Information Knowledge Systems Management 10 (2011) 335–344
DOI 10.3233/IKS-2012-0200
IOS Press

Chapter 18

Towards safe information technology in health care

Jos Aarts*

Abstract: Health information technology is widely accepted to increase patient safety and reduce medical errors. The widespread implementation makes evident that health information technology has become of a complex sociotechnical system that is health care. Design and implementation may result in a failure; even health information technology can lead to adverse events instead of mitigating them. In this chapter seeks to outline the complexity of health information technology as a part of a sociotechnical systems, describes two failures at different organizational levels and presents a model how risks can occur. Unfortunately there is a mainly anecdotal knowledge about health information technology failure and potential adverse effects. Therefore the author suggests how as a first step proper and mandatory reporting can lead to better knowledge of failures of health information technology as part of a sociotechnical system and improve deployment in the coming years.

Keywords: Health informatics, patient safety, information systems

1. Introduction

Like aviation health care is a complex sociotechnical system. The number of preventable deaths, injuries and incidents is in health care relatively spoken much higher according to the landmark report "To Err is Human" [1]. Apparently it is difficult to achieve a substantial reduction that the aviation industry has been able to accomplish. Several strategies have been suggested to reduce the number of adverse events, including health information technology (HIT). A number of studies have shown that especially electronic prescribing can reduce medical errors [2]. According to these studies reduction of errors can be achieved by eliminating illegible handwriting of orders, improving completeness, better and ready availability of patient information and use of decision support technology to improve medical decision-making. However, a recent study showed however that the adoption of electronic patient records in the United States had a limited effect on the quality of care in hospitals [3]. There is even mounting evidence that information technology can induce errors, instead of correcting them [4]. A special committee of the Institute of Medicine outlined the complexity and risks of HIT and makes a number of suggestions how to improve deployment and use [5]. This paper seeks to address the issue that complex information technology is still vulnerable for a number of reasons and suggests how a better understanding of these vulnerabilities and responding to mishaps may lead to more safe information technology.

*Corresponding auhtor. E-mail: aarts@bmg.eur.nl.

Programmed systems are complex. The software engineering profession still struggles to reduce software failures to meet use requirements in complex environments [6]. When different programmed systems are connected, complexity increases exponentially, and the chance of software errors and failures increases. Humans interacting with technology add a new level of complexity. Risks and errors can arise as a result of poorly designed interfaces, a poor fit of technology in work practices and poor training. Humans do apply smart, creative and context sensitive methods to circumvent shortcomings of a system and get their work done. It is actually surprising that not many serious fatalities have occurred. An interesting observation about software errors comes from an analysis of the destruction of the Ariane 5 launcher. The analysis noted that a piece of software handling floating-point calculations, which functioned well in the older Ariane 4, was not able to handle data that were outside the range designed for this older launcher. The authors of the analysis concluded that it was not a software error persé, but an Ariane 5 design problem. The problem of the software, which was clearly not wrong, was seen as a wider problem of uncertainty about the dynamics of the vehicle. It is not difficult to see that similar problems could occur in health information systems that consist of complex interrelated technological components.

According to Heeks most health information systems fail in some way [7]. He attributed failures to gaps between the reality and purpose of design. Unfortunately, evidence is anecdotal and reported failure rates that go up to 80% are not reliable. In the medical informatics literature most studies, including my study of a failed implementation of a computerized order entry system, are case reports attempting to offer a rich description of what went wrong and how the failure might be understood [8]. Heeks argues that formal planning and control in systems development must be set alongside reflections from practice suggesting a critical role for improvisation. The number of actual reported serious events using health information technology is actually very low. The latest reported health IT related accident in the Netherlands was in 2000 the death of two hospitalized patients, who erroneously received blood of a wrong type, because the information system did not signal conflicting blood type data [9]. It is not unlikely that the accelerated deployment of health IT in organizations across Western countries will increase the risk of incidents and accidents. In the next paragraph I will elaborate on two problematic projects to implement health IT. In the last paragraph I will draw some conclusions and put the issue of sociotechnical information systems in a wider context taking into account recent discussions on the potential risks of health IT and suggestions how to deal with these issues.

2. Two case studies

In this section I present two case studies on the outcome of health IT implementations. The common denominator is the fact that both HIT projects affect the work processes of health professionals. In 1997 a major academic medical center in the Netherlands decided to adopt a computerized physician order entry system (CPOE) for ordering diagnostic and therapeutic tests in an outpatient laboratory [10]. The reasons were the large volume of lab orders, the apparent large number of incorrect filled-in orders and the presence of a full-fledged information technology infrastructure. It was decided to start a pilot project in the neurology outpatient department because its well-organized working practices including the use of clinical protocols. Some components of the system, such as the database, were purchased and the user-interface software layer was to be developed in-house. Since the system was to become part of the hospital IT infrastructure, it required changes to the hospital information system. Changes in staffing led to the establishment of a new project team in 2003 that defined system specifications based on interviews with prospective users and earlier analyses of requirements. The implementation of the pilot system was

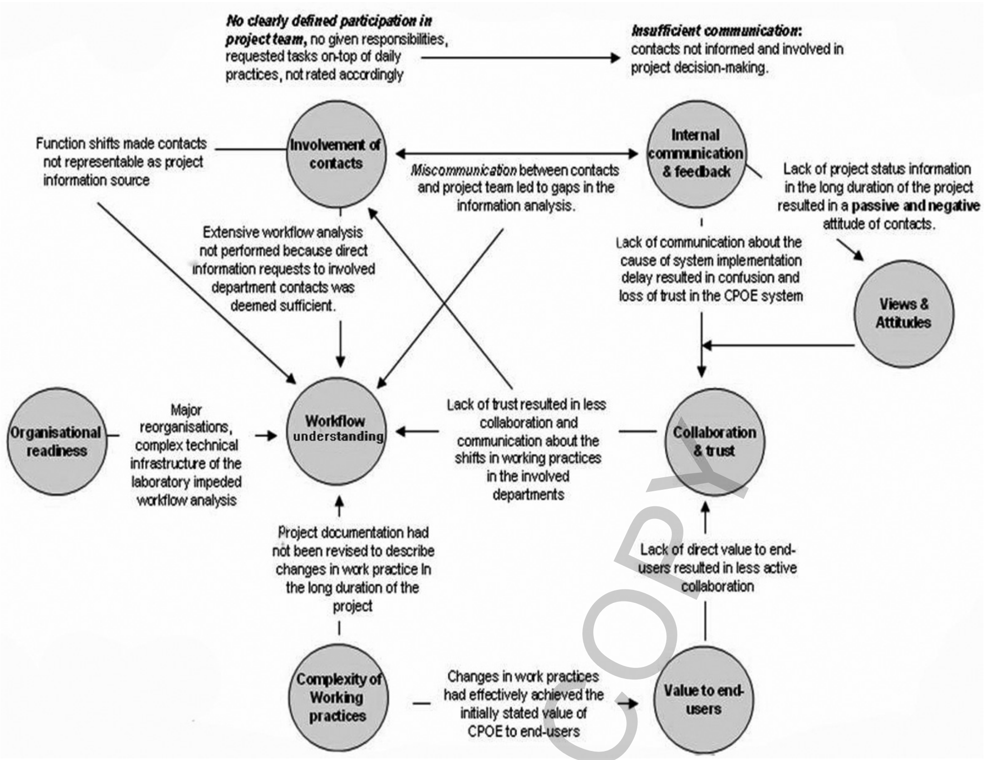
No clearly defined participation in project team, no given responsibilities, requested tasks on-top of daily practices, not rated accordingly
Insufficient communication: contacts not informed and involved in project decision-making.
Function shifts made contacts not representable as project information source
Involvement of contacts
Miscommunication between contacts and project team led to gaps in the information analysis.
Internal communication & feedback
Lack of project status information in the long duration of the project resulted in a passive and negative attitude of contacts.
Extensive workflow analysis not performed because direct information requests to involved department contacts was deemed sufficient.
Lack of communication about the cause of system implementation delay resulted in confusion and loss of trust in the CPOE system
Views & Attitudes
Organisational readiness
Major reorganisations, complex technical infrastructure of the laboratory impeded workflow analysis
Workflow understanding
Lack of trust resulted in less collaboration and communication about the shifts in working practices in the involved departments
Collaboration & trust
Project documentation had not been revised to describe changes in work practice In the long duration of the project
Lack of direct value to end-users resulted in less active collaboration
Complexity of Working practices
Changes in work practices had effectively achieved the initially stated value of CPOE to end-users
Value to end-users

Fig. 1. The interrelated events and issues that led to the mismatch between the neurology department's workflow and system design. The first author of the failed implementation study observed and interviewed the people involved and identified the issues using a sociotechnical framework [10].

however not successful and the system was pulled back late 2004. Analysis of the project showed that the mismatch between the department's workflow and system design was the root cause of the failure. The mismatch was the result of a series of interrelated issues and events impacting workflow that eventually led to the abandonment of the systems, depicted in Fig. 1.

Though the root cause was a mismatch between the laboratory workflow and the designed system, Fig. 1 makes clear that an accumulation of events and issues lead to the abandonment of the system. It resonates well with Reason's model of breakdown of complex systems [11]. Each of the events does not necessarily lead to system failure, but it is rather the convolution of events. Other reported information system failures can be interpreted in a similar fashion.

Until not too long ago information systems in health care organizations were basically stand-alone. The increasing mobility of citizens led to initiatives at national and regional levels to establish health care communication infrastructures. In the Netherlands key stakeholders decided on a system enabling health care providers to query locally stored electronic health records [12]. In several countries the implementation of such infrastructures has met serious setbacks. An example is the National Program for Information Technology (NPfIT) in the United Kingdom, which was marred by its sheer size and numerous stakeholders, and of which the current conservative government in September 2010 [13] ended its deployment. A study of the implementation of an summary care record system as part of NPfIT showed less benefits than the sponsors had anticipated and storing patient data centrally remained highly controversial [14]. In a study of the implementation of information systems in the public sector Goldfinch posits that the larger the project the more likely it will be unsuccessful because of exponential growing complexity [15]. Implementation failures are mainly seen as problems of control. The roots of developing a national infrastructure can be traced back to 1996 when the Ministry of Health required an integral vision on the use of IT in health care, which would focus on quality and efficiency. A few years later, the rationale of the national health IT infrastructure became the need to reduce the number preventable deaths – estimated at about 1200 per year – and hospital readmissions. The characteristics of a future health care information system were described as an infrastructure that would make all electronic patient data available to authorized professionals at all times at locations. This was achieved by introducing a central node or hub that would process all information requests by health care professionals. Information of patients would be identified through their unique social security number. Originally development and implementation of IT was seen as a responsibility of the health care field, but in 2002 the national IT project became a responsibility of the government to be supported by appropriate legislation to adopt the technology. The National Institute for Health IT (Nictiz) was entrusted with the task of development and implementation. The Ministry of Health as a dominant stakeholder did not only set health care policy but also provided funding for the project. The project evoked controversies [16]. Patient advocacy groups aligned themselves with the ministry since they recognized the benefits of reducing medical errors, but also as an instrument to strengthen their position of not being dependent on the willingness of individual health care professionals to share records. The professional societies expressed support through their leadership, but their membership was much more critical because of their concerns about the confidentiality of patient-provider relationship, budgetary consequences for practices and professional autonomy and discretional space of medical decision-making. At the regional level hospitals, primary care organizations and pharmacies developed digital networks to exchange health care data. Though these bottom-up initiatives were welcomed at the national level as examples how different parties could work together, they were also seen as a problem because the perceived non-adherence to emerging national standards for information exchange as a risk for medical errors and breach of privacy. It renewed a discussion about the need and privacy safeguards of the national electronic patient record. Legislation that passed in the lower chamber of the Dutch parliament was voted down in the upper chamber in April 2011. As a result financial government support was withdrawn, and Nictiz will pull the plug on the system on January 1, 2012.

3. Analysis

Health care is a complex sociotechnical system. Introducing health IT adds to this complexity. The number of reported fatal accidents is very low. However, increasingly studies show that health IT may have unintended, and usually undesired consequences [17]. The widespread, accelerated adoption resulting from policies, regulation and legislation in different countries may engender unintended consequences throughout health care organizations under pressure to accommodate the changes. Moreover, the track record of putting health IT to use is dismal. Under the current circumstances we can expect the number of health IT incidents will increase. The two case studies presented are exemplary of their own right. Implementation failures happen at the micro-level of organizational departments and occur at the national level. Health IT is by itself a complex sociotechnical system. In this paragraph I will analyze the source of risks of implementing IT, how risks are being mitigated in practice and barriers to safe systems. Where appropriate I will refer to the case studies described above but also quote other studies.

Health IT systems should serve organizational purposes, fit in work processes, be usable and safe. Figure 3 depicts what risks are involved, how these risks can be mitigated and what barriers exist to mitigate the risks.

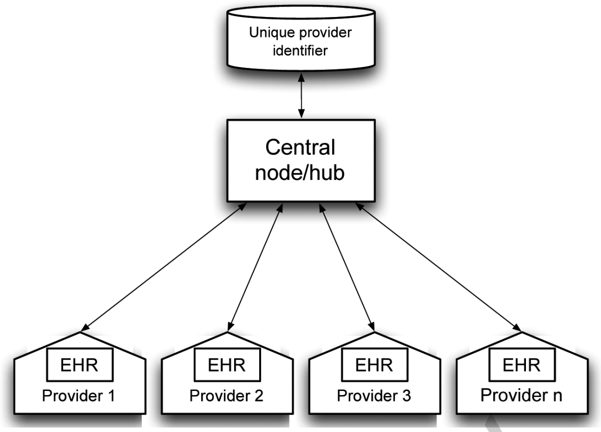

Fig. 2. Simplified scheme of the Dutch national health IT infrastructure. Patient data resides in electronic health records (EHRs) at the location of the provider, e.g. primary care center, pharmacy or hospital. Health care provider 1 can query through the central node availability of patient data with other providers. The hub finds that information is available with provider n and requests transmission. After authorization the information is sent to provider 1. Not only patients are identified through their unique social security number, but each provider has also a computer-stored unique identifier. A suite of software applications handles queries, checks authorization, retrieves and sends patient data, and logs activities. The electronic health record of each provider should comply with national standards, including those for data protection. Nictiz characterized the national infrastructure as a "Google for health care".

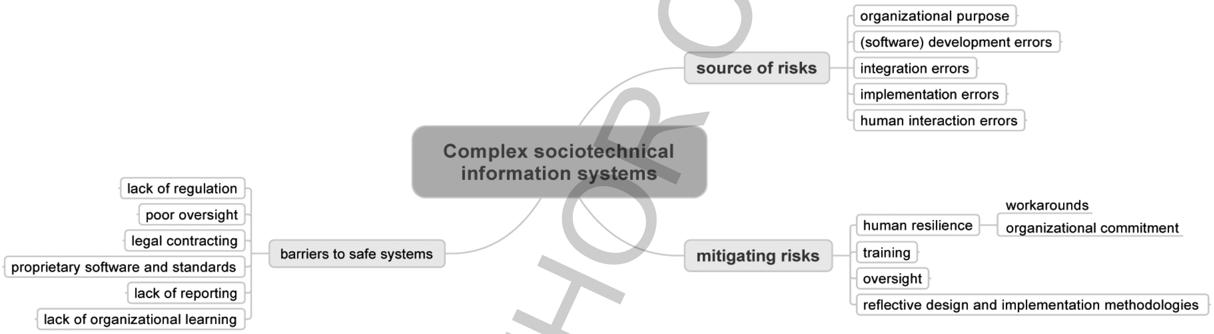

Fig. 3. Health IT as a complex sociotechnical system.

Basically I identify five sources of risk. The first is risks involving organizational purpose. Often writing software only starts when a decision is made that an information system should be implemented to address an organizational problem. The risk is then that the organizational purpose is not well understood, so that a development trajectory is initiated that is doomed from the outset. In quite a few cases it only becomes clear that there is a problem when the project is well underway. This was the case in the implementation of a computerized physician order entry system in another Dutch university medical center [8]. The project team assumed that the intended users were familiar with entering medication orders in a computerized system. This was not the case. One of the physicians observed: "The system requires a doctor to send electronic notes. Doctors don't send notes. They have other people doing that for them." The implementation was a failure. The example shows how crucial it is that a system is aligned with organizational purposes. Software (development) errors are a second source. Any programmed systems contain software code errors. Software verification and validation procedures are in place to reduce errors as much as possible. Therefore very few accidents have been

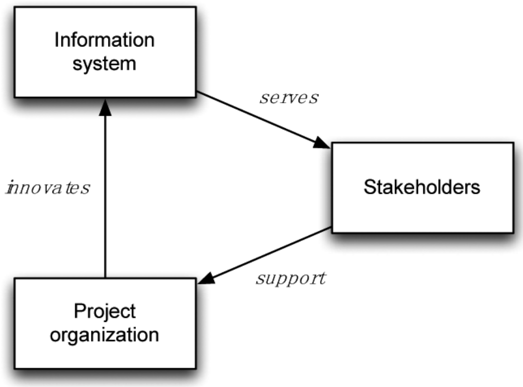

Fig. 4. Triangle of dependences. Failure is likely to happen when the project organization is not able to deliver the benefits of an information system and so loses support from the stakeholders.

reported that contain coding errors, but many more that can be related to the management of the software development process [18]. Two aspects of software development need to be taken into account. First, software development is increasingly modular and even done in different locations. Joining together software modules into an application can be a serious risk. Second, a health IT application can be seen as a number of tightly coupled software components; for example the data processing, data storage and data presentation components can be different software modules that are joined together in a later stage of development. Each component can be fault-free, but generate serious errors when integrated. Software errors are now mainly seen as resulting from software development management errors [19]. The fact that an IT system consists of many components points to the third cause of risk of errors caused by integration. Often the components come from different software companies and are only integrated by systems integrators, usually a company that offers a suite of software products. It is also not very uncommon that a health care organization as customer is responsible for integration. The problematic integration of the laboratory order entry software and hospital information system described above may be interpreted as such. The fourth source of risk, implementation errors, is broad encompassing category. I consider implementation as a trajectory of introducing an information system from the very first moment of a perceived need to address an organizational problem to the dynamics of use in work practices. In this context Sauer established dependency between the system, the project organization for its realization and the supporters [20]. The dependences are pictured in Fig. 4. There exists an exchange relation between the project organization and its stakeholders where the information system and support are the resources traded. The project organization delivers and gets support in the form of material and human resources, help in coping with contingencies and other exercises of power. Support is dependent on the benefits that the stakeholders receive. A project failure can thus happen when this interdependency breaks down, especially when the project is not able to deliver the resources that the stakeholders expect.

Both case studies show how these dependencies are broken. The laboratory order entry system failed to meet the expectations of the physicians of the neurology outpatient clinic. The department withdrew its support and the project had to be abandoned. The national electronic patient record system lost support from the politicians who allocate funding. The space of this chapter prohibits a detailed analysis of factors contributing to a breakdown of dependences. Most published studies of information system failures can be interpreted according to the Sauer model. The last category is human interaction errors. It can be argued that belong to the previous category of implementation errors, but often they become manifest after some time of use. Though Nielsen has developed guidelines for proper human-computer interaction design, I single them also out because of the fact that they often ignored in the whole picture of system design and implementation [21,22].

4. Reducing risks

Risks become mostly manifest in practice. It can already be in the beginning of an implementation trajectory and more often in the phase that the system is (intended) to being used. Humans are an important factor in reducing risks of health IT. When a system interferes with the workflow they often devise workarounds that mitigate the shortcomings [23]. Workarounds do have a negative connotation since they either refer to people not handling appropriately technology, or to technology that is not properly designed. Here I would argue that workarounds are sometimes beneficial since no piece of technology will fit perfectly with work practices, and then workarounds will indeed help to reduce risks. Another aspect of human interference of reducing risks is organizational commitment. In the long-run health IT can be beneficial and, knowing that the road towards such systems can be bumpy, organizational commitment can helpful to convince people to use the system and find ways of fitting into work practices. Organizational commitment seems to be one of the factors contributing to adopting electronic prescribing in hospitals [24]. Proper training is a second important factor to reduce risks of health IT. However trivial, it is surprising how often timing of training programs can be wrong or how misdirected it can be. Acquiring skills and knowledge of using a system is most effective when it related to an immediate need of use. For example, in many hospitals physicians are required to take a course before they authorized to prescribe medication electronically. Often, training is aimed at the wrong audience. Anecdotal reports suggest that often managers are offered a training program, while the actual users are left in the dark. Oversight may help also to reduce risks of technology. The goal of oversight is to be informed, to respond and take appropriate measures. It is still open for debate at what level oversight should be based. Overseeing implementation can best organized within the organization ensuring that the entity entrusted with this task is the not the same as the project management team. Finally reflective design and implementation methodologies can help mitigate. The keyword is ‘reflective.’ At its simplest it is about asking the question whether the right things are being done and what the effects might be on the realization of the system. I follow here the plea by Claudio Ciborra for reflective practices when designing and implementing systems and to allow improvisations to address contingencies that are so characteristic of highly complex sociotechnical systems [25]. Focusing on technical and functional specifications is not sufficient, eliciting context of use by inquiring about and observation of work practices is equally important. Reflective practices can also help to draw from previous experiences of designing and implementing systems. This is not only a responsibility of a manufacturer of systems, but also of the vendor and the organization where those systems are being implemented.

5. Barriers to safe systems

A new drug or new medical procedure can only be used in health care after a long process of testing its efficacy and effectiveness and assessing potential harmful side effects by government bodies and after approval the drug remains subject to oversight. Health IT systems that impact patient are not subject to such assessment requirements. This points to the first barrier to safe systems, the lack of regulation. The lack of regulation means that there are no explicit quality criteria for health IT, apart from what is custom in contractual relationships and given state of knowledge. It is compounded by the fact that health IT is not a "single product", but exists of components that at the one hand are often tightly connected and at the other provided by different vendors and/or manufacturers. Not surprisingly Hoffman and Podgurski have recently commented that regulation is completely absent [26]. Because of little regulation the burden of proof sits with the victim and possibly the organization at large involved if an accident happens that involves health IT. A lack of regulation means that there is also poor oversight. In many countries supervising bodies act only in the case of a serious accident or incident and usually there is little prevention. In many cases it also because of shortage of expert staffing. Increasingly supervisory bodies require reporting on the basis of performance indicators that include information on health IT. The indicators have unfortunately too little granularity to be meaningful to assess safety of complex health IT systems. Another question is what body is most suited to exercise oversight. In the United States there are already minimal three organizations that address information technology: the FDA, NIST and the Office of the National Coordinator for Health IT (ONCHIT). Health care organizations can subject themselves to voluntary accreditation by the Joint Commission, which most organizations do.

Another serious impediment to safe systems is legal contracting. Koppel and Kreda reported in a commentary in the Journal of the American Medical Association three problematic clauses in contracts between hospitals and vendors, which are the "hold harmless", "learned intermediary" and "non-disclosure" clauses [27]. The hold harmless clause stipulates that the vendor can never be held liable for any flaws of the product. The learned intermediary clause assumes that the user has sufficient knowledge and skills to understand and handle an IT application appropriately and excludes the vendor liability for any errors. The non-disclosure clause prohibits public reporting of potential faults and hazards of a software product because of proprietary rights and protection of corporate reputations.

A methods of health IT vendors to get a share of the market and protect their business is the use of proprietary software and standards. Proprietary software cannot be modified without permission or direct involvement of the vendor. Often modifications must be requested and only if there is a positive business case they will be implemented. It is for this reason that use of open source software has gained popularity in health care [28]. For example, information systems developed in the Veterans Health Systems are based on open source software tools and can be uses and modified by any party. By proprietary standards vendors ensure that customers can only buy their suite of products. Though standardization of data exchange, communication and terminologies has increasingly been mandated, slow progress is being seen as one of the barriers for regional and national wide health information systems [29]. There is consensus that voluntary standardization does not work well and that government intervention is needed to ensure better interoperability between systems.

The above-mentioned disincentives to safe systems are reflected in a dismal lack of structured reporting of problems of information systems that may compromise proper use or even patient safety. Most reporting is anecdotal and often result from formal inquiries stipulated by government agencies or health inspectorates in case of serious incidents and accidents [30,31]. Underreporting is not only specific for health IT, but also seen in the wider context of a protective culture in health care organizations. Noble and Pronovost report how underreporting of patient safety incidents can lead to serious bias and inability to respond to serious incidents and accidents [32]. There is also evidence of lack of evaluative reporting at the level of organizations.

Finally, lack of organizational learning is a serious impediment to safe systems [33]. Again, this lack can be inferred from the factors that pose a barrier to safe systems. Adding to the problem is the high turnover of personnel involved in designing and implementing health IT. The usual project nature of health IT implementation does not help either because of the inherent flux of participants. There is therefore strong evidence that within an organization mistakes are being made over and over again [34].

6. Conclusion

Health IT forms part of a complex sociotechnical system that is health care. Unlike drugs and medical procedures as medical interventions it cannot be evaluated unambiguously. There is no simple relation between intervention and effect. It is hard then to establish a root-cause in the event of incidents and accidents involving health IT. Bad outcomes are still anecdotal contrary to high-profiled cases of insufficient testing of medications such as the thalidomide affair, which led to strict testing procedures before a drug could be approved [35]. It means that regulations that require pre-implementation assessments for health IT are meaningless. Most problems of health IT occur in the phase of implementing. I have identified six barriers to safe systems. I would like to single out mandatory interoperability and incident reporting as the two most important measures to be taken. Vendor products could be certified for interoperability by an independent agency, in the United States by organizations such as ONCHIT or NIST and in the European by comparable bodies. I do not exclude private agencies as long as they operate independently from vendors and customers. Reporting is essential as an early warning system for potential serious hazards and to increase the knowledge about these incidents by systematic analysis.

References

[1] Landrigan CP, Parry GJ, Bones CB, Hackbarth AD, Goldmann DA, Sharek PJ. Temporal trends in rates of patient harm resulting from medical care. N Engl J Med. 2010 Nov 25;363(22):2124-34.
[2] 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 Jul–Aug;6(4):313-21.
[3] Jones SS, Adams JL, Schneider EC, Ringel JS, McGlynn EA. Electronic health record adoption and quality improvement in US hospitals. Am J Manag Care. 2010;16(12):SP64-71.
[4] 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 Mar 9;293(10):1197-203.
[5] Services Committee Patient Safety and Health Information Technology Board on Health Care Services. Health IT and patient safety: building safer systems for better care. Washington: Institute of Medicine, 2011.
[6] Lyu MR. Software reliability engineering: a roadmap. Future Softw Eng. 2007:153-70.
[7] Heeks R. Health information systems: failure, success and improvisation. Int J Med Inform. 2006 Feb;75(2):125-37.
[8] Aarts J, Doorewaard H, Berg M. Understanding implementation: the case of a computerized physician order entry system in a large Dutch university medical center. J Am Med Inform Assoc. 2004 May-Jun;11(3):207-16.
[9] Mat J. Fout bloed blijkt computerfout (Wrong blood due to computer error). NRC Handelsblad. 2000 April 20, 2000.
[10] Peute LW, Aarts J, Bakker PJ, Jaspers MW. Anatomy of a failure: A sociotechnical evaluation of a laboratory physician order entry system implementation. Int J Med Inform. 2010 Apr;79(4):e58-e70.
[11] Reason J. Human error: models and management. BMJ. 2000 Mar 18;320(7237):768-70.
[12] de Graaf JC, Vlug AE, van Boven GJ. Dutch virtual integration of healthcare information. Methods Inf Med. 2007;46(4): 458-62.
[13] Sauer C, Willcocks L. Unreasonable expectations – NHS IT, Greek choruses and the games institutions play around mega-programmes. Journal of Information Technology. 2007;22(3):195-201.
[14] Greenhalgh T, Stramer K, Bratan T, Byrne E, Russell J, Potts HW. Adoption and non-adoption of a shared electronic summary record in England: a mixed-method case study. BMJ. 2010;340:c3111.
[15] Goldfinch S. Pessimism, computer failure, and information systems development in the public sector. Public Admin Rev. 2007 Sep–Oct;67(5):917-29.
[16] Verhage SJ. Better health care through better information? Mapping the health care information technology of the EPD and the controversy over its implementation in Dutch health care. Unpublished Master Thesis Amsterdam: University of Amsterdam; 2010.
[17] Bloomrosen M, Starren J, Lorenzi NM, Ash JS, Patel VL, Shortliffe EH. Anticipating and addressing the unintended consequences of health IT and policy: a report from the AMIA 2009 Health Policy Meeting. J Am Med Inform Assoc. 2011 Jan 1;18(1):82-90.
[18] Leveson NG, Turner CS. An investigation of the Therac-25 accidents. Comput. 1993 Jul;26(7):18-41.
[19] Ewusi-Mensah K. Software development failures. Cambridge (MA): The MIT Press; 2003.
[20] Sauer C. Why information systems fail: a case study approach. Henley-on-Thames: Alfred Waller; 1993.

[21] Carroll JM. Human-computer interaction: psychology as a science of design. Annual Review Of Psychology. 1997;48:61-83.

[22] Olson GM, Olson JS. Human-computer interaction: psychological aspects of the human use of computing. Annual Review Of Psychology. 2003;54:491-516.

[23] Halbesleben JR, Wakefield DS, Wakefield BJ. Work-arounds in health care settings: literature review and research agenda. Health Care Manage Rev. 2008 Jan-Mar;33(1):2-12.

[24] Aarts J, Koppel R. Implementation of computerized physician order entry in seven countries. Health Aff (Millwood). 2009 Mar–Apr;28(2):404-14.

[25] Ciborra C. The labyrinths of information, challenging the wisdom of systems. Oxford: Oxford University Press; 2002.

[26] Hoffmann S, Podgurski A. Finding a cure: the case for regulation and oversight of electronic health record systems. Harvard Journal of Law and Technology. 2008;22(1):103-65.

[27] Koppel R, Kreda D. Health care information technology vendors' "hold harmless" clause: implications for patients and clinicians. JAMA. 2009 Mar 25;301(12):1276-8.

[28] Sfakianakis S, Chronaki CE, Chiarugi F, Conforti F, Katehakis DG. Reflections on the role of open source in health information system interoperability. Yearb Med Inform. 2007:50-60.

[29] Yellowlees PM, Marks SL, Hogarth M, Turner S. Standards-based, open-source electronic health record systems: a desirable future for the U.S. health industry. Telemed J E Health. 2008 Apr;14(3):284-8.

[30] Leveson N. Safeware: system safety and computers. Reading, Mass.: Addison-Wesley; 1995.

[31] Beynon-Davies P. Human error and information systems failure: the case of the London ambulance service computer-aided despatch system project. Interact Comput. 1999;11(6):699-720.

[32] Noble DJ, Pronovost PJ. Underreporting of patient safety incidents reduces health care's ability to quantify and accurately measure harm reduction. J Patient Saf. 2010 Sep;6(4):247-50.

[33] Edmondson AC. Learning from failure in health care: frequent opportunities, pervasive barriers. Qual Saf Health Care. 2004 Dec;13 Suppl 2:ii3-9.

[34] Pan G, Hackney R, Pan SL. Information systems implementation failure: Insights from prism. Int J Inform Manage. 2008 Aug;28(4):259-69.

[35] Mellin GW, Katzenstein M. The saga of thalidomide. Neuropathy to embryopathy, with case reports of congenital anomalies. N Engl J Med. 1962 Dec 6;267:1184-92.