Evidence-Based Health Informatics
E. Ammenwerth and M. Rigby (Eds.)

doi:10.3233/978-1-61499-635-4-25

Health IT for Patient Safety and Improving the Safety of Health IT

Farah MAGRABI[a1], Mei-Sing ONG[a,b] and Enrico COIERA[a]
[a] *Centre for Health Informatics, Australian Institute of Health Innovation, Macquarie University, Sydney, Australia*
[b] *Computational Health Informatics Program, Boston Children's Hospital, Boston, MA, USA*

Abstract. Alongside their benefits health IT applications can pose new risks to patient safety. Problems with IT have been linked to many different types of clinical errors including prescribing and administration of medications; as well as wrong-patient, wrong-site errors, and delays in procedures. There is also growing concern about the risks of data breach and cyber-security. IT-related clinical errors have their origins in processes undertaken to design, build, implement and use software systems in a broader sociotechnical context. Safety can be improved with greater standardization of clinical software and by improving the quality of processes at different points in the technology life cycle, spanning design, build, implementation and use in clinical settings. Oversight processes can be set up at a regional or national level to ensure that clinical software systems meet specific standards. Certification and regulation are two mechanisms to improve oversight. In the absence of clear standards, guidelines are useful to promote safe design and implementation practices. Processes to identify and mitigate hazards can be formalised via a safety management system. Minimizing new patient safety risks is critical to realizing the benefits of IT.

Keywords. Medical informatics, patient safety, medical errors.

1. Introduction

IT systems are integral to healthcare delivery and have a tremendous potential to bring about an overall improvement to patient safety. IT broadly includes all computer software used by health professionals and patients to support care [1]. At the same time, use of IT, just like any other technology, can introduce new, often unforeseen, errors that can affect care delivery and can lead to patient harm. It is now widely recognized that problems with IT and their use can pose risks to patient safety.

The objective of this contribution is to provide a motivation for evidence-based health informatics to improve patient safety, and to minimise the risks of harm associated with IT. The contribution begins with a broad-based review of the impact of IT on patient safety. We then turn our attention to the current evidence about patient harms. The next section examines the underlying causes of errors associated with IT and the final section looks at the types of safety strategies that need to be applied

[1] Corresponding author: Associate Professor Dr. Farah Magrabi, Centre for Health Informatics, Australian Institute of Health Innovation Level 6, 75 Talavera Road, Macquarie University, NSW 2109, Australia, farah.magrabi@mq.edu.au.

throughout the lifecycle of an IT system to improve safety. By understanding how problems with IT 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.

2. Health IT can improve patient safety

Much of clinical care involves the gathering and synthesizing of information. In healthcare systems with increasing patient complexity and distribution of care, traditional paper-based information management is no longer adequate for supporting high patient care standards. Effective clinical decision-making requires careful assimilation of patient information from multiple fragmented sources, and the integration of vast amounts of new scientific evidence into practice. Reliable and efficient care can often only be achieved with the use of IT [2]. IT can substantially improve the safety of care by improving information collation, sharing, and access.

IT systems like electronic health records (EHR) facilitate access to patient information in a distributed manner. Using an EHR, patient information such as diagnoses, medications, and test results can be consolidated into a single system that can be accessed at any time, in different localities, and by different team members. Wireless technology coupled with portable handheld devices allows clinicians to retrieve the most up-to-date patient information while on the move. This has the potential to significantly improve information sharing across the continuum of care, enhancing patient safety and coordination of care [3].

A study that assessed the quality of diabetes care showed 51% of patients at EHR sites, as compared with 7% of patients at paper-based sites, received care for diabetes that met the recommended standards of care [4]. Following the implementation of computerized handoff system, the number of patients missed on resident rounds was reduced by half [5], and the rate of preventable adverse events was also reduced [6]. The advantage of electronically enhancing the availability of medical data was perhaps most evident during the recent storms in the US, notably Hurricane Katrina in 2005 [7], and the Joplin tornado in 2011 (Box 1) [8]. In both storms, many medical paper records were lost. Health care providers who were supported by decentralized EHR systems were able to continue the provision of care during and after the storm, while patients from paper-based sites were left stranded without adequate care.

Box 1: A Tale of Two Cities

The 2005 Hurricane Katrina

In 2005, Hurricane Katrina caused severe destruction in New Orleans. In the chaos that ensued after this disaster, displaced individuals many of whom had chronic health conditions left their medications and medical records behind. Responding clinicians were challenged by the need to care for these patients without any knowledge of their medical history. Standing in stark contrast were Veteran Affairs providers in the same city, who were able to maintain uninterrupted care supported by nationwide access to comprehensive EHR systems.

The 2011 Joplin tornado

In 2011, a devastating tornado struck Joplin, killing 134 people. A hospital in Joplin, St John's Regional Medical Center, was severely damaged, and medical paper records were lost. Three weeks before the storm, the hospital had completed its transfer to an EHR system. Six days after the tornado, the hospital staff returned to work in a new temporary mobile medical unit. Because the full patient records were available through the EHR, medical staff was able to continue deliver care and identify displaced individuals.

3. Evidence about IT-related patient harms is mounting

While IT promises to improve the provision of care, as discussed before, it is important to note the unanticipated negative consequences of such systems. The extent of patient harm associated with IT is, however, hard to quantify, due to the lack of empirical data [9]. The "hold harmless" clauses that protect software vendors from lawsuits effectively limit the freedom to publicly raise questions about software errors [10]. Thus, many problems with IT remain hidden, and unresolved. Based on error rates in other industries, the US Agency for Healthcare Research and Quality estimates that if EHRs are fully adopted, they could be linked to at least 60,000 adverse events a year [11].

While we currently cannot ascertain the actual rate of adverse events associated with IT, a growing body of evidence elucidates the pervasiveness of IT-related problems. The largest source of evidence comes from incident reports voluntarily submitted by software vendors and clinical workers to governing bodies, both at national and local levels [12-15]. The US Food and Drug Administration (FDA) maintains a medical device incident reporting system, known as the Manufacturer and User Facility Device Experience (MAUDE) database. In 2010, 260 IT-related incident reports were submitted to the database, 44 of which were linked to patient injuries, and 6 deaths were reported [13]. The Australian Incident Management System (AIMS) is yet another national initiative for the surveillance of patient safety issues. Between 2003 and 2005, 117 IT-related incidents were submitted to AIMS [12]. 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 IT-related adverse events, it is very likely that they were under-reported.

At a local level, the Pennsylvania Patient Safety Authority received 3,099 reports from Pennsylvania hospitals on EHR-related problems, between the years 2004 and 2012 [16]. More than 2,700 incidents involved near misses and 15 involved patient harm. The report showed a stark rise in the number of IT-related incidents over the years. Of the 3,099 incidents reported over an eight-year period, 1,142 were filed in 2011, more than double the number in 2010. With the increased adoption of IT incentivized by the Affordable Care Act, the problem will only worsen.

Flaws in software design and system glitches accounted for many of the reported incidents. 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 healthcare setting, could potentially cascade into serious life-threatening events.

The transition between paper-based and EHR records represents a risky period, as physicians often use both systems in tandem [16]. At Children's Hospital of Pittsburg, mortality rates increased after the implementation of an EHR system in 2002 [17]: During the 18 months following the EHR implementation, 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 systems 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 [18].

The incidence of IT-related medication errors has been explored in several other studies [19-23]. A report on 4,416 incidents submitted to the Dutch central reporting system showed that 16% of incidents were linked to IT [20]. 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 [23]. Of the 1,164 prescribing errors observed, 43% were caused by selection errors, 32% were due to failure to complete prescription task, and 21% were a result of editing errors.

Another unintended consequence arising from the digitalization of the medical records is the risk of data breach. The number of medical data breaches has increased dramatically in recent years. As of July 2012, there were 464 data breaches reported to the U.S. Department of Health and Human Services (HHS) since August 2009, involving more than 20 million patients – the most common forms of data breach were thefts, unauthorized access or disclosure, and data loss [24]. In the same year, a bi-annual survey of 250 U.S. healthcare organizations showed that 27% of respondents had at least one security breach over the past year, compared to 19% in 2010 and 13% in 2008 [25]. 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 required of health care providers that contract or subcontract with business associates to handle medical information [26]. Providers can be penalized up to $1.5 million if the 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 [27]. While the actual number of incidents is difficult to assess, news reports on cyber-attacks proliferate. In a recent case, research computers at Kaiser Permanente were infected with malicious software for more than two and a half years before being discovered, affecting in excess of 5,000 patients [28]. In another high profile case, the infamous hacker group, Anonymous, allegedly launched a cyber-attack against Boston Children's Hospital [29]. Such events can bring down IT systems, causing disruptions in care delivery. With increased interconnectedness of health care information systems, the potential for large-scale events due to cyber-attacks is real.

4. IT-related harms have their origin in system design, implementation and use

Processes undertaken to design, build, implement and use IT provide the fundamental system safety against errors [30]. As we have seen in the previous sections, patients are harmed when design issues cause systems to fail or behave in unexpected ways.

4.1. System design

A clinical system 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 [13]. Errors are also generated when there is a mismatch of the system with the mental model of users. An example is an EHR that did not represent weight in the unit of measure used by clinicians e.g. displaying weight in pounds instead of kilograms [13].

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) [31][2]. IT 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 re-establish 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 received an excessive dose of a medication [13]. 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 [12].

Another design related issue is a *mismatch between the system model and actual clinical workflow* which can lead to errors in task execution [32, 33]. 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 pre- and postoperative orders resulting in a wrong procedure being undertaken based on a preoperative order.

Software defects introduced during development also cause IT to behave in unexpected ways. Such defects will remain if software is not adequately tested. For instance, an EHR 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.

4.2. System implementation

Beyond system design, IT safety is influenced by sociotechnical variables of the clinical setting in which systems are used [34]. 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

[2] See also: R. Marcilly et al., From usability engineering to evidence-based usability in health IT, in: E. Ammenwerth, M. Rigby (eds.), Evidence-Based Health Informatics, Stud Health Technol Inform 222, IOS Press, Amsterdam, 2016.

new technology, changes to clinical workflows and, organizational policies and procedures are not effectively managed [35]. Creation of a hybrid paper and electronic records system due to partial system implementation has also been shown to create new opportunities for error [36]. Any changes to an IT system post-implementation such as updates to software or installation of new hardware can similarly be a threat [37]. Conversely, failure to update software in a timely manner can also pose a risk. For example, a new guideline may not be updated in an operational EHR.

Errors can arise from unexpected *interactions between system modules or with other systems* [12]. IT systems are usually composed of multiple modules and they seldom operate in isolation. For instance, an ambulatory care system will contain 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 (picture archiving and communication system) [38]. And the x-ray needed to be repeated to acquire the missing images, re-exposing the child to high levels of radiation.

The supporting IT infrastructure including computer hardware, software, networks and data storage facilities are critical to safe implementation and operation. Analysis of US and Australian data indicates that technical failure is a major contributor to IT incidents [12, 13]. Ninety-six percent of the problems reported to the FDA were associated with technical failure [13]. 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 hours making it impossible to read or create records while the system was unavailable [38]. As a result procedures were cancelled and clinics were rescheduled. Failure of back up facilities and computer viruses can similarly disrupt care delivery.

4.3. System use

Safe IT 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 [39].

The *knowledge and skills* of users are fundamental to safe use of IT[3]. 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 [40]. For instance, a clinician may inadvertently prescribe the wrong medication wrongly assuming that the system will alert them about any drug interactions [41, 42]. Errors

[3] See also: E. Hovenga et al., Learning, training and teaching of health IT and its evidence for informaticians and clinical practice, in: E. Ammenwerth, M. Rigby (eds.), Evidence-Based Health Informatics, Stud Health Technol Inform 222, IOS Press, Amsterdam, 2016.

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 [43]. For example, when interrupted by a phone call a physician wrote a prescription for the wrong patient because they returned to the wrong record at the end of the call [37].

Deficiencies in *organizational policies and procedures* for system use are another threat. As we have already discussed, training is critical to safe operation of IT. 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 was unable to access critical test results from a previous hospital admission because the results of an HIV test were only visible to the ordering physician due to privacy considerations [38].

Thus we have seen that the safety of IT is an emergent property of the broader sociotechnical system. As safety is an emergent system property it needs to be addressed throughout the lifecycle of IT systems including design, build, implementation and use [44]. All the possible interactions among system components are not predictable at design, especially when IT systems are used in context of a broader sociotechnical system[4]. In large complex systems, safety problems or *hazards* tend to emerge from unexpected interactions between system components and human users. There is potential for unsafe interactions when IT systems are integrated with local clinical workflows including other technology and the organizational structure. Therefore safety should also be addressed during and after the implementation of systems.

5. Safety management covers the IT lifecycle

Strategies to improve the safety of health IT can be formalised. The overall set of processes used to identify and mitigate hazards throughout the life cycle of a system is called a safety management system, and these have evolved in other high-risk industries like aviation.[45]. For example, England has a safety management program for health IT [46]. Such programs formalize and document hazard assessment and mitigation so that system safety can be independently verified. A range of hazard assessment techniques can be applied at different points in the system life cycle [44]. The documents that set out the evidence for how hazards have been identified and managed are called a *safety case* [47]. For instance, a manufacturer is required to create a safety case when deploying a new EHR. The safety case will be continuously updated with new hazards identified during deployment or when changes are made to the system.

Standardization via guidelines or mandatory standards, and operational oversight via certification, regulation or surveillance are the two main governance approaches that are relevant to improving the safety of health IT [30, 48]:

[4] See also: B. Kaplan, Evaluation of people and organizational Issues – Sociotechnical ethnographic evaluation, in: E. Ammenwerth, M. Rigby (eds.), Evidence-Based Health Informatics, Stud Health Technol Inform 222, IOS Press, Amsterdam, 2016.

Standards: Many international technical standards can be applied to clinical software and to the quality of processes at different points in the system life cycle, spanning design, build, implementation and use in a clinical setting. However, few standards directly address the safety of clinical systems [49]. England's safety management program has implemented two standards for managing clinical risks in the design, implementation and use of health IT [47, 50]. These standards are consistent with those for safety critical software (e.g. International Electrotechnical Commission IEC 61508) and medical devices (e.g. International Organisation for Standardisation ISO 14971), and were formally adopted as NHS standards in 2009.

Guidelines: In the absence of clear standards, looser guidelines can still offer a mechanism to promote safe design and implementation practices. For instance, a guideline can be used to provide recommendations for the safe display of patient information within an EHR based upon usability principles. The US National Institute of Standards and Technology (NIST) has published a guide to evaluate EHR usability [51]. The NIST guide proposes formative usability evaluation by experts and summative testing in the hands of users incorporating a risk-based approach to examining usability problems.[5] Guidelines can similarly be applied to system implementation and use. The Australian guidelines for implementing medication systems in hospital are one example [52]. Another example is the Safety Assurance Factors for EHR Resilience (SAFER) guides sponsored by the US Office of the National Coordinator for Health IT [53]. Such guidelines are generally directed at manufacturers and healthcare organizations to assess the safety of clinical software systems as they are used in clinical setting.

Certification: Oversight process can be set up at a national or regional level to ensure that clinical software systems meet specific standards. Certification provides independent assurance that software is fit for purpose and that it meets specific requirements for functionality, interoperability and security. For instance, the manufacturer of a prescribing system may be required to show that their system provides certain core clinical functions, that it is secure and that it can be integrated with other information systems such as the EHR. Safety is addressed alongside interoperability in the Australian certification program but it is not explicitly addressed in the US and Canadian programs, though conformance with functionality, usability, interoperability, security and privacy requirements may lead to safer systems [49].

Regulation: Certification can be voluntary, and it requires regulation to compel manufacturers to comply with standards or performance targets [54]. Regulation ensures that manufacturers comply with legal requirements for software to be designed and built in a manner that its use does not compromise patient safety. For example, a manufacturer may need to submit a safety case that demonstrates that its equipment is safe for use in a clinical setting before it is allowed to deploy the system. Although standalone software has largely been outside the strict regulatory regimen applied to medical devices, current initiatives indicate a gradual move towards regulation. Existing regulatory regimens for medical devices such as the US FDA process and the CE mark in Europe provide a template for the regulation of clinical software. In Europe the safety of medical devices is regulated through a directive that focuses on manufacturing and pre-market testing leading to a declaration of conformity. In general,

[5] See also: R. Marcilly et al., From Usability Engineering to Evidence-based Usability in health IT, in: E. Ammenwerth, M. Rigby (eds.), Evidence-Based Health Informatics, Stud Health Technol Inform 222, IOS Press, Amsterdam, 2016.

the level of oversight or regulatory control should be proportional to the degree of risk that an information system poses to patients [1].

Surveillance of emerging safety issues: Beyond the stages of design and implementation, effective surveillance mechanisms are required to track any emergent safety problems associated with routine use of IT. The monitoring of incidents is central to detecting emerging problems in mainstream patient safety programs which are now well-established in most developed nations [55]. While it is mandatory to report incidents associated with regulated software, the reporting of general patient safety incidents (including those involving most health IT) is voluntary. One large-scale program directed at monitoring and responding to IT incidents reported by healthcare organizations and manufacturers is part of the England's safety management program which has been in place since 2005 [46, 49]. Yet, as we have seen before, IT incidents are being reported amongst general patient safety incidents and alongside reports of medical device failure and hazards. One source of such reports is the US FDA's MAUDE. Although the FDA does not enforce its regulatory requirements with respect to IT, some manufacturers have voluntarily listed their systems and reported incidents [13]. To facilitate the reporting of such incidents the US AHRQ has developed a new standard called a "common format" and a software tool to support detection and management of IT-related hazards [56]. The Health IT Hazard Manager facilitates the characterisation and communication of hazards along with their actual and potential adverse effects to support learning within healthcare organisations, across organisations using the same software and, by manufacturers and policymakers [11].

6. Conclusion

IT systems can enhance patient safety by improving access to information and by providing decision support, but problems with IT can pose new risks. Minimizing these risks is critical to realizing the benefits of IT. 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 IT is used, and errors arise from processes to design, build, implement, and use IT. Thus a holistic system approach that addresses IT errors at different points the system lifecycle is needed. In addition to greater standardisation and oversight to ensure safe system design and build, appropriate implementation and use of IT is critical to bring about overall improvements to patient safety. The effectiveness of specific strategies to address risks is not known and further research is required to evaluate their impact for a more evidence-based approach to IT safety. There is also a need for greater transparency where manufacturer contracts are governed by commitment to patient safety; and a balanced risk avoidance and safety promoting culture across the clinical process and IT support spectrum. When IT is used and governed responsibly it can improve patient safety, but it is not a panacea for managing safety risks. Taking a 'blind eye' approach to the risks of health IT can only lead to new forms of avoidable patient harm.

Recommended further readings

1. E. Coiera, F. Magrabi, *Information system safety*, Guide to Health Informatics, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2015, pp. 195-220.

2. Institute of Medicine, *Health IT and Patient Safety: Building Safer Systems for Better Care,* The National Academies Press, Washington, DC, 2012, http://www.nap.edu/catalog/13269/health-it-and-patient-safety-building-safer-systems-for-better, last access 11 February 2016.
3. N.G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety.* Massachusetts Institute of Technology, 2011, https://mitpress.mit.edu/books/engineering-safer-world, last access 11 February 2016.
4. W. Runciman, P. Hibbert, R. Thomson, T. van der Schaaf, H. Sherman, P. Lewalle, Towards an International Classification for Patient Safety: key concepts and terms, *Int J Qual Health Care* **21**(1) (2009), 18-26.
5. W.B. Runciman, J.A. Williamson, A. Deakin, K.A. Benveniste, K. Bannon, P.D. Hibbert, 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* **15** Suppl 1 (2006), i82-90.

Food for thought

1. Discuss the safety benefits and risks of a hybrid paper and electronic records system in a hospital setting.
2. Examine the patient safety risks of implementing a personal health record on a large-scale e.g. for a hospital, healthcare system or nationally. Hint: Think about how individual incidents can harm or increase the risk of harm to numerous patients when an IT system is used at different scales.
3. Why is a highly usable EHR not necessarily safe?
4. Why is an EHR built on the best clinical principles not necessarily safe?
5. What are some ways to improve surveillance of IT-related safety issues? Discuss the role of automated techniques.
6. Discuss the advantages and disadvantages of regulating all clinical software systems as medical devices.

References

[1] E. Coiera, *The guide to health informatics*, third edition, CRC Press, 2015.
[2] D.W. Bates, A.A. Gawande, Improving safety with information technology, *N Engl J Med* **348**(25) (2003), 2526-34.
[3] C.M. DesRoches, E.G. Campbell, S.R. Rao, K. Donelan, T.G. Ferris, A. Jha, R. Kaushal, D.E. Levy, S. Rosenbaum, A.E. Shields, D. Blumenthal, Electronic health records in ambulatory care - a national survey of physicians, *N Engl J Med* **359**(1) (2008), 50-60.
[4] R.D. Cebul, T.E. Love, A.K. Jain, C.J. Hebert, Electronic health records and quality of diabetes care, *N Engl J Med* **365**(9) (2011), 825-33.
[5] E.G. Van Eaton, K.D. Horvath, W.B. Lober, A.J. Rossini, C.A. Pellegrini, A randomized, controlled trial evaluating the impact of a computerized rounding and sign-out system on continuity of care and resident work hours, *J Am Coll Surg* **200**(4) (2005), 538-45.
[6] L.A. Petersen, T.A. Brennan, A.C. O'Neil, E.F. Cook, T.H. Lee, Does housestaff discontinuity of care increase the risk for preventable adverse events? *Ann Intern Med* **121**(11) (1994), 866-72.
[7] S.H. Brown, L.F. Fischetti, G. Graham, J. Bates, A.E. Lancaster, D. McDaniel, J. Gillon, M. Darbe, R.M. Kolodner, Use of electronic health records in disaster response: the experience of Department of Veterans Affairs after Hurricane Katrina, *Am J Public Health* **97** Suppl 1 (2007), S136-41.
[8] M. Abir, F. Mostashari, P. Atwal, N. Lurie, Electronic health records critical in the aftermath of disasters, *Prehosp Disaster Med* **27**(6) (2012), 620-2.

[9] *Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington, DC: The National Academies Press: Institute of Medicine; 2012.
[10] R. Koppel, D. Kreda, Health care information technology vendors' "hold harmless" clause: implications for patients and clinicians, *JAMA* **301**(12) (2009), 1276-8.
[11] J.M. Walker, A. Hassol, B. Bradshaw, M.E. Rezaee. *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. May 2012.
[12] F. Magrabi, M.S. Ong, W. Runciman, E. Coiera, An analysis of computer-related patient safety incidents to inform the development of a classification, *J Am Med Inform Assoc* **17**(6) (2010), 663-70.
[13] F. Magrabi, M.S. Ong, W. Runciman, E. Coiera, Using FDA reports to inform a classification for health information technology safety problems, *J Am Med Inform Assoc* **19**(1) (2012), 45-53.
[14] R.B. Myers, S.L. Jones, D.F. Sittig, Review of Reported Clinical Information System Adverse Events in US Food and Drug Administration Databases, *Appl Clin Inform* **2** (2011), 63-74.
[15] D. Warm, P. Edwards, Classifying Health Information Technology patient safety related incidents - an approach used in Wales, *Appl Clin Inform* **3**(2) (2012), 248-57.
[16] E. Sparnon, W.M. Marella, The role of the electronic health record in patient safety events, *Pennsylvania Patient Safety Authority* **9**(4) (2012), 1276-8.
[17] Y.Y. Han, J.A. Carcillo, S.T. Venkataraman, R.S. Clark, R.S. Watson, T.C. Nguyen, H. Bayir, R.A. Orr, Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system, *Pediatrics* **116**(6) (2005), 1506-12.
[18] K.E. Walsh, W.G. Adams, H. Bauchner, R.J. Vinci, J.B. Chessare, M.R. Cooper, P.M. Hebert, E.G. Schainker, C.P. Landrigan, Medication errors related to computerized order entry for children, *Pediatrics* **118**(5) (2006), 1872-9.
[19] J.S. Ash, D.F. Sittig, E.G. Poon, K. Guappone, E. Campbell, R.H. Dykstra, The extent and importance of unintended consequences related to computerized provider order entry, *J Am Med Inform Assoc* **14**(4) (2007), 415-23.
[20] K.C. Cheung, W. van der Veen, M.L. Bouvy, M. Wensing, P.M. van den Bemt, P.A. de Smet, Classification of medication incidents associated with information technology, *J Am Med Inform Assoc* **21**(e1) (2013), e63-70.
[21] R. Koppel, J.P. Metlay, A. Cohen, B. Abaluck, A.R. Localio, S.E. Kimmel, B.L. Strom, Role of computerized physician order entry systems in facilitating medication errors, *JAMA* **293**(10) (2005), 1197-203.
[22] P. Littlejohns, J.C. Wyatt, L. Garvican, Evaluating computerised health information systems: hard lessons still to be learnt, *BMJ* **326**(7394) (2003), 860-3.
[23] J.I. Westbrook, M.T. Baysari, L. Li, R. Burke, K.L. Richardson, R.O. Day, 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* **20**(6) (2013), 1159-67.
[24] U.S. Dept. Health & Human Services, *Breaches Affecting 500 or More Individuals*, https://ocrportal.hhs.gov/ocr/breach, last access 11 February 2016.
[25] Ponemon Institute LLC, *Fourth annual benchmark study on patient privacy & data security.* March 2014. https://www2.idexpertscorp.com/ponemon-report-on-patient-privacy-data-security-incidents, last access 11 February 2016.
[26] *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 (Jan. 25, 2013).
[27] US Food and Drug Administration, Cybersecurity for medical devices and hospital networks: FDA *safety communication*, http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm, last access 11 February 2016.
[28] *Computer virus at heart of Kaiser data breach*, in: Government Health IT, 2014, April 7, http://www.govhealthit.com/news/computer-virus-heart-kaiser-data-breach, last access 11 February 2016.
[29] M.B. Farrell, P. Wen, *Hacker group Anonymous targets Children's Hospital,* in: The Boston Globe; 2014, April 24.
[30] J.M. Walker, P. Carayon, N. Leveson, R.A. Paulus, J. Tooker, H. Chin, A. Bothe, Jr., W.F. Stewart, EHR safety: the way forward to safe and effective systems, *J Am Med Inform Assoc* **15**(3) (2008), 272-7.
[31] J. Nielsen, *Usability engineering*, Morgan Kaufmann, San Francisco, 1993.
[32] L.L. Novak, R.J. Holden, S.H. Anders, J.Y. Hong, B.T. Karsh, Using a sociotechnical framework to understand adaptations in health IT implementation, *Int J Med Inform* **82**(12) (2013), e331-44.

[33] D.S. Debono, D. Greenfield, J.F. Travaglia, J.C. Long, D. Black, J. Johnson, J. Braithwaite, Nurses' workarounds in acute healthcare settings: a scoping review, *BMC Health Services Research* **13** (2013), 175.
[34] D.F. Sittig, H. Singh, Defining health information technology-related errors: new developments since to err is human, *Arch Intern Med* **171**(14) (2011), 1281-4.
[35] B.T. Karsh, Beyond usability: designing effective technology implementation systems to promote patient safety, *Qual Saf Health Care* **13**(5) (2004), 388-94.
[36] Spotlight on Electronic Health Record Errors: Paper or Electronic Hybrid Workflows, Pennsylvania Patient Safety Advisory **10**(2) (2013), 55-8.
[37] F. Magrabi, T. Liaw, D. Arachi, W.B. Runciman, E. Coiera, M.R. Kidd, Identifying patient safety problems associated with information technology in general practice: an analysis of incident reports, *BMJ Qual Saf* , doi:10.1136/bmjqs-2015-004323.
[38] F. Magrabi, M. Baker, I. Sinha, M.S. Ong, S. Harrison, M.R. Kidd, W.B. Runciman, E. Coiera, Clinical safety of England's national programme for IT: A retrospective analysis of all reported safety events 2005 to 2011, *Int J Med Inform* **84**(3) (2015), 198-206.
[39] B.T. Karsh, R.J. Holden, S.J. Alper, C.K. Or, A human factors engineering paradigm for patient safety: designing to support the performance of the healthcare professional, *Qual Saf Health Care* **15** Suppl 1 (2006), i59-65.
[40] J. Horsky, G.J. Kuperman, V.L. Patel, Comprehensive analysis of a medication dosing error related to CPOE, *J Am Med Inform Assoc* **12**(4) (2005), 377-82.
[41] K. Goddard, A. Roudsari, J.C. Wyatt, Automation bias: a systematic review of frequency, effect mediators, and mitigators, *J Am Med Inform Assoc* **19**(1) (2012), 121-7.
[42] R. Parasuraman, D.H. Manzey, Complacency and bias in human use of automation: an attentional integration, *Hum Factors* **52**(3) (2010), 381-410.
[43] S.Y. Li, F. Magrabi, E. Coiera, A systematic review of the psychological literature on interruption and its patient safety implications, *J Am Med Inform Assoc* **19**(1) (2012), 6-12.
[44] N.G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*, Massachusetts Institute of Technology, USA, 2011.
[45] *Safety Management Manual (SMM),* 3rd edition, Montreal, Canada, International Civil Aviation Organisation (ICAO), 2012.
[46] M. Baker, I. Harrison, M. Gray, Safer IT in a Safer NHS: account of a partnership, *The British Healthcare Computing & Information Management* **23**(7) (2006), 11-14.
[47] *ISB 0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems*, http://systems.hscic.gov.uk/clinsafety/dscn, last access 11 February 2016.
[48] H. Singh, D.C. Classen, D.F. Sittig, Creating an oversight infrastructure for electronic health record-related patient safety hazards, *J Patient Saf* **7**(4) (2011), 169-74.
[49] F. Magrabi, J. Aarts, C. Nohr, M. Baker, S. Harrison, S. Pelayo, J. Talmon, D.F. Sittig, E. Coiera, A comparative review of patient safety initiatives for national health information technology, *Int J Med Inform* **82**(5) (2013), e139-48.
[50] *ISB 0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems*, http://systems.hscic.gov.uk/clinsafety/dscn, last access 11 February 2016.
[51] *NIST Technical Evaluation, Testing, and Validation of the Usability of Electronic Health Records,* US National Institute of Standards and Technology (NISTIR 7804), 2012, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909701, last access 11 February 2016.
[52] Australian Commission on Safety and Quality in Health Care. *Electronic Medication Management Systems - A Guide to Safe Implementation, 2nd edition, ACSQHC*, 2012, http://www.safetyandquality.gov.au/our-work/medication-safety/electronic-medication-management-systems/development-of-the-guide-to-safe-electronic-medication-management-in-hospitals, last access 11 February 2016.
[53] D.F. Sittig, J.S. Ash, H. Singh, The SAFER guides: empowering organizations to improve the safety and effectiveness of electronic health records, *Am J Manag Care* **20**(5) (2014), 418-23.
[54] E. Coiera, J. Westbrook, J. Wyatt, The safety and quality of decision support systems, *Methods Inf Med* **45** Suppl 1 (2006), 20-5.
[55] J.C. Pham, S. Gianci, J. Battles, P. Beard, J.R. Clarke, H. Coates, L. Donaldson, N. Eldridge, M. Fletcher, C.A. Goeschel, E. Heitmiller, J. Hensen, E. Kelley, J. Loeb, W. Runciman, S. Sheridan, A.W. Wu, P.J. Pronovost, Establishing a global learning community for incident-reporting systems, *Qual Saf Health Care* **19**(5) (2010), 446-51.
[56] Agency for Healthcare Research and Quality. *Common formats.* Rockville, Maryland: US Department of Health and Human Services, http://www.pso.ahrq.gov/common, last access 11 February 2016.