The dangerous decade
Enrico Coiera,1 Jos Aarts,2 Casimir Kulikowski3

ABSTRACT
Over the next 10 years, more information and communication technology (ICT) will be deployed in the health system than in its entire previous history. Systems will be larger in scope, more complex, and move from regional to national and supranational scale. Yet we are at roughly the same place the aviation industry was in the 1950s with respect to system safety. Even if ICT harm rates do not increase, increased ICT use will increase the absolute number of ICT related harms. Factors that could diminish ICT harm include adoption of common standards, technology maturity, better system development, testing, implementation and end user training. Factors that will increase harm rates include complexity and heterogeneity of systems and their interfaces, rapid implementation and poor training of users. Mitigating these harms will not be easy, as organizational inertia is likely to generate a hysteresis-like lag, where the paths to increase and decrease harm are not identical.

There is a paradox in the relationship between information and communication technology (ICT) and patient safety. ICT can improve the quality, safety and effectiveness of clinical services and patient outcomes,1 although the evidence base for this is sometimes weak.2 As a consequence, the rapid deployment of ICT on a national scale is a priority for many nations faced with a diminishing clinical workforce, increasing workloads, and resource constraints.3 4

However, ICT use can also lead to patient harm.5 Many commentators have raised concerns that ICT has yet to deliver on its promises,6 or that the rapid adoption of ICT is a risk.7 8 Errors persist in clinical practice even after ICT is introduced,9 because manual processes co-exist with the automated, and the interfaces between the two are seldom perfect. Others counter that such overemphasis on ICT-related harm only delays the implementation of a crucial technology that will save lives.9

It appears that we are caught in a bind. The demands for health system reform are now so compelling that there appears no choice but to implement complex ICT on a large, often national, scale. Yet these ICT systems appear less mature than we would like and our understanding about how to implement and use them safely remains in its infancy. A such, we are faced with a pressing policy challenge on both the national and international stages.10

The Institute of Medicine (IOM) of the USA’s National Academy of Sciences has now issued a report entitled “Health IT and Patient Safety: Building Safer Systems for Better Care”.10 It identifies what is known about health ICT safety, and comments on the complex socio-technical context within which these systems are developed and operate. The report makes clear that there is currently a significant gap in our understanding of the extent and severity of ICT related harm, but that to await more evidence before dealing with the problem is no longer an option. It recommends standards for safety of health IT systems be developed for manufacturers to follow, that a new federal entity be created to specifically monitor and investigate patient deaths, serious injuries, and unsafe conditions associated with health IT, and to make public its findings. It concludes that the Food and Drug Administration should immediately begin on a framework for regulating health ICT. There is however caution in the report that safety regulations would impede industry innovation, an argument which would literally not fly in the aviation industry. Indeed dissenting views, within the IOM report and without, feel that the time for regulation has now well and truly arrived.10b Indeed, calls for regulation of clinical software have been with us for some time now.10b 10c The IOM report is a welcome request both for the resources needed to fill in the gaps in our research evidence about the safety of ICT, but also to put resources into the active detection and management of ICT related harms and near misses. Its caution toward recommending regulation may however be misplaced. Simply put, if healthcare wants the benefits of ICT then it must actively manage its risks.

While basic technical standards for interoperability are now being adopted in many nations, clear standards for user interface design, decision support system construction, or clinician training are only slowly emerging. We are now beginning to appreciate the complex sociotechnical construct that is created when ICT is placed in the hands of busy clinicians in busy clinical environments.11 Implementing the same ICT in highly similar organizations can still end up having different results, because of local differences in work or communication patterns.12

Our understanding of the unintended opportunities for harm that arise when interruptions and multitasking disrupt clinicians using information systems is also in its infancy. The psychological literature on interruption is complex, and designing ICT that is ‘interruption safe’ remains a challenging goal.13 14

If we look to industries in which technical safety is also crucial, history tells us that the journey to creating robust, industrial strength and safe systems is a sometimes perilous one.15 The aviation industry, often held up as a paragon of safety, developed its safety culture, processes and technology after a very challenging period. Commercial aircraft did crash, lives were lost, and out of catastrophic failures, learning occurred. The learning cycle repeats with every new ‘quantum leap’ in plane design and the human–machine adaptations that must follow. Technological change always creates new pathways to harm, as evidenced by the sensor malfunctions that led to the Air France airbus catastrophe.
In comparison to aviation, healthcare appears to be more complex, heterogeneous, and harder to control. Yet over the next 10 years, around the world, we will build and deploy more ICT into the health system than in the entire previous history of our discipline. These systems will be larger in scope, more complex, and move from regional to national, and possibly supranational scale. Yet we could argue that we are at roughly the same place the aviation industry was in the 1950s. Will health ICT have to go through a similar painful period of learning from unexpected accidents?

At present ICT-related errors are slowly being identified, and their different types and causations described. Analysis of incident reports from the clinical front line is of particular importance right now, and is revealing the complex nature of the human and technical problems that combine to harm patients. Unsurprisingly, the majority of incident reports reflect the mundane reality of working in organizations in which there are power outages, resource constraints, network disruptions, and printer failures, as well as the human factors associated with working in technologically, cognitively, and socially complex environments. Not all types of ICT-related patient harm are the same. Some are serious, as with patient injuries from incorrect dosage of medications or radiotherapy. Other events may have a minor impact on individual patients but signal widespread organizational disruption.

**THE DIFFERENCE BETWEEN HARM CREATION AND HARM MITIGATION**

Should we expect the number of patient harm events to rise as ICT is widely introduced into healthcare environments? With increased use of ICT the number of harms due to ICT is indeed likely to rise. Assuming a fixed probability of harm associated with each ICT use, in a setting of increased ICT use, there can indeed only be an increased number of ICT harm events (figure 1). To capture this simple observation, we suggest a first postulate of patient safety: For a given configuration of a system, the number of patient harm events increases in proportion to the frequency of events likely to cause harm.

The actual rate of harm will also be shaped by the intrinsic safety of the system in its entirety. This ‘opportunity for harm’ in a given system configuration is governed by two broad sets of factors. One set diminishes the chances for harm and relates to technology maturity, improvements in quality of system development, testing, implementation and end user training. Simplification of systems through the adoption of common standards should also lead to reduced harm rates. The second set of factors is associated with an increased harm rate. These include increasing complexity and heterogeneity of systems and interfaces between systems, overly rapid implementation schedules and poor training of users.

At first glance it seems that all we now have to do is work on harm mitigation, to offset any growth in system size, use and complexity. However, health systems have repeatedly been observed not to behave in a simple linear fashion. There are indeed factors that have some sort of direct linear relationship with harm—the direct correspondence between the number of times a piece of software is used and the likelihood of harm, for example. Reduce how often the software is used, and you should reduce the associated harm.

Other factors are unlikely to be so well behaved. The health system often appears to exhibit system inertia, a resistance to change or a failure to achieve the degree of change expected for a specific amount of effort. System inertia may well underpin our slow progress with reducing iatrogenic patient harm and delivering evidence-based recommended care. System inertia has been long studied in the organizational science literature, and one specific manifestation of inertia is a hysteretic-like lag, in which the paths to increase and decrease an output of an organization are not identical, possibly because of the way organizations are structured, and their competing demands. We should not be surprised that in the complex feedback systems designed to control patient harm, many system states will lag attempts to change them, resulting in a ‘hysteresis-like’ relationship between output and control variables.

The gives rise to a second patient safety postulate: For a given configuration of a system, the rate of harm relative to opportunity to harm will exhibit a ‘hysteretic-like’ curve, as system inertia may impede attempts to reduce the harm rate, once it has increased.

This means that mitigating the expected increase in ICT-related harm due to increased use will not be easy (figure 2). Making the health system do what we want it to do is non-trivial. We thus need to understand better how those factors that increase or decrease harm rates interact to help find ways of reducing the rate of harm attributable to ICT.

**FACTORS THAT INCREASE THE RATE OF HARM**

**Increased system usage**

The level of investment in ICT provides a simple proxy measure for the growth in the number of system implementations and users. According to one estimate, the US health ICT market is experiencing a 4.5% compound annual growth rate over the next few years. According to our first ‘postulate’, and only assuming a linear relationship between increasing system deployments and harm, we could expect an approximately 5% per annum compound growth in ICT-related patient harms. This is, however, likely to be a lower bound, as the harm rate is more likely be non-linear. The opportunities for harm are likely to be governed by complex network effects, in which the number of new implementations, the number of new users, and the growth in rate of usage, all contribute to increased harm, suggesting more of a logistic curve.

**Increased system complexity**

We know from clinical practice that harm occurs at the boundaries of care, when information is passed from one party to the next. The situation is the same with ICT. For example, most hospitals have no homogenous ICT ‘system’ but rather maintain a patchwork of different departmental systems.
plumbed together to meet the organization’s needs. Unsurprisingly, networking errors and failure of information to pass between different clinical subsystems are a commonly reported event when patient safety incident reports are analyzed.²⁵

Differences in information models between systems mean that semantic and technical interoperability always remains imperfect. There is thus a patient safety trade-off between opting for flexible choice of the most suitable systems for specific clinical needs and the risks of interfacing heterogeneous systems. As system standards are an ever-moving and dynamic ‘target’, this problem is unlikely to be solved in the near term.

System complexity is also encountered at the user interface, and simpler systems that better fit the tasks at hand and the cognitive models of users are considered the ideal. Ensuring such usability requires system designers to engage, using different methods, at multiple stages in the software life cycle.²¹ underscoring the challenge to us all in managing the multiple interactions that occur between user, task, information system and environment.²¹α

**Reduced implementation times**

There is evidence that quick ICT implementation times are associated with increased risks of error and patient harm.²² Shortened implementation is often the result of artificial time-tables, driven by factors including a failure to appreciate the importance of training the clinical workforce, a need to minimize implementation costs, or externally imposed timetables.²²α In the USA, those institutions with mature ICT systems and a trained and expert workforce still need to make substantial efforts to comply with meaningful use requirements. There is likely to be a tail of laggard health organizations that have no or immature existing systems, little local expertise, but are facing looming deadlines with significant cost penalties. These laggards face a choice of wearing the penalties, which may have substantial fiscal impacts, or undertaking programmes of rapid adoption of ICT systems. Adopting ICT in haste, without clinical leadership and support, and to avoid penalties based upon highly specific rules will probably see organizations attempting to ‘tick the boxes’ for meaningful use certification. They will not necessarily be implementing the systems they need, nor attending to long-term issues of system quality and safety. An unintended consequence of a short deadline to comply with meaningful use requirements in the USA is that we may see a spike in harm associated with poorly implemented systems in laggard organizations. It may also mean the financial failure of some organizations that are unable to comply.

**FACTORS THAT DECREASE THE RATE OF HARM**

**Better software quality**

There are scant public data about the rate of software errors in clinical systems or their impact on patient safety. Such data, when they are actually collected, are likely to be commercial and kept confidential, and there appear to be no formal mechanisms for enforcing the recording or reporting of software error rates.

One now decade old dataset was generated from three releases of a major commercial USA medical record system and is illustrative.²³ ²⁴ The system contained 188 separate software components across 6500 files. Release 1 had defects in 58 of 180 components, seven of which were only discovered post-release. Release 2 had 64 defects in 185 components, with five discovered post-release. Release 3 showed a numerical improvement in quality, with only 40 of 185 components being defective, but still six were discovered post-release. Such analyses allow us to estimate the defect rate in even good quality software, and help developers decide on when to release software, based upon estimates of the number of as yet undetected errors.

We can expect improvements in the software development process, and maturation of existing clinical products and the organizations that produce them, all to contribute in a positive way to error reduction post-implementation. Our challenge at present is that there appear to be no public mechanisms for tracking or studying clinical software errors before and after system release, making it difficult to shape policy that would support improved software quality. Sophisticated analytical techniques to model the safety profiles of ICT in use, such as accident models,²⁵α are also still not commonplace.

**Improved standards compliance**

Technical standardization improves the interoperability of disparate software systems, and minimizes the opportunity for error inherent in federated data systems, at the level of individual health services, or at a national scale. Standards for messaging, clinical documentation, and security can harness the ‘many eyes’ of the technical community who can come together to produce inherently more robust, and thus safer, systems. Certification of the software development process, and of the quality of service provided, should inherently reduce the likelihood that systems when implemented contain errors. Certification for locally implemented systems, and accredited and certified education for clinical users in system use will also help flatten growth in ICT-related harm.²⁶ However, adopting standards occurs in a resource-constrained world, and as the burden of standards compliance grows, there are penalties to be paid in what in the end is a zero-sum resources game. A wealth of standards will lead to a poverty of their implementation, to paraphrase Herb Simon’s famous aphorism.²⁸

**THE CHALLENGES OF THE DECADE AHEAD**

Predicting the actual harm rate and total patient harms that we will see through the use of ICT in healthcare over the next decade is currently not possible. However, it is realistic to make qualitative predictions, based upon those factors that are likely to dominate the patient safety equation. It is prudent to prepare for the likelihood that there will initially be a substantial increase in harm associated with health ICT over the next decade. The increased opportunity for harm arising from the increased
penetration of complex ICT into healthcare is likely to be a remarkable feature of the next few years, and it is unlikely that mitigating strategies will develop as quickly. Harm rates are likely to be compounded by systems being implemented according to artificially truncated implementation times, or being put into the hands of under-trained users. There is still a road to be traveled before we are able to construct information systems that we know are certifiably safe in the clinical workplace, and we can train clinical hands that are certified safe to use them.

Our urgent challenge is now to move beyond observing that ICT may lead to patient harm. As underscored by the IOM report on ICT safety,16 we must move to tracking true harm rates with active monitoring of incidents,27 and exploring the underlying controllability of the system. Because of its complex socio-technical nature, the health system is not easily ‘controllable’ and we need to understand the limits to our influence on health system performance, and how that shapes our responsibilities to patients, and our responses to outbreaks of ICT-related harm.

For the majority of ICT-related incidents that lead to little or no patient harm, our responsibilities are to understand the underlying root cause and eliminate or minimize future occurrences. For those hopefully rare events that may be of a catastrophic nature, we need to explore the notion of design-standardized human overrides. Patient safety is not just about studiously dissecting past events. It is also about managing events as they play out in real (dare we say ‘internet’) time. Where is the ‘kill switch’ in our health ICT systems when large-scale privacy breaches are occurring, or large volumes of critical patient data are being corrupted? Who is authorized to activate such a switch? How will clinical services operate when all their computers are temporarily shut down? These are serious issues of joint responsibility between practitioners, healthcare administrators, ICT managers and policy-makers that need to be understood.

We should not shy away from this reality. The next 10 years are going to see the fruits of many decades of hard work transforming the healthcare system through the application of ICT. The coming years, however, need to be years of caution and learning, as we institute governance systems, probably global in scale, which allow us to learn rapidly from what has gone wrong, and alert others to the risk. Most vendors sell their products in many different nations, and the lessons from a failure of a system in one country are likely to be as relevant when the same system is implemented in another. Any industry that shows that it is serious about learning, is honest and transparent about its failings, and demonstrates that it can rapidly improve when things go wrong is bound to succeed. That has been the lesson from aviation. However for some it is going to be a dangerous decade. Let us not kid ourselves that it will be anything else.

Competing interests None.

Provenance and peer review Commissioned, internally peer reviewed.

REFERENCES