Clinical safety of England's national programme for IT: A retrospective analysis of all reported safety events 2005 to 2011

Farah Magrabi [a,*], Maureen Baker [b], Ipsita Sinha [c], Mei-Sing Ong [a], Stuart Harrison [b], Michael R. Kidd [d], William B. Runciman [e,f], Enrico Coiera [a]

[a] Centre for Health Informatics, Australian Institute of Health Innovation, Macquarie University, Australia
[b] Health and Social Care Information Centre, Leeds, England
[c] Oxford University NHS Trust, England
[d] Faculty of Medicine, Nursing and Health Sciences, Flinders University, Australia
[e] The School of Psychology, Social Work & Social Policy, University of South Australia, Australia
[f] Australian Patient Safety Foundation, Adelaide, Australia

ARTICLE INFO

ABSTRACT

Objective: To analyse patient safety events associated with England's national programme for IT (NPfIT).

Methods: Retrospective analysis of all safety events managed by a dedicated IT safety team between September 2005 and November 2011 was undertaken. Events were reviewed against an existing classification for problems associated with IT. The proportion of reported events per problem type, consequences, source of report, resolution within 24 h, time of day and day of week were examined. Sub-group analyses were undertaken for events involving patient harm and those that occurred on a large scale.

Results: Of the 850 events analysed, 68% ($n = 574$) described potentially hazardous circumstances, 24% ($n = 205$) had an observable impact on care delivery, 4% ($n = 36$) were a near miss, and 3% ($n = 22$) were associated with patient harm, including three deaths (0·35%). Eleven events did not have a noticeable consequence (1%) and two were complaints (<1%). Amongst the events 1606 separate contributing problems were identified. Of these 92% were predominately associated with technical rather than human factors. Problems involving human factors were four times as likely to result in patient harm than technical problems (25% versus 8%; OR 3·98, 95%CI 1·90–8.34). Large-scale events affecting 10 or more individuals or multiple IT systems accounted for 23% ($n = 191$) of the sample and were significantly more likely to result in a near miss (6% versus 4%) or impact the delivery of care (39% versus 20%; $p < 0·001$).

Conclusion: Events associated with NPfIT reinforce that the use of IT does create hazardous circumstances and can lead to patient harm or death. Large-scale patient safety events have the potential to affect many patients and clinicians, and this suggests that addressing them should be a priority for all major IT implementations.

© 2015 Elsevier Ireland Ltd. All rights reserved.

* Corresponding author. Tel.: +61 298502429.
  E-mail address: farah.magrabi@mq.edu.au (F. Magrabi).

1. Introduction

Healthcare systems worldwide are confronted with the twin challenges of reaping the benefits of information technology (IT) whilst minimising risks to patients [1,2]. While IT innovations offer many benefits through improved management of health information, any new development has the potential to introduce new errors and risks into healthcare delivery [3]. Risks to patients can arise from problems with the IT systems themselves, the way they are implemented, and how they are used; many only become apparent when systems are deployed [2].

Implementation of IT at a national level poses particular risks because of the scale and scope, and the inherent complexity of connecting many often different systems [1]. England's national programme for IT (NPfIT) was arguably the world's largest single health IT project, but its costs and benefits remain controversial [4–7]. While there have been some reports of technical failure [8], no systematic assessment has yet been made of risks to patients in NPfIT. In particular, implementations on a large scale such as NPfIT may introduce risks that could affect many patients simultaneously [1], and these have not previously been examined.

Incident reports are a crucial early source of information about safety problems. They have proved invaluable in identifying emerging risks and harm in many patient safety domains (e.g. medications [9], falls [10]), including the risks of IT systems [11,12]. We have previously examined incidents associated with IT from a state-wide incident monitoring system in Australia and those reported to the US Food and Drug Administration (FDA) [13,14]. These studies have helped us understand the types of safety problems associated with IT and their consequences. The objectives of the current study are for the first time, to analyse all reported safety events from across the English National Health Service (NHS) to understand the nature of the risks associated with NPfIT, and to determine whether national IT programmes such as NPfIT pose special risks because of their large scale. Unlike routine incident reporting, the events examined in this study represent all known problems with national scale IT systems that impacted patient safety and that were addressed by a dedicated safety team.

2. Methods

2.1. Setting

As part of NPfIT a range of national scale IT systems was gradually implemented across the NHS from 2003 onwards [15]. The NHS serves a population of 53 million and health services are provided by public sector organisations called trusts [16]. In primary care, the national-scale IT systems supported the electronic transfer of prescriptions to pharmacies, notes between GP surgeries, and electronic referrals for outpatient appointments. A summary care record of medicines, allergies and adverse reactions supported emergency and out-of-hours care and was accessible to patients. In acute care the implementation focussed on electronic medical records, and picture archiving and communication systems (PACS). Other components of the IT infrastructure included fast broadband networking and email.

The monitoring of safety events relating to the national-scale IT systems was an integral component of the NHS's *clinical safety management system* which was a formal process that was set up in 2005 to provide safety assurance and is described in detail elsewhere [17]. As part of the safety management system a dedicated *IT safety team* made up of safety engineers, clinical safety officers, clinicians and clinical safety analysts was available 24 h a day, 7 days a week to respond to reports about events involving all national-scale IT systems. We examined all 899 reports managed by the IT safety team between September 2005 and November 2011. Of these 404 were forwarded by a *national IT help desk* which was responsible for the triage of reports so that only serious issues were referred to the safety team. For instance, a problem with a login or password would be resolved at the national IT help desk. As a benchmark 10,250 issues were logged by the national IT help desk between November 2006 and November 2011. The national help desk was also available 24 h a day, 7 days a week. Events were reported by clinicians (i.e. healthcare professionals), IT system vendors or were escalated from local IT help desks within trusts. Reporters also submitted events directly to the safety team by phone or email. The safety team logged the reports in an event database and sought to address problems within 24 h of receiving a report. The event database was maintained using the Hewlett Packard Quality Centre. It was independent of the National Reporting and Learning System (NRLS) that was used to monitor patient safety events in all clinical domains, although some IT events could also be reported to the NRLS [18]. Events associated with local clinical IT systems within trusts which were not part of the national infrastructure were not captured by the national IT helpdesk or the safety team.

2.2. Data source

Event reports consisted of five structured and two free text fields to describe the problem and its consequences along with any supporting material (e.g. computer screenshots, Appendix A). An event could contain multiple problem descriptions. All reports were screened and 24 duplicate entries in the database were removed. Multiple reports that related to the same event were grouped (i.e. 850 events were described in 875 reports).

2.3. Classification of problems

The events were categorised using an existing classification for safety problems associated with health IT systems that was developed by the authors (Fig. 1, Appendix B).[13,14]. Problems were first divided into those primarily involving *human factors* or *technical* problems, and then assigned to one or more subclasses. Human factors problems related to interaction of humans with IT. The type of use error as well socio-technical contextual variables that contributed to events were examined (e.g. training, cognitive load and clinical workflow) [19,20]. For problems falling into the technical space, the type of machine error and technical problems including a range of hardware and software issues were examined. After analysis of 25% of