longer answers questions, fixes bugs or provides enhancements for the software to comply with new regulations. At that point, most customers will want to upgrade to a new version or find another vendor, often at additional cost.

Sometimes the technology is provided as a service without a license (often referred to as "Software as a Service" or "in the cloud"). The service agreement will be for a definite time period, sometimes with renewal periods, but the vendor typically will not be obligated to renew unless this point is negotiated.

The customer should be aware of the risk that the vendor will elect not to renew support because it wants to shift customers to a new version (possibly for an additional fee). This may also occur if the vendor is acquired and the new owner wants to shift the vendor's customers to the new owner's product.

Moreover, at some point the customer will want to change technology, which will often require assistance from the initial vendor. This will be much easier if a contract provision was negotiated in advance requiring the current vendor to assist with transition to a new vendor. This would typically include an agreement to continue to provide standard services (at the customer's request) during a transition period in case the contract terminates abruptly for any reason.

Ideally the transition period would provide the customer enough time to select and implement replacement technology. The vendor should also be obligated to

cooperate with the new vendor, generally assist the customer with transition, and return the customer's data (and patient data) in an industry standard format that does not require the use of the vendor's software. The customer should expect to pay the vendor's standard charges for this continued support and assistance, but transition services are important to avoid a gap in service which could present serious risks to patient safety.

Understanding Backup and Possible Exclusion of Damages for "Lost Data"

Many technology contracts are silent on the frequency of data backup, exactly what data will be backed up, which party is to perform it and how long it will take to restore in the event that the primary source of information is lost. This is especially important in a "cloud" or "Software as a Service" arrangement where the customer is much less likely to be able to perform backup itself.

There are obvious safety risks to patients whose data is unavailable. It is therefore critical to understand what the vendor and the customer are each required to do in order to have patient information available from backup quickly in the event of a problem with the system. This usually requires input from technical personnel of both parties as well as legal assistance to clearly document each party's obligations in the agreement.

The contract should also be carefully reviewed to determine if the vendor has disclaimed responsibility for lost data. This often is found in a provision that excludes "consequential damages" and may read as follows (emphasis added):

> *EXCLUSION OF CONSEQUENTIAL DAMAGES. UNDER NO CIRCUMSTANCES WILL VENDOR BE LIABLE FOR ANY INCIDENTAL, SPECIAL, EXEMPLARY, CONSEQUENTIAL OR OTHER INDIRECT DAMAGES ARISING UNDER OR RELATING TO THIS AGREEMENT OR TO ANY SERVICES, SOFTWARE, OR OTHER MATERIALS PROVIDED BY VENDOR TO CUSTOMER, INCLUDING, WITHOUT LIMITATION, LOST DATA, LOST PROFITS OR THE FAILURE TO ACHIEVE ANTICIPATED SAVINGS, WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY HEREIN.*

A discussion of the various types of damages should involve knowledgeable legal counsel, so the following is provided only as background for that discussion:

- "Direct" damages usually are not excluded although they may be limited to a specific dollar amount. A claim for direct damages typically would involve an assessment of what additional costs the customer incurred *as a direct result* of the vendor's breach—for example, did the customer need to obtain additional software or equipment?
- "Consequential" damages often include lost profits, damage to reputation (goodwill) or other types of harm that flow *as a consequence* of the breach. Consequential damages are often excluded but the scope of the exclusion should be negotiated.

- Vendors often want to disclaim responsibility for "lost data." A court might not agree that "lost data" is a type of consequential damage, so vendors may try to specifically exclude this type of damage in their standard contracts in the consequential damages clause. However a loss of data is often very serious and reducing the risk of data loss may be one of the main reasons why the customer selected the vendor's cloud or Software as a Service offering. Counsel for customers usually resist excluding damages for lost data unless the customer has agreed to full responsibility for data backup.

More generally, counsel for customers often negotiate to have certain types of claims excluded from *any* limitations of the vendor's liability. Examples include:

1. Claims subject to indemnification;
2. Personal injury (including death) and property damage;
3. Breach of confidentiality and breaches of a vendor's business associate obligations under HIPAA; and
4. Damages arising from the other party's negligence or willful misconduct.

Not all of these types of exclusions directly impact patient safety, so they are beyond the scope of this chapter. However, they should be the subject of discussion between the customer and its attorney.

Indemnification

"Indemnification" or "hold harmless" are general terms for one party's promise to reimburse or "make whole" the other party for certain types of claims. Indemnification is often used in technology contracts to cover claims that a **third party** who has not signed the contract (such as a patient) may bring against the vendor or the customer.

These third parties do not have the right to sue under the contract itself because they are not parties to it. However, they may have the right to sue the vendor and/or the health care provider (customer) for negligence or other claims that arise in connection with the technology itself and/or how it was used by the customer.

Although the results of indemnification are primarily financial, some customers believe that if the vendor is able to shift responsibility to the customer for the vendor's errors by using indemnification provisions, the vendor will be less likely to address safety issues. Customers may also feel that such broad indemnification does not allocate risk in a fair or equitable manner. As a result, customers often resist indemnifying the vendor for patient claims arising from technology errors. Instead they prefer an approach that makes each party responsible for its own acts, omissions, and negligence. However, vendors often strenuously resist changing their standard language, arguing that it is too difficult to determine how various factors in patient care resulted in a bad outcome for the patient so the customer should be solely responsible.

An example of this type of indemnity provision is set forth below. The last paragraph illustrates one negotiated approach to achieving a somewhat more balanced allocation of responsibility for errors that resulted solely from the vendor's technology.

> Customer agrees to defend, indemnify and hold harmless Vendor and its employees, officers, directors or contractors (collectively, "Vendor Indemnitees") from any claim by or on behalf of any patient of Customer, which is brought against any Vendor Indemnitee regardless of the cause (except as provided below) if such claim arises for any reason whatsoever out of the operation of the EHR Software licensed to Customer under this Agreement.
>
> To the extent applicable, Customer will obtain Vendor's prior written consent to any settlement or judgment in which Customer agrees to any finding of fault of Vendor or defect in the EHR Software or Vendor's services.
>
> Notwithstanding the foregoing, the indemnification obligation under this Section shall not apply if all of the following conditions are satisfied: (1) the proximate and direct cause of the event giving rise to the claim for indemnification is Vendor's sole negligence with respect to an error in the EHR Software, (2) Customer has used the EHR Software only in accordance with the documentation manuals and (3) Customer has given prompt notice to the Vendor of any and all possible problems with the EHR Software and satisfied all of Customer's other responsibilities under this Agreement.

However, customers may feel the exception in the last paragraph above does not protect the customer enough because it leaves the customer responsible for claims in which both the vendor and the customer were at fault.

It should be noted that the Board of Directors of the American Medical Informatics Association (AMIA) adopted various task force findings as an AMIA Position Statement. One of the findings with respect to contract language was that:

> "Hold Harmless" clauses in contracts between Electronic Health Application vendors and purchasers or clinical users, if and when they absolve the vendors of responsibility for errors or defects in their software, are unethical. Some of these clauses have stated in the past that HIT vendors are not responsible for errors or defects, even after the vendors have been informed of problems [6].

It is also critical for the customer to consult with its insurance broker regarding the possible impact of indemnification on customer's insurance coverage. Under some insurance policies, if the insured party (the customer) agrees to indemnify the vendor for certain acts or accepts liability that otherwise would be the vendor's responsibility under applicable law, the customer's insurance carrier may deny coverage for this "assumed" contractual liability. This would leave the provider without insurance coverage for the amounts it might have to pay the vendor under the indemnification clause. The advice of a knowledgeable insurance broker as well as legal counsel should be helpful in addressing questions of coverage.

Confidentiality and Non-disclosure Agreements (NDAs)

Most technology vendors regard the intellectual property in their software and services as a "crown jewel" because it is their main asset. This results in very strong contractual protection of the vendor's intellectual property. A vendor may also include contract language regarding non-disclosure because state laws providing

trade secret protection require such contractual provisions. A vendor's intellectual property protections may also include copyright and patent rights which are beyond the scope of this chapter.

Vendor contracts typically define confidential information very broadly to include almost everything the vendor discloses or provides to the customer, regardless of whether it is marked as confidential. The vendor's standard agreement protects its confidential information with restrictions on disclosure and serious consequences for a customer's breach. For example, a customer's breach of the confidentiality provisions may give the vendor the right to terminate the agreement for breach without a cure period. Even if there was a cure period, a violation of confidentiality provisions may be almost impossible to cure because the information cannot effectively be recalled.

The vendor's natural desire to protect its intellectual property rights may, if asserted too broadly, conflict with the customer's desire to share information about the technology to reduce patient safety risks or to report perceived errors. For example, an expansive definition of confidential information may limit the customer's ability to grant access to the vendor's software or services in order to compare different technology systems, provide access to consultants or researchers, or address possible patient safety concerns. The customer should therefore review the confidentiality and non-disclosure language carefully to make certain it does not unduly limit the customer's ability to conduct activities it would like to pursue.

There are certain common exceptions to the vendor contract provisions that prohibit the customer from disclosing the vendor's confidential information. They include the following:

- Disclosure of information that is available to the general public or has been provided separately to the customer without violation of an agreement;
- Disclosures required by law or regulation, sometimes with an obligation to give the vendor advance notice and the opportunity to oppose the disclosure or seek confidential treatment; and
- Disclosure of information that has been independently developed by the customer.

If the standard exception for disclosures required by law is included, the customer could report a technology problem or safety issue including disclosures of confidential information if the disclosure is required by law. However, such disclosures generally are not required by law so the customer may want to negotiate to have the ability to make voluntary disclosures of such problems and safety issues even if they include some "confidential information" such as screenshots or the vendor's user manuals.

Reporting adverse events is increasingly viewed as key to patient safety, so some vendors encourage such reporting and enable it using their software. Indeed some authors have noted that although the "enforced non-sharing of software problems is an industry norm, it is anathema to improving care, to HIT and to evidenced-based medicine [7]." A vendor's position on this point therefore could be an important factor in vendor selection.

From the opposite perspective, it should be noted that customers often have information other than patient information that the customer would like to prohibit the vendor from disclosing or using for any purpose other than supporting the customer's technology. Such information may include proprietary information about the customer's business such as quality metrics, managed care contracts, and marketing information. If the contract does not protect the customer's confidential information, the customer may want to consider requesting that the confidentiality provisions be made mutual.

Conclusion

As noted in a review of the literature on safety issues related to electronic medical records (EMR) from 2000 to 2009:

> The pressure on hospitals to implement EMR has never been greater. A large part of the driving force relates to demonstrated and presumed improvements to patient safety. The findings of this review reveal … unintended consequences of EMR deployment that must be considered ….The role of health care leaders in the safety of EMR cannot be understated [8].

There are several purposes of technology contract review and negotiation that may improve patient safety:

- To first understand exactly what the vendor is and is not committing to provide and how risks are allocated. Vendor contracts are complicated with numerous exhibits and legalistic language, much of which has been crafted over time to best protect the vendor. The vendor is very familiar with the contract, but the document and the process of negotiation is an infrequent event for the customer.
- To make sure that there are express warranties in the contract that adequately commit the vendor to provide what the customer expects. It is also critical that the customer understands its own assumptions and whether the vendor is able to satisfy them. If there are gaps discovered in this process but the customer still wishes to use the technology, the customer will have the opportunity to reduce the risks with additional resources or procedures.
- To provide for a more equitable allocation of risk that does not remove the vendor's incentive to provide a safe product. For example, vendor contracts often require the customer to indemnify the vendor for all claims arising from use of the software or service regardless of whether the claim arose in part from problems with the vendor's technology. This may be unreasonable from the customer perspective and indicate an unwillingness of the vendor to stand behind its product as much as the customer expects.
- To provide for a sufficient transition period at the end of the contract and transition services to assist in moving to new technology.

- To allow disclosures of a limited amount of the vendor's intellectual property (such as screenshots) if necessary to voluntarily report patient safety risks to patient safety organizations and researchers if desired by the customer.
- To determine whether the vendor collects data about errors and makes it available to all of its customers in order to reduce patient safety risks.

In order to effectively address these points each party should understand the key issues and negotiate an acceptable allocation of risk for the particular issue and the overall transaction. In crafting a solution it may be helpful to use one of the fundamental principles of contract risk allocation—that the more control a party has over the factors giving rise to a particular risk, the more responsibility the party should have for liability that may result if that particular risk results in damages to the other party.

While contract review and negotiation may be time-consuming and challenging, the resulting benefits to patient safety and the customer's confidence in the technology should make it well worth the effort.

References

1. Joint Commission Sentinel Event Alert 42. Available at http://www.jointcommission.org/sentinel_event_alert_issue_42_safely_implementing_health_information_and_converging_technologies/. Joint Commission Sentinel Event Alert 54. Available at http://www.jointcommission.org/sea_issue54/. Accessed 13 June 2016.
2. SAFER guides. Available at https://www.healthit.gov/safer/safer-guides. Accessed 3 July 2016.
3. Sittig DF, Singh S. Defining health information technology-related errors. Arch Intern Med. 2011;171(14):1281–4.
4. Sittig DF, Campbell E, Guappone K, Dykstra R, Ash JS. Recommendations for monitoring and evaluation of in-patient computer-based provider order entry systems: results of a delphi survey. AMIA 2007 Symposium Proceedings. p. 671–675.
5. The Electronic Health Record (EHR) Association has published the EHR Developer Code of Conduct in support of patient safety and other issues. Its principles include notice to customers if software issues are identified that could materially affect patient safety. See http://www.himss-ehra.org/ASP/codeofconduct.asp. Accessed 3 July 2016. If the vendor in question has adopted the Code of Conduct, it may be more willing to negotiate access to information about errors and other points.
6. Goodman KW, Berner ES, Dente MA, Kaplan B, Koppel R, Rucker D, 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 Med Inform Assoc. 2011;18:77–81.
7. Koppel R, Kreda D. Health care information technology vendors' "hold harmless" clause: implications for patients and clinicians. JAMA. 2009;301:1276–8.
8. Harrington L. Safety issues related to the electronic medical record (EMR): synthesis of the literature from the last decade, 2000–2009. J Healthc Manag. 2011;56(1):31–44.

Chapter 19
Improving Safety of Medical Device Use Through Training

Peter A. Doyle

Introduction

This chapter addresses Information Technology (IT) embedded in medical devices as opposed to Health Information Technology (HIT). HIT is defined as "hardware or software that is used to electronically create, maintain, analyze, store, or receive information to aid in the diagnosis, cure, mitigation, treatment, or prevention of disease and that is not an integral part of (1) an implantable device or (2) an item of medical equipment" [1]. While such products are receiving attention in other chapters in this book, one cannot deny that risks associated with software-driven technologies are not constrained to Electronic Health Records (EHR), Provider Order Entry (POE) and similar systems. Many medical devices for diagnosis, treatment and monitoring of medical conditions use software-driven control systems for hardware such as pumps, ventilators, anesthesia machines, and defibrillators. In contrast to IT systems that handle information only, these software-driven medical devices produce physical outputs in the form of gases, fluids, electrical energy, and heat that can directly affect patients. As such, these devices are subject to the similar types of errors as found with EHRs (e.g., failures of attention or memory, rule-based error or in the case of poor design coupled with poor training, nescient errors) [2] and the result may impact the patient directly.

The increase in numbers and complexity of medical devices is driven in part by the introduction of software to control the functions in devices we use for surgery, for inpatients and for home-care applications. The often broad and deep menus designed to enable increased device functionality make it difficult to establish equipment competencies for safe and successful use due to device complexity. Mastering the many control options and maintaining awareness of device status

P.A. Doyle, Ph.D. (✉)
Clinical Engineering Services, The Johns Hopkins Hospital,
600 N. Wolfe St, Baltimore, MD 21287, USA
e-mail: pdoyle6@jhmi.edu

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4_19

through the use of complex displays can present challenges. Such challenges are further exacerbated by the frequent introduction of new devices and by the rapid rate of upgrades and software revisions that require continuous learning. As an indication of the increase in the number of medical devices in use, in a recent 4-year period the number of device *makes and models* in the Johns Hopkins clinical engineering database increased by 23 %.

Furthermore, multiple users with different roles during the setup and use phases require close coordination of activities to ensure proper use. Surgery technicians and nurses must learn proper equipment setup and how to conduct preuse checks to assure all functions are operational and properly set. If not, the user may be deceived into thinking the device is prepared for safe use when in fact it is not. This situation is further complicated when we consider that during breaks, handoffs and change of shifts, clinicians and support staff new to the case or patient assume control of devices already in specific states of use. All of these factors present challenges to users and support staff in keeping pace with new learning requirements to achieve and maintain mastery of tools used in life-critical situations. In addition to the possibility of patient harm, improper tool use can cause prolonged or aborted surgeries. Other concerns include unnecessary loss of costly disposable tools thought to be defective and expenses related to unnecessary equipment investigations when users attributed use error failures to equipment failure.

Much of the technology we have today originated in the military, aviation, and space industries—other high reliability organizations with critical missions. After encountering the challenges technology places on users, these industries established an order of precedence for controls to mitigate risks. Eliminating hazards by design, use of safety devices, and use of warning devices all precede training as priorities for risk mitigation [3]. The health care system has adopted a similar approach as shown in Table 19.1 [4]. When devices are not designed with the order of precedence for safety in mind, when usability in general is poor or operation is unduly complex, we must compensate for such misgivings with training—the least effective means of ensuring safety. So the need for better training materials and subsequent skill validation becomes vital. The burden is placed on the user to avoid operational pitfalls by mastering and remembering complex operational procedures. In these cases the traditional, rather quick "see one, do one, teach one" approach to training, and the short in-service, so deeply embedded in health care education do not always serve well in preparing users for safe outcomes. To protect the safety of patients and its own interests, the institution in turn assumes the burden of providing adequate training to overcome the risk of using complex, software-driven devices.

Table 19.1 Priorities for risk control options

Priority	Means to reduce risk
1	Inherent safety by design (forcing functions)
2	Protective measures in the medical device itself (such as guards or barriers)
3	Information for safety (e.g., warnings, cautions, procedures, and training)

Source Adapted from ANSI/AAMI/ISO 14971:2007

During the course of incident evaluations, examinations of product failures (real or imagined) and during development activities with the goal of integrating medical equipment, the author has learned that some software-based products require more or better training than originally envisioned. This is due to all of the challenges cited above. Furthermore, there are opportunities to improve the quality of Instructions for Use (IFUs) provided by vendors, especially since these may be used as tools to develop training or support later use. Relying on the vendor alone to determine training content, delivery methods and competency assessment criteria may invite risk to your organization. In our institution we are in the process of assessing how the value of device training affects risk. This chapter identifies examples of design shortcomings that, once the procured product is in hand, can only be addressed by training. Approaches to improve training outcome are then offered.

Case Studies

Smart Infusion Pump

Using a smart infusion pump, a nurse intended to program an infusion with a delayed start and a "callback" alarm to indicate the infusion had completed. Once the infusion had completed the pump did not produce a callback alarm. An engineering investigation showed that the pump was functioning normally. A review of the pump's log file showed that the user selected the delay option feature, setting the delay for 22 min then 120 min without setting the callback function to "after." This left the pump's callback feature in the default setting, which is "none" because the delay option does not automatically set an audible callback alarm after a delayed infusion is complete. The investigator recommended additional hospital-wide training regarding use of the delay function and callback alarm.

PCA Pump

The use of drug libraries in smart pumps helps assure proper dosing. However, the means for selecting the proper menu item from the library must take into account the possibility of use errors. One such error is neglecting to scroll down to a new screen in a list of drug concentrations and selecting a concentration that only appears to be the intended target. Another is failing to follow the proper sequence in changing drug concentration per a new order during an extant infusion, as one might do for pain medication. Changing concentration for a new order requires closely comparing the new order to the medication label then changing the program for the new concentration. This requires starting a new infusion for the patient. If this is not done the former concentration will remain in effect.

To perform this change successfully one must verify the Therapy (route), Qualifier (Standard or High), Drug, and Concentration. One pump provides an

opportunity to review and confirm these settings in a one-time, confirm all, manner. Experience has shown that doing so has led to confirmation when the concentration remained at the previous setting. This could prove harmful depending on the dose or rate in use. A preferred design approach would be to require confirmation of each separate infusion parameter, an apparently simple solution to encourage safe use. To address instances of improper concentration we found it necessary to develop and deliver training in the form of a PowerPoint presentation instructing users to:

- Start a new protocol for the same patient
- Program the pump per the new infusion order
- Change the drug, concentration, rate, dose, max doses/h
- Verify the pump and order through comparison of the order, drug label, and pump display
- Have a second RN verify the programming per the steps above

This training aid, which we developed to support the training provided by vendors, supports nurses in successfully performing requirements for a menu-driven task sequence.

Physiological Monitor

The menus to configure physiological monitors for desired settings can be deep and confusing to both nurses in their clinical work and to biotech staff when they change defaults or set up other parameters. Such interfaces make it difficult for technicians and users to form a mental model of the control system hierarchy and to transition through modes to perform discrete actions such as those to control alarm volume levels.

We decided to conduct a Failure Modes and Effects Analysis (FMEA) to learn how physiological alarms could be intentionally or inadvertently silenced, possibly resulting in a missed alarms and subsequently undesired outcomes for patients. In examining the possible failure modes in one model of monitor we learned that due to the complexity of monitor menus and controls, and the many steps required to maintain safety, there are multiple ways in which one might inadvertently turn alarms off. A sample of failure modes is described below as an indication of interface complexity and the need for training as a means to avert incidents.

1. A bedside monitor can be set so a high level alarm can break through the silence of a paused alarm. If the default for this feature is “off,” it would prevent high level alarms from sounding when alarms are paused, inducing risk of overlooking alarms and possibly injury or death. This default is set in service mode and requires biomedical technicians to coordinate with nursing to determine the preferred setting, and users need to be aware of the default status.
2. Failure to discharge a patient and subsequently admit the next patient with the former patient’s alarm settings will carry over the alarm volume setting from the

initial patient. The volume setting will stay at the set value until discharge at which point it will return to the default volume level.
3. Silencing a patient's alarm at a central monitor also silences all *active* patient alarms simultaneously for one minute at both the central monitor and all bedsides in the unit.
4. In the Alarm Control Menu, after staff selects a volume level on a monitor, failure to confirm the new setting by selecting the "Alarm Vol." option will result in a return to the previous volume setting. As a result the volume could be too low and result in an overlooked alarm.
5. If the menu option for "Display Off Alarm Pause" is selected the display becomes blank and the monitor stays in alarm pause indefinitely.
6. Should someone push silence at the central monitor to silence an alarm, and someone else pushes silence at the bedside within a very short interval, the 2nd push unintentionally puts the alarm in pause. Alarms for that bed are then defeated for 3 or 5 min. Training should include the importance of verifying the status of the alarm silence/pause function on the display when silence switch is pushed.

Among other preventive measures instituted to prevent these failure modes, training was recommended as a risk mitigation measure to ensure competency, responsiveness, and related safety.

Solutions

Enabling training activities and verifying user competency on the multitude of device types encountered taxes the resources of health care organizations. This section addresses some practical solutions that can be taken to improve the likelihood of safe device use.

Select Wisely

Ideally your organization is making a worthy effort to select and purchase safe and effective medical technology. Selecting devices designed for safe use is the best way to reduce risk and institutional expenses related to staff effort. This requires coordination between different professional roles in your organization such as purchasing, risk management, clinical users of the device in question, clinical engineering, and others. Some criteria to help assure you are making wise choices are provided in Table 19.2 [5]. One can review the device manual to gauge complexity of use. Keep in mind that devices loaded with every conceivable feature may invite errors due to their difficulty in use. You may also find it helpful to evaluate the training material to see if it sufficiently addresses the warning, cautions and tasks for use.

Table 19.2 Selecting and purchasing medical equipment

1. Determine if the device has undergone usability testing per FDA Guidance
2. Thoroughly evaluate the device in trials with your clinicians in the actual use environment
3. Consult the Software User Interface standards in Chapter 21 of ANSI/AAMI HE 75:2009
4. Ask specific question to determine whether the command input process and output sequences are well-designed. Does the device:
(a) Offer the actions I wish to initiate?
(b) Understand my instructions?
(c) Deny inappropriate inputs?
(d) Offer clear opportunities to change inputs?
(e) Provide ready access to needed status information?
(f) Provide proper cues for subsequent commands?
(g) Do all this in a manner that is safe and easy to use?

Source Adapted from Doyle, P. AAMI Horizons, Fall 2013

We know that when operation of equipment is intuitive, and when the command and control mechanisms have good affordance, i.e., are perceived directly [6], devices are more likely to be used as intended. To encourage this property in medical devices the FDA has provided guidance for the application of human factors and usability engineering to optimize medical device design [7]. One expects that usable devices require less training. Therefore, selection of software-driven devices that have undergone development and testing per the FDA's guidance should provide less challenge with respect to training.

If there is no evidence of human factors and usability engineering in the development of a product, you can conduct your own usability comparison of product alternatives. We did this at The Johns Hopkins Hospital with three models of infusion pumps by developing use scenarios and evaluating pump features in simulated medication administrations. This enabled us to choose the pump with the most favorable and safest control features.

In addition to the methods above you can research FDA's MAUDE database [8] and ECRI Institute's resources [9] to learn about device characteristics. Purchasing decisions can then be made with these and other factors in mind.

Develop Training to Supplement That Provided by the Vendor

The vendor's objectives and motivation to develop and provide training to your institution may differ somewhat from your own. For instance, sales representatives have no desire to present their product in a poor light and may "overlook" certain device characteristics during demonstration and instruction. Developing comprehensive training can be costly, and vendors may have an interest in supporting the product in use rather than training your staff. In a short unpublished informal survey with nine hospitals responding, we learned that two of the hospitals (22 %) relied on vendors only to provide physician training. In these two cases the institution is relying on vendor training quality and assuming the risk of any training oversight.

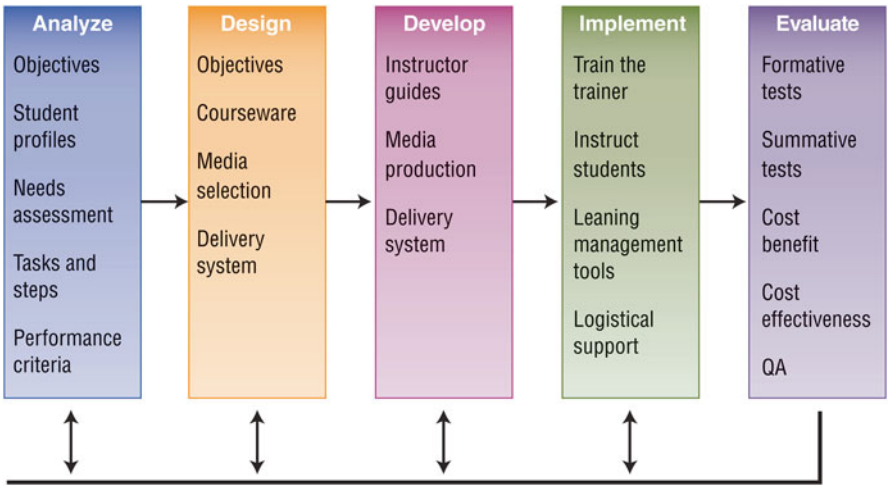


Fig. 19.1 Instructional systems development model

Considering that four (44 %) of respondents rated the vendor training very adequate and four (44 %) rated it very inadequate, it seems advisable in many instances that institutions should supplement vendor training or take other measures to assure adequate training.

The ADDIE training development model (short for Analyze, Design, Develop, Implement, and Evaluate) provides guidance for the successful development and implementation of training [10]. It is based on the systems approach to training developed in the 1970s by the military [11] and variations are used ubiquitously in both commerce and the military [12]. In this approach tasks are analyzed, training is designed, instructional materials developed, then training is implemented, evaluated, and revised [12]. As represented in Fig. 19.1, it is a thorough systems approach to training development and validation. Use of this comprehensive model is not detailed here, but familiarization with the process can provide guidance on steps useful for improving training in health care settings.

When limitations preclude conduct of a detailed ADDIE training development program, an analysis of the tasks can help prepare you to assure the necessary training content in is included in training sessions. At the very least you can review both operators and service manuals and make sure users and those who service software-driven equipment are knowledgeable of all device capabilities and how features should be invoked for use. One way to do this is to make a list of the tasks required to perform the device functions along with the cautions and warnings. Then make sure that all information pertinent to safe use is included in the training. We found that doing this helps identify the steps and their proper sequence to encourage proper use of hypo/hyperthermia machines. Vendor material such as IFUs and task analysis, data from usability, or FDA validation studies are other sources for developing training content.

If a detailed analysis of tasks is not a feasible undertaking for your institution, one means to identify the areas requiring development of training is to develop an analysis of the functions performed by the device users. In one case at Hopkins a nurse educator and a human factors engineer documented an analysis of the physiological monitoring training requirements in the form of a nine module curriculum. The challenges of fully developing all nine modules and the practicality of providing it to more than 3000 nurses curtailed our ability to proceed in an idealized manner. However, by developing the nine module curriculum, we had a basis for identifying additional knowledge and specific skills that should to be addressed. Performing a Failure Modes and Effects Analysis (FMEA) or other forms of risk analysis can also help identify necessary training content. Using an FMEA approach we identified multiple ways in which one can inadvertently turn off the alarm volume of physiological monitors when manipulating the complex menu structure. This led directly to recommendations to avert such risks. At the very least, conducting a simple walk-through or demonstration of all the features and functions with a critical eye for hazards can be enlightening.

Determine What Needs to Be Trained

Once you have a good grasp of the tasks, determine which tasks need to be trained, Fig. 19.2 provides a good model for determining training needs based on task difficulty, criticality, and frequency [11]. As indicated in the figure, these three dimensions are used to determine if a task should be trained at all and if trained, should it be overtrained to ensure sustainability.

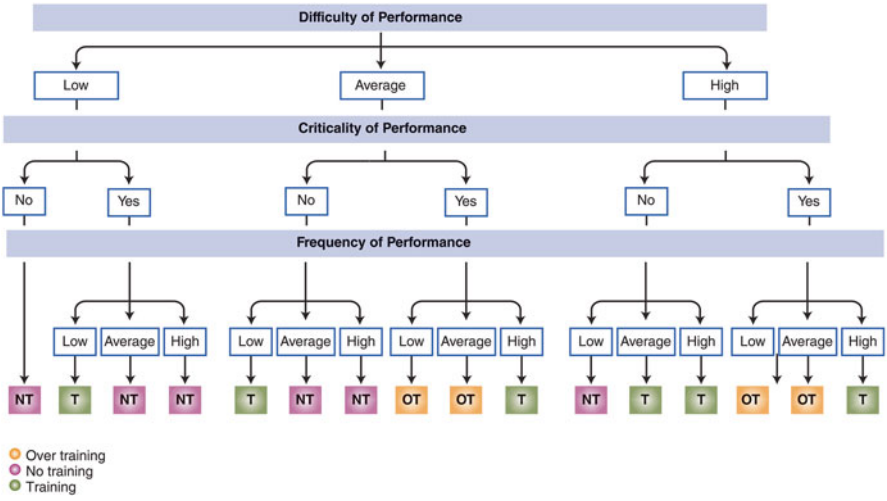


Fig. 19.2 What to train (Source Mil-Hdbk-1379-2)

Standardize Training

An important aspect of developing your training is to ensure that each trainer from the vendor and the institution is working from a single set of approved training materials for each device. Otherwise irregularities in the materials will result in variability in how software-driven devices are used, perhaps resulting in risky behaviors. For example, IFUs of infusion pumps may be contained not only in your policy and procedures documents but they may also be supplemented in operating manuals, videos, other vendor materials, fast facts sheets, hang tags, and other job aids. Perhaps no one source provides a comprehensive set of instruction, forcing the trainers and users to research all sources—if they are even aware of them. This can result in nonstandardized use, a situation that can be moderated by collating material to a primary source and standardizing associated training.

Obtain Assistance from External Resources

One approach to solving training challenges is to collaborate with institutions with degree programs in education or instructional systems development. Graduate students may be yearning for a project to complete their degree and a chance to gain entry into the workplace. This strategy afforded us opportunities to improve our endoscope cleaning process. A student performed a task analysis and video documented the required activities. This assisted in development of an improved cleaning procedure, replete with instructions at the subtask level and the required warnings and cautions. Once you demonstrate the value of this approach you may find an opportunity to acquire a valuable asset to your staff.

Embedded Training

A possible training option is to take advantage of embedded training in devices that present task simulations in a walk-through, wizard-like fashion. This enables initial and refresher training on flexible schedules with far less demand on training personnel. Only if health care organizations demand such higher levels of training experiences will embedded training become more of a reality.

Assess Competency

A requirement for each trainee to demonstrate skill competency on tasks critical to safety improves the value of the training experience. Competency assessment should be addressed at the technical, interpersonal, and organizational levels [13].

Wright observes that the technical aspect should include competencies that matter, and that the right competency verification methods be used. This reflects the guidance in the Systems Approach to Training and ADDIE models [10–12]. Assessment steps include analyses to determine the tasks or steps to be evaluated, the use of proper media for training, the selection of criteria (objective standards) for showing mastery and the use of appropriate methods for verification. Verification could include tests of knowledge but with complex technology a skill demonstration for specific tasks is more likely appropriate. The Joint Commission adds, "Use of a self assessment, such as a skills checklist as the sole assessment method, does not constitute a competency assessment" [14]. Critical thinking, interpersonal and communication skills are examples of skills needed to round out the competent employee [13]. Of course observing basic use of equipment from a distance in a short in-service does not substitute for competency assessment. Nor does it ensure that staff is prepared to use equipment safely.

Discussion

Vendor Supplied Training

The model used by health care organizations to acquire equipment training often contrasts with the model used by other high-reliability enterprises such as national defense and nuclear power generation. In those cases training is more often purchased as a separate line item from the vendor. This enables the organization to closely specify and evaluate the value of the training provided. In contrast, for hospital training the vendor often independently determines the content, presentation media and duration of training in a manner that controls their costs. As a result training may be conducted as brief "See one, do one" exercises, hardly the ideal method in many cases. In addition to this situation the value of the training presented is subject to difficulties in reaching all staff and maintaining attention in short sessions between surgeries or clinical duties. It may encourage, in some situations, a feeling that the in-service prepares the user for all contingencies, while the operator's manual, with its many warning and cautions, is stored on a shelf or saved in a crowded computer folder.

New Forms of Training Delivery

As we know, developments in computer-based training have afforded excellent opportunities to deliver knowledge-based training and skill-based training in cases where appropriate levels of simulation fidelity are used. Vendors do offer video instruction tools and instructional material hosted on computer tablets. Portable tablets show promise as a resource for training, maintaining proficiency and use as job

aids as a "just in time" approach. Another helpful form of simulation would be the use of embedded software for training. This approach uses simulation training software that is embedded in functional equipment. The author is aware of use of embedded training in one hospital bed product and one might surmise it would be useful in other devices such as infusion pumps and ventilators.

Key Lessons Learned

In summary, it should be recognized that many medical devices have software-driven control features that may contribute to use errors. With this in mind the following points are offered as key lessons.

- Due to the complexity of some software-driven devices, a user's mental concept of the device's status may deviate from its actual status, resulting in risk.
- At times, to control risk for medical equipment with poor software-based design, we must compensate with training.
- The "quick in-service" is not always the best means for training software-driven medical devices.
- Adequate guidance for developing training content, delivering training and assessing competency is plentiful in the literature.
- Hands-on learning and practice experiences suitable for demonstrating competency are needed to address all contingencies of use.

References

1. PSO Privacy Protection Center [Internet]. Available from: https://www.psoppc.org/c/document_library/get_file?uuid=75912503-7bd1-4e99-a678-5dbb70008e95&groupId=10218. Accessed 23 Dec 2014.
2. Medical Devices—Application of usability engineering to medical devices, AAMI/IEC 62366:2007, International Electrotechnical Commission.
3. United States. Department of Defense. Standard practice for system safety, MIL-STD-882D, 2000.
4. Medical Devices—Application of risk management to medical devices, ANSI/AAMI/ISO 14971:2007.
5. A roundtable discussion, understanding medical devices and users in context, AAMI Horizons, Fall 2013.
6. Greeno JG. Gibson's Affordances. Psychol Rev. 1994;101(2):336–42.
7. The Federal Food and Drug Administration [Internet]. Available from: http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddevgen/documents/document/ucm259760.pdf Accessed 25 April 2016.
8. The Federal Drug Administration, MAUDE Database [Internet]. Available from: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm. Accessed 23 Dec 2014.
9. ECRI Institute [Internet] Plymouth Meeting, PA. https://www.ecri.org/Pages/default.aspx. Accessed cited 23 Dec 2014.
10. Clark D. The ADDIE model, instructional system design: a handbook for practitioners [Internet]. Available from: http://www.nwlink.com/~donclark/hrd/sat.html. Accessed 23 Dec 2014.

11. United States. Department of Defense. Instructional systems development/systems approach to training and education, DoD Handbook, (Part 2 of 5 Parts), MIL-HDBK-29612-2A, 2001.
12. United States. Department of the Army. Interservice procedures for instructional systems development model (ISD). TRADOC Regulation (Pamphlet 350-30), 1975.
13. Wright D. The ultimate guide to competency assessment in healthcare. 3rd ed. Minneapolis, MN: Creative Healthcare Management Inc.; 2005.
14. The Joint Commission: Standards FAQ Details [Internet]. Available from: http://www.jointcommission.org/standards_information/jcfaqdetails.aspx?StandardsFaqId=31&ProgramId=47. Accessed 23 Dec 2014.

Index

A. Agrawal (ed.), *Safety of Health IT*, DOI 10.1007/978-3-319-31123-4