A comparative review of patient safety initiatives for national health information technology

Farah Magrabi\textsuperscript{a,*}, Jos Aarts\textsuperscript{b}, Christian Nohr\textsuperscript{c}, Maureen Baker\textsuperscript{d}, Stuart Harrison\textsuperscript{d}, Sylvia Pelayo\textsuperscript{e}, Jan Talmon\textsuperscript{f}, Dean F. Sittig\textsuperscript{g}, Enrico Coiera\textsuperscript{a}

\textsuperscript{a} Centre for Health Informatics, Australian Institute of Health Innovation, The University of New South Wales, Sydney, Australia
\textsuperscript{b} Institute of Health Policy and Management, Erasmus University Rotterdam, Rotterdam, The Netherlands
\textsuperscript{c} Danish Centre for Health Informatics, Department of Development and Planning, Aalborg University, Denmark
\textsuperscript{d} Department of Health Informatics Directorate, Leeds, England, United Kingdom
\textsuperscript{e} EVALAB – INSERM CIC IT, University Hospital of Lille, University of Lille Nord de France, F-59000 Lille, France
\textsuperscript{f} Department Medical Informatics, Maastricht University, Maastricht, The Netherlands
\textsuperscript{g} University of Texas – Memorial Hermann Center for Healthcare Quality & Safety, School of Biomedical Informatics, University of Texas Health Sciences Center, Houston, TX, United States

\textbf{A R T I C L E I N F O}

Article history:
Received 1 March 2012
Received in revised form
20 November 2012
Accepted 23 November 2012

Keywords:
Health information technology
Patient safety
Oversight
Regulation
Standards
Clinical governance
e-Health
Safety governance
Internet/legislation and jurisprudence
Patient safety/legislation and jurisprudence
Internet/standards
Medical Informatics/legislation and jurisprudence
Medical Informatics/standards

\textbf{A B S T R A C T}

Objective: To collect and critically review patient safety initiatives for health information technology (HIT).
Method: Publicly promulgated set of advisories, recommendations, guidelines, or standards potentially addressing safe system design, build, implementation or use were identified by searching the websites of regional and national agencies and programmes in a non-exhaustive set of exemplar countries including England, Denmark, the Netherlands, the USA, Canada and Australia. Initiatives were categorised by type and software systems covered.
Results: We found 27 patient safety initiatives for HIT predominantly dealing with software systems for health professionals. Three initiatives addressed consumer systems. Seven of the initiatives specifically dealt with software for diagnosis and treatment, which are regulated as medical devices in England, Denmark and Canada. Four initiatives dealt with blood bank and image management software which is regulated in the USA. Of the 16 initiatives directed at unregulated software, 11 were aimed at increasing standardisation using guidelines and standards for safe system design, build, implementation and use. Three initiatives for unregulated software were aimed at certification in the USA, Canada and Australia. Safety is addressed alongside interoperability in the Australian certification programme but it is not explicitly addressed in the US and Canadian programmes, though conformance with specific functionality, interoperability, security and privacy requirements may lead to safer systems. England appears to have the most comprehensive safety management programme for unregulated software, incorporating safety assurance at a local healthcare organisation level based on standards for risk management and user interface design, with national incident monitoring and a response function.

\* Corresponding author at: Centre for Health Informatics, Australian Institute of Health Innovation, The University of New South Wales, Sydney 2052, Australia. Tel.: +61 2 9385 8694; fax: +61 2 9385 8692.
E-mail address: f.magrabi@unsw.edu.au (F. Magrabi).
1386-5056/$ – see front matter © 2012 Elsevier Ireland Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijmmedinf.2012.11.014
Conclusions: There are significant gaps in the safety initiatives for HIT systems. Current initiatives are largely focussed on software. With the exception of diagnostic, prognostic, monitoring and treatment software, which are subject to medical device regulations in some countries, the safety of the most common types of HIT systems such as EHRs and CPOE without decision support is not being explicitly addressed in most nations. Appropriate mechanisms for safety assurance are required for the full range of HIT systems for health professionals and consumers including all software and hardware throughout the system lifecycle. In addition to greater standardisation and oversight to ensure safe system design and build, appropriate implementation and use of HIT is critical to ensure patient safety.

© 2012 Elsevier Ireland Ltd. All rights reserved.

1. Introduction

1.1. HIT can pose a risk to patient safety

The safety of health information technology (HIT) needs to be urgently addressed [1,2]. HIT broadly includes computer hardware and software used by health professionals and consumers to support care. Evidence that problems with HIT can pose a risk to patient safety is emerging even though such systems are central to improving the safety and quality of health services [3-8]. For instance, there were 42 reports of patient harm and four deaths in 436 critical incidents involving HIT that were reported to the US Food and Drug Administration (FDA) over a 30-month period ending July 2010 [5]. HIT problems also disrupt clinical work contributing to new types of errors leading to delays and re-work [4,9-12]. Safety issues involving information technology are not unique to healthcare [13], but this sector has lagged behind other industries in addressing such problems [2].

1.2. Background: safety needs to be addressed throughout the system cycle

Safety is an emergent system property and needs to be addressed throughout the lifecycle of HIT systems [14]. The safety of patients is not solely dependent upon HIT systems on their own but is influenced by their interactions with users and other technology in a given environment [15]. Patients are harmed when interactions between system components (human and machine) create unsafe states [3]. As safety is inextricably linked to how a system operates, safety considerations should be at the forefront of design and build processes.

All the possible interactions among system components are not predictable at design, especially when HIT are used in context of a broader sociotechnical system. In large complex systems, safety problems tend to emerge from unexpected interactions between system components. Therefore safety must also be addressed during and post system implementation. The potential for unsafe interactions needs to be investigated when HIT are integrated with local clinical workflows including other technology and the organisational structure. Beyond implementation any unsafe interactions that emerge during routine use need to be detected and mitigated by monitoring for critical incidents involving patient harm (adverse events) and near misses.

1.3. Ensuring the safety of HIT

Historically HIT has not been subject to regulation. In particular standalone software systems (i.e. software not embedded in hardware) such as electronic health records (EHR) or computerised provider order entry (CPOE) systems have not been subject to regulatory requirements whereas software that is part of a medical device is regulated [16]. With the increasing proliferation of HIT, the safety of software is at last being addressed within large national programmes in many countries. Examples of such programmes are the National Health Service (NHS) Connecting for Health (CfH) programme in England; the American Reinvestment and Recovery Act (ARRA) “meaningful use” programme for adoption and use of EHRs; and the Australian Government’s Personally Controlled Electronic Health Record System that was launched in 2012.

Little has been published about HIT safety initiatives. Recommended strategies to address software safety are largely based upon increasing standardisation and introducing mechanisms for oversight [2,17,18], though some argue that such measures may hamper innovation [19]. The recently revised European Union (EU) Medical Device Directive 93/42/EC (MDD) considers certain standalone software for diagnosis, prognosis, treatment and monitoring as medical devices and has become mandatory [20]. A directive is a type of legislation issued by the EU which sets out certain end results that must be achieved in every member country. As directives are not self-executing each country within the EU is now required to implement the MDD within their national regulations. In this paper we thus set out to collect and critically review current national initiatives for HIT relevant to improving patient safety.

2. Methods

We defined HIT safety initiatives as any publicly promulgated set of advisories, recommendations, guidelines, or standards potentially addressing safe system design, build, implementation or use. Using a broad definition of HIT we included, “computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making” [21]. To understand the full range of initiatives a non-exhaustive set of exemplar countries was selected by the authors (England, Denmark, the Netherlands, the USA, Canada and Australia).
The websites of national agencies and programmes were searched including the NHS CfH programme in England [22], the European Commission’s Directorate general for health and consumers [20], the Danish Patient Safety Database [23], the Dutch Health Care Inspectorate [24], the US Office of the National Coordinator for HIT [25], the US FDA [26], Health Canada [27], Canada Health Infoway [28], and the Australian National e-Health Transition Authority [29]. Initiatives were categorised by type and software systems covered.

3. Results

We found 27 safety initiatives for HIT across the six nations examined (Table 1). England had eight initiatives and the USA had nine. HIT safety initiatives predominantly dealt with software systems for health professionals while hardware was implicitly addressed. For example, requirements for appropriate hardware were included within guidance for implementing electronic medication management systems [30] or managing the risks of EHRs [21]. Seven initiatives dealt with software for diagnosis and treatment, which is regulated as a medical device in England, Denmark and Canada. Four initiatives dealt with blood bank and image management software which are regulated in the USA, and 16 were directed at unregulated software. More than half of the initiatives (n = 16) were directed at increasing standardisation including guidance, standards and regulation-mandated standards (Table 2). The remaining initiatives were concerned with providing oversight using certification, regulation and incident monitoring. Only three initiatives addressed consumer systems.

3.1. Standardisation

Guidelines and standards can be applied at many different points in the lifecycle of HIT, from design, to build, to implementation and use in a clinical setting, and can be informed guidance or become mandatory standards. There are a range of international standards for HIT, for this review we chose to focus upon standards and guidelines for patient safety.

3.1.1. Guidelines

Efforts to promote safe design and implementation of software have largely relied on guidance for manufacturers and healthcare organisations. With a specific focus on the safety of user interactions the English NHS CfH Common User Interface programme has developed interface design guides for the display of patient identifiers, clinical notes, medications and navigation [34]. Guides for patient demographics will become mandatory NHS standards in December 2015. The CfH programme has also developed guides for design and implementation of software based upon their standards (discussed in Section 3.1.2) [35,36]. A similar guide for implementing hospital medication management systems was released by the Australian Safety Commission in 2011 [30].

In the USA, the 2011 Agency for Healthcare Research and Quality (AHRQ) guide addresses safety risks as part of reducing the broader unintended consequences of EHR implementation [21]. The FDA also provides guidance for validation of software by manufacturers [42], with a particular focus on the implementation and use of blood bank software [43] and image management systems [44]. Considering safety in the broader context of usability the US National Institute of Standards and Technology (NIST) published a guide to evaluate EHR usability in 2012 [40]. The NIST guide is specifically focused on improving safety by encouraging user centred development processes. It proposes formative usability evaluation by experts and summative testing in the hands of users incorporating a risk-based approach to examining usability problems. NIST has also published consensus recommendations for critical user interactions influencing the usability and safety of paediatric EHRs [41]. While improved usability can contribute to safety a high usable system is not necessarily safe [47].

3.1.2. Standards

We found only three standards that formally address the safety of software that is not subject to regulatory requirements. Along with standards for patient demographics, the English CfH programme has implemented two standards for risk management in software design, implementation and use [37,38]. 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. Based upon these standards the CfH Clinical Safety Management System requires manufacturers and health organisations to demonstrate safe design and implementation practices. An internal assurance process encompasses hazard assessment, a safety case and safety closure report. It should be noted that the NHS standards were originally proposed as ISO standards in 2008 but were withdrawn before they were put up for ballot. The ISO is currently working on ISO/TR 17791 Health informatics – Guidance on standards for enabling safety in health software, which will provide recommendations on best practices in assuring the safer implementation of software, irrespective of whether it is regulated as a medical device.

3.1.3. Regulation mandated standards

For software formally regulated as a medical device (see Section 3.2.2) international standards for usability, risk management and networks are mandatory [31–33].

3.2. Oversight

As with medical devices, certification and regulation offer formal mechanisms to assure the safety and effectiveness of standalone software (e.g. an EHR or CPOE). Certification can provide independent assurance for specific software requirements. Regulation, on the other hand, 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. In general the level of oversight or regulatory control should be proportional to the degree of risk that the software poses to patients. Beyond the stages of design and implementation, incident monitoring is a mechanism to track any emergent safety problems associated with routine use of HIT. For the initiatives we reviewed it was
<table>
<thead>
<tr>
<th>Safety initiative</th>
<th>Software covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>European Union</strong></td>
<td>Diagnosis and treatment software</td>
</tr>
<tr>
<td>b Medical devices – application of risk management to medical devices (EN International Organisation for Standardisation, ISO 14971: 2007) [31]</td>
<td></td>
</tr>
<tr>
<td>b Medical devices – application of usability engineering to medical devices (International Electrotechnical Commission, IEC 62366:2007) [32]</td>
<td></td>
</tr>
<tr>
<td>b Application of risk management for IT-networks incorporating medical devices (IEC 80001: 2010) [33]</td>
<td></td>
</tr>
<tr>
<td>Revised Medical Device Directive 93/42/EC [20]</td>
<td></td>
</tr>
<tr>
<td><strong>England</strong></td>
<td></td>
</tr>
<tr>
<td>The National Health Service (NHS) Connecting for Health (CFH) Common User Interface programme [34]</td>
<td>All software delivered through NHS CFH contracts (except regulated software i.e. for diagnosis and treatment)</td>
</tr>
<tr>
<td>Safer Design: Clinical Risk Guidance Document [36]</td>
<td></td>
</tr>
<tr>
<td>Health Informatics – Application of clinical risk management to the manufacture of health software [37]</td>
<td></td>
</tr>
<tr>
<td>Health Informatics – Guidance on the management of clinical risk relating to the deployment and use of health software [38]</td>
<td></td>
</tr>
<tr>
<td>Common User Interface standards for patient identifiers [34]</td>
<td></td>
</tr>
<tr>
<td>NHS CFH clinical safety management system incl. incident monitoring [22]</td>
<td></td>
</tr>
<tr>
<td>UK Medical Device regulations [39]</td>
<td>Diagnosis and treatment software</td>
</tr>
<tr>
<td><strong>Denmark</strong></td>
<td>Diagnosis and treatment software</td>
</tr>
<tr>
<td>Danish Patient Safety Database [23]</td>
<td></td>
</tr>
<tr>
<td><strong>Netherlands</strong></td>
<td>All patient safety incidents</td>
</tr>
<tr>
<td>Health Care Inspectorate [24]</td>
<td></td>
</tr>
<tr>
<td><strong>USA</strong></td>
<td>EHRs</td>
</tr>
<tr>
<td>Technical Evaluation, Testing and Validation of the Usability of Electronic Health Records [40]</td>
<td>Paediatric EHRs</td>
</tr>
<tr>
<td>Human Factors Guide to Enhance EHR Usability of Critical User Interactions when Supporting Paediatric Patient Care [41]</td>
<td>All healthcare software</td>
</tr>
<tr>
<td>General Principles of Software Validation: Final Guidance for Industry and Food and Drug Administration (FDA) Staff [42]</td>
<td>Blood bank software</td>
</tr>
<tr>
<td>Guidance for the Submission of Premarket Notifications for Medical Image Management Devices [44]</td>
<td>EHR; prescribing systems</td>
</tr>
<tr>
<td>Certification for meaningful use including the Certification Commission for Health Information Technology (CCHIT) programme [45]</td>
<td>Reports about medical devices</td>
</tr>
<tr>
<td>FDA Manufacturer and User Facility Device Experience database [46]</td>
<td>Mobile applications incl. consumer applications</td>
</tr>
<tr>
<td>Draft Guidance for Industry and FDA Staff – Mobile Medical Applications [26]</td>
<td></td>
</tr>
<tr>
<td><strong>Canada</strong></td>
<td>Registries: client, provider, immunisation; consumer systems; diagnostic imaging; drug information systems; EHRs</td>
</tr>
<tr>
<td>a Canada Health Infoway [28]</td>
<td>Diagnosis and treatment software incl. consumer systems.</td>
</tr>
<tr>
<td><strong>Australia</strong></td>
<td>Medication management systems</td>
</tr>
<tr>
<td>National e-Health Transition Authority Compliance, Conformance and Accreditation programme [29]</td>
<td></td>
</tr>
</tbody>
</table>

\[\text{a} \text{ Initiatives that do not directly address patient safety.}\]

\[\text{b} \text{ Global standards that are mandatory in the EU.}\]

usually mandatory to report incidents associated with regulated software whereas the reporting of general patient safety incidents (including those involving unregulated software) by healthcare professionals was voluntary.

3.2.1. Certification

We found HIT certification programmes in three nations, however safety was explicitly addressed in only one programme. US certification programmes are focussed around the
meaningful use of EHRs. The Office of the National Coordinator for HIT has authorised six testing and certification bodies including the Certification Commission for Health Information Technology (CCHIT) to support the ARRA programme. A second CCHIT programme covers functionality, interoperability, and security for EHRs in ambulatory, inpatient, emergency, behavioural health and long-term care; and electronic prescribing [45]. It requires key aspects of successful use to be verified at live sites. For ambulatory EHRs, usability is assessed by expert review using validated instruments (e.g. After Scenario Questionnaire, Perceived Usability Questionnaire and System Usability Survey [48]). Professional training and certification for EHR use are another response to ARRA (e.g. www.healthtccertification.com).

Focusing on a broader range of software the Canadian Health Infoway’s (Infoway) certification programme includes consumer software, shared records, EHRs and core modules including medications, imaging, and registries for patients, providers and immunisations [28]. Infoway’s certification criteria focus on privacy, security, and interoperability based on international and Canadian standards. A fourth set of criteria focusing on manufacturer practices for managing risk, data, system security, as well as third party solutions and services is noteworthy from a safety perspective. Risk management is based upon Canadian Standards Association’s Risk Management guidance and international IT governance standards. The programme requires manufacturers to report all changes to certified software and report incidents involving the software. In Australia, the National e-Health Transition Authority has established a Compliance, Conformance and Accreditation programme to oversee a national framework for assurance with respect to clinical safety alongside interoperability and security [29].

### 3.2.2 Regulation

Although HIT (i.e. standalone software) has largely been outside the strict regulatory regimen applied to medical devices, current initiatives indicate a gradual move towards regulation. In the EU the safety of medical devices is regulated through a directive that focuses on proper manufacturing and pre-market testing leading to a declaration of conformity [49,50]. Each member state is required to appoint a Competent Authority who is responsible for implementing the requirements of the Directive. For example, in the Netherlands the Health Care Inspectorate is entrusted with this responsibility and the Medicines and Healthcare products Regulatory Agency fulfils this role in England.

The revised EU MDD considers standalone software intended by its manufacturer to be used for, “(a) diagnosis, prevention, monitoring, treatment or alleviation of disease, (b) diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, (c) investigation, replacement or modification of the anatomy or of a physiological process,” as a medical device in its own right [20]. Such software or devices incorporating software are required to be validated in accordance with state of the art processes for software development, risk management, validation and verification. The MDD explicitly mentions the role of clinical evaluation for proving that the device is safe and meets the stated objectives. While patient safety considerations are part of the essential requirements, usability considerations are implicit. The directive states that software should minimise risks of use error using ergonomic features in context of the operating environment. Manufacturers must (i) adopt a usability engineering process during design and development; (ii) document the process; and (iii) ultimately prove the “ergonomic quality” (usability) of the device. Technical documentation must include the usability engineering process based on the IEC 62366:2007 standard [27], which relies on widely accepted usability methodologies [e.g. ISO 9241-210:2010].

Follow-up guidance to the MDD (MEDDEV 2.1/6) was published in early 2012 and provides a flowchart to help decide whether or not standalone software should be considered as a medical device [51]. Software that merely stores, archives or communicates clinical information (e.g. an EHR) is not considered as medical devices. However decision support modules which combine medical knowledge databases and algorithms with patient specific data to provide recommendations for diagnosis, prognosis, monitoring and treatment of individual patients are considered as devices. Image viewers, medication modules and software that generates alarms based on the monitoring and analysis of patient specific physiological parameters are also considered as devices.

The MDD applies across the EU, yet regulators in different member states interpret it in differing fashions. In England, software qualifies as a medical device if a clinician relies on its output (e.g. a radiotherapy treatment planning system) and it is regulated by the Medicines and Healthcare products

<table>
<thead>
<tr>
<th>Table 2 – National and regional HIT safety initiatives by type.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Country/region</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>European Union</td>
</tr>
<tr>
<td>England</td>
</tr>
<tr>
<td>Denmark</td>
</tr>
<tr>
<td>Netherlands</td>
</tr>
<tr>
<td>USA</td>
</tr>
<tr>
<td>Canada</td>
</tr>
<tr>
<td>Australia</td>
</tr>
</tbody>
</table>

* Initiatives that do not directly address patient safety.
Regulatory Agency. For example, software intended to enhance images from an X-ray or ultrasound is considered a medical device.

Health Canada similarly announced the regulation of specific software as medical devices in 2010. In this regimen software used to store, acquire, transfer, or view clinical data or images is considered as a Class I device, and Class II if it manipulates the data and images upon which clinical decisions are based. Software that simply replaces patients’ paper records is excluded if it is only intended to store and view patient information (for example: age, weight, notes about patients’ appointments, test results, order processing, scheduling, or managing patient movements). Software that (i) performs administrative calculations and manipulations (e.g. appointment and workflow management systems); or (ii) connects two or more HIT applications (i.e. middleware) so that they can exchange data is also excluded. As for consumer HIT, software used to manage data (e.g. blood pressure, spirometry) from patients’ homes is classified as a Class II device if it is used to analyse data for diagnosis and treatment, and Class I if it only transmits and stores the data.

At present there is considerable debate in the USA about the FDA’s role in regulating HIT [52,53]. Under the Federal, Food, Drug, and Cosmetic Act, HIT are considered as medical devices. However, the FDA does not currently enforce its regulatory requirements with respect to HIT. In 2011, the FDA moved towards enforcing its regulatory requirements with respect to software for mobile platforms (e.g. smartphones and tablet computers). Specifically, applications (apps) for mobile platforms which are used as an accessory to a currently regulated device (e.g. an app to view medical images on an iPad and make a diagnosis) or transform a mobile platform to a device (e.g. “an app that turns a smartphone into an electrocardiography, or ECG, machine to detect abnormal heart rhythms or determine if a patient is experiencing a heart attack.”).

3.2.3. Incident monitoring

The monitoring of critical incidents is central to detecting emerging problems in mainstream patient safety programmes which are now well-established in most developed nations [54]. The only large-scale programme directed at monitoring and responding to HIT incidents is part of the English NHS Clinical Safety Management System which has been in place since 2005 and has handled more than 900 incidents reported by health organisations and manufacturers. Yet HIT incidents are also being reported among general patient safety incidents. An analysis of 40,000 incidents submitted by health professionals to a state-wide incident monitoring system in Australia yielded 99 HIT-related incidents associated with 32 categories of safety problems [4]. Another potential source of HIT incidents are reports about medical device failure and hazards submitted by users and manufacturers. One source of such reports is the US FDA Manufacturer and User Facility Device Experience database. Although the FDA does not enforce its regulatory requirements with respect to HIT, some manufacturers have voluntarily listed their systems and reported incidents. A search of almost 900,000 reports from January 2008 to July 2010 yielded 436 incidents, of these 11% were associated with patient harm including four deaths [5,6].

To facilitate the reporting of such incidents the US AHRQ has included categories for HIT in its new standard for reporting hazardous events called the “common format” [55]. The AHRQ has also developed and tested a comprehensive software tool to support detection and management of hazards throughout the HIT lifecycle. 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 organisation using the same software and, by vendors and policymakers [56].

The Danish Patient Safety Database is another example which has collected reports about adverse events from clinicians since 2004 [23]. In addition to medical devices the system collects reports about, “software necessary for its proper application intended by the manufacturer to be used for human beings for the purpose of: diagnosis, prevention, monitoring, treatment or alleviation of disease” [57]. It does not have an inbuilt coding system for automatic identification of incidents involving HIT and was opened up to reporting by patients and their relatives in 2011. In the Netherlands, HIT safety problems are addressed on a case-by-case basis by the Health Care Inspectorate and no provision exists for collection of incidents involving HIT [24].

4. Discussion

4.1. Current safety initiatives

We found that current national safety initiatives for HIT are largely focussed upon software for health professionals. Standalone software that is “intended by its manufacturer to be used specifically for diagnostic, prognostic, monitoring and/or therapeutic purposes” is subject to regulatory oversight [20]. Where enforced, only a small subset of software is legally required to be safe, the vast majority of common HIT systems such as EHRs and CPOE without decision support are seen to be outside this subset (Fig. 1). For such unregulated software, safety initiatives aim to increase standardisation.
using guidelines and standards to ensure safe design, build, implementation and use. Our review identified 11 such initiatives [21,30,34–38,40–42]. At present most certification programmes for unregulated software do not explicitly address safety, although improvements to specific functionality, interoperability, security and privacy requirements may indirectly lead to safer systems [28,29,45]. At the time of writing England appears to have the most comprehensive safety management programme for unregulated software, incorporating safety assurance at a local healthcare organisation level based on standards for risk management and user interface design, with national incident monitoring and a response function. However the effectiveness of such initiatives is not known and further research is required to evaluate their impact on minimising risks to patients.

4.2. Improving oversight of HIT

Certification and regulation offer two mechanisms to improve oversight of software. Canada has announced regulation of a select group of software very similar to the new EU device directive. The US Institute of Medicine (IOM) report recommended compulsory registration of all manufacturers and public listing of HIT systems with the Office of the National Coordinator which is already administering EHRs as part of the meaningful use programme [2]. Secondly it recommended mandatory adoption of quality management and risk management principles in processes to build HIT systems based upon ISO standards with a particular focus on human factors, safety culture, and usability. Thirdly the IOM called for oversight to ensure compliance along with mandatory manufacturer and voluntary user reporting of HIT related patient safety incidents including aggregation, analysis, and investigation by an independent body. The IOM recommendations to monitor and publicly report progress towards safety at the top level, and to direct the FDA to develop a regulatory framework seem to indicate that regulation is inevitable in the USA.

National safety initiatives need to address a broad range of HIT including consumer systems. While it is appropriate to deal with specific software systems (e.g. e-prescribing) for certification of particular functionality, safety assurance is required for all software and interactions at a system level. For instance, software intended to store patients’ demographic details and appointment schedule (currently excluded in the EU directive and the Canadian regulatory regimen) may pose risks if data corruption results in a failure to follow-up on an abnormal test result indicating a potential cancer [58]. Moreover software systems are usually interconnected i.e. software storing demographic details may provide input to a safety critical prescribing module. Therefore even software that is merely ‘storing’ patient information requires safety assurance even though it may not be appropriate to subject such systems to full regulation. Ultimately the level of oversight should be proportional to the risk posed by HIT.

Safety assurance also needs to be extended to the hardware that hosts software. In an analysis of 712 HIT problems reported to the US FDA 16% directly involved computer hardware [6]. In general, hardware and network configurations across disparate organisations and clinical settings are likely to be highly heterogeneous. While existing standards for risk management (such as the IEC80001) can be applied to networks, standardisation of hardware and operating systems may prove to be more challenging. One strategy is to design software with the ability to detect and activate pre-defined corrective or fail-safe responses in the event of hardware or network failures [59]. In this regard HIT safety efforts can be usefully informed by the experience of implementing computer systems in other safety critical industries [14,60–62].

4.3. Need for HIT specific standards

The effectiveness of any mechanism to improve oversight is contingent on sound certification criteria and safety standards. Patient safety is currently on the agenda of the ISO and the European Committee for Standardisation (CEN) Technical Committees on Health Informatics. A new technical report providing guidance on standards for safety in design, implementation and use of software is scheduled for release in 2013. While existing standards for the safe design and use of medical devices might be a good starting point, there is a need for HIT specific standards for development, evaluation and post-market surveillance of software. For instance, hazard assessment techniques need to focus on identifying classes of HIT specific errors [3–6]. There is a need for suitable approaches to interface design as well as methods to ensure that the implemented interfaces are indeed safe to use. The question arises whether approaches, which are proposed as means to develop software that will meet users’ requirements (e.g. Agile approaches like Scrum [63]), are sufficiently grounded in safety principles.

4.4. Beyond certification and regulation – ensuring safe operation

Regulation and certification of software will not address safe implementation and use of HIT within the context of clinical work processes and the underlying IT infrastructure (i.e. hardware) as this must be addressed locally by the organisation implementing and using the technology [64]. For instance, a certified CPOE system can pose a risk to patient safety due to a range of local issues including if: (i) it is not available; (ii) it cannot reliably communicate with the local EHR system; (iii) there is a mismatch between the system and actual clinical work process; or (iv) users are not adequately trained (use error) [7]. Currently the approach to safety in implementation is through guidelines, with the exception of the English standard for risk management. However there are no guides about safe system use and further research is required to address this gap. One possible way to address safe use and operation is to incorporate specific use requirements into existing accreditation of health organisations’ safety practices (e.g. the US Joint Commission’s safety standards [65]).
5. Conclusions

There are significant gaps in safety initiatives for HIT systems. Current initiatives are largely focussed on software for health professionals. With the exception of diagnostic, prognostic, monitoring and treatment software, which is subject to medical device regulations in some countries, the safety of the majority of all types of HIT is not being explicitly addressed in most nations. England appears to have the most comprehensive programme explicitly addressing the safety of unregulated software. Appropriate mechanisms for safety assurance are required for all types of HIT systems for health professionals and consumers including all software and hardware throughout the system lifecycle. In addition to greater standardisation and oversight to ensure safe design and build, appropriate implementation and use is critical to ensure patient safety.

Authors' contributions

This paper emerged from a workshop on the, “Safety of health information technology: Identifying and mitigating risks” by FM, JA, Marie-Catherine Beuscet-Zephir and CN at the XXIII International Conference of the European Federation for Medical Informatics (EFMI), 28–31 August 2011. FM, EC, JA and CN conceptualised the study; all authors contributed to collating the safety initiatives, and the analysis and interpretation of findings. FM drafted the initial version. All the authors contributed to subsequent versions and gave final approval.

Conflict of interest

MB is Clinical Director for Patient Safety and SH is a Lead Safety Engineer at NHS Connecting for Health, Department of Health Informatics Directorate in England. The other authors have no conflict of interest to declare.

Acknowledgements

This research is supported in part by grants from the Australian National Health and Medical Research Council (NHMRC) Program Grant 568612 and Project Grant 630583. The funding sources did not play any role in the study design, in the collection, analysis and interpretation of data; in the writing of the manuscript; and in the decision to submit the manuscript for publication.

The authors wish to thank Tim Cheeran, Stephen Corbett and Don Newsham for information about the English and Canadian initiatives; and Dr David Greenfield his valuable advice. We also wish to thank the EFMI Working Group on Human and Organisational Factors of Medical Informatics and participants of the workshop at the 2011 EFMI meeting.

REFERENCES


Summary points

What was already known on the topic:

- Alongside benefits health information technology (HIT) can pose risks to patient safety.
- The safety of HIT needs to be urgently addressed.

What this study added to our knowledge:

- There are significant gaps in patient safety initiatives for HIT.
- Current safety initiatives are largely focused on software.
- The safety of the most common types of HIT systems such as EHRs and CPOE without decision support is not being explicitly addressed in most nations.
- Greater standardisation and oversight is required to ensure safety throughout the lifecycle of all types of HIT systems for health professionals and consumers including all software and hardware.


