An analysis of computer-related patient safety incidents to inform the development of a classification

Farah Magrabi,[1] Mei-Sing Ong,[1] William Runciman,[2,3] Enrico Coiera[1]

► Additional appendices are published online only. To view these files please visit the journal online (www.jamia.org).

[1]Centre for Health Informatics, University of New South Wales, Sydney, Australia
[2]Australian Patient Safety Foundation, Adelaide, Australia
[3]School of Psychology, Social Work and Social Policy, University of South Australia, Adelaide, Australia

Correspondence to
Dr Farah Magrabi, Centre for Health Informatics, University of New South Wales, Sydney, 2052 Australia; f.magrabi@unsw.edu.au

Received 30 November 2009
Revised 1 September 2010
Accepted 3 September 2010

ABSTRACT

Objective To analyze patient safety incidents associated with computer use to develop the basis for a classification of problems reported by health professionals.

Design Incidents submitted to a voluntary incident reporting database across one Australian state were retrieved and a subset (25%) was analyzed to identify 'natural categories' for classification. Two coders independently classified the remaining incidents into one or more categories. Free text descriptions were analyzed to identify contributing factors. Where available medical specialty, time of day and consequences were examined.

Measurements Descriptive statistics; inter-rater reliability.

Results A search of 42 616 incidents from 2003 to 2005 yielded 123 computer related incidents. After removing duplicate and unrelated incidents, 99 incidents describing 117 problems remained. A classification with 32 types of computer use problems was developed. Problems were grouped into information input (31%), transfer (20%), output (20%) and general technical (24%). Overall, 55% of problems were machine related and 45% were attributed to human–computer interaction. Delays in initiating and completing clinical tasks were a major consequence of machine related problems (70%) whereas rework was a major consequence of human–computer interaction problems (78%). While 38% (n=26) of the incidents were reported to have a noticeable consequence but no harm, 34% (n=23) had no noticeable consequence.

Conclusion Only 0.2% of all incidents reported were computer related. Further work is required to expand our classification using incident reports and other sources of information about healthcare IT problems. Evidence based user interface design must focus on the safe entry and retrieval of clinical information and support users in detecting and correcting errors and malfunctions.

INTRODUCTION

Patient safety risks and incidents caused by problems with the use of computers are now widely recognized as an unintended consequence of healthcare information technology (IT),[1–3] just as 'revenge effects' have been described after other system changes.[4] A definition of a patient safety incident is 'an event or circumstance which could have resulted, or did result, in unnecessary harm to a patient'.[5] In this study we focus on patient safety incidents involving problems with the use of IT or 'computer-related incidents.'

Although evidence about the risks associated with healthcare IT is scarce, the available data suggest that it can pose a significant risk to patient safety. In February 2010, the US Food and Drug Administration (FDA) reported receiving information on 260 incidents with potential for patient harm including 44 injuries and six deaths.[6] This FDA report is based on incidents that cover all healthcare IT, including related devices. In 2008, the US Joint Commission on Accreditation of Healthcare Organizations (JCAHO) published a new Sentinel Events alert, providing general guidance to minimize risks through safe design, implementation, and use of IT to support clinical work.[7] While such general guidance is a useful first step to enhancing patient safety, the lack of specific information about the underlying causes of computer-related incidents and the severity of their impact means that it is currently not possible to prioritize corrective strategies for safety-critical risks of healthcare IT systems.

There has been some qualitative investigation of the problems arising from the use of IT in healthcare across the United States, the Netherlands, and Australia. Ash *et al*[1] distinguished two high level categories of process errors—those related to entering and retrieving information, and those related to communication and coordination. A similar categorization was used by Koppel *et al*[8] to describe the causes of 22 types of medication error specifically associated with computerized physician order entry (CPOE) systems at one US hospital. The study found that errors in the process of entering and retrieving information were largely due to a mismatch between workflow and the system model. Errors in the process of communication and coordination, on the other hand, were attributed to data fragmentation and lack of integration with other hospital systems. Other studies have identified unintended effects of CPOE implementation including: (1) extra work for clinicians; (2) unfavorable workflow changes; (3) endless demands to change hardware and software; (4) problems related to paper persistence; (5) degradation in communication patterns and practices; (6) negative emotions; (7) unexpected changes in the power structure; and (8) overdependence on IT systems.[9 10]

The impact of computer use on patient safety is less well understood. Weiner and colleagues[11] have used the term 'e-iatrogenesis' to describe patient harm resulting from the use of IT systems. Focusing on hospital-based systems, one study documented high rates of adverse drug events with CPOE in a VA hospital.[12] Another examination of a commercial CPOE system in a US pediatric hospital found a significant increase in patient deaths following rapid implementation over 6 days, associated with not ensuring optimal integration of the system into clinical workflow.[13 14] In another investigation, Horsky *et al* found that the absence of multiple system safeguards to check for the type of drug and dose at successive stages of the medication process contributed to a serious error.[15] Singh and colleagues found that 20% of 532 errors resulting from inconsistent entry of dosage information within a CPOE could have resulted in moderate to severe harm.[16]

Reports of patient safety incidents paint a broader picture. In 2006 almost 25% of 176 409 medication errors reported to the United States Pharmacopeia voluntary incident reporting database were computer related.[7] In 2003, 7029 CPOE-related medication incidents were reported, 0.1% of which resulted in harm.[17] A comprehensive examination of these reports found common human errors such as knowledge deficit, erroneous computer data entry, use of ambiguous abbreviations, and faulty dose calculations to be leading causes of the incidents. Distractions were reported to be a significant contributing factor, contributing to eight out of 10 errors. Other contributing factors were inexperienced staff, heavy workloads, and computer system failure.

Incident reporting systems are now central to patient safety initiatives worldwide. Incident reports provided by healthcare professionals have been shown to be useful in examining the risks and harm caused by healthcare (eg, falls, medication errors, therapeutic devices, and equipment).[18 19] Analysis of narratives about adverse events and near misses informs policy and practice for safer care. Indeed, incident reporting to facilitate rapid communication of safety flaws and critical events arising from computer use is one of seven steps which have been proposed to improve the safety of healthcare IT.[20] Sittig and Classen[21] endorse the reporting of computer-related incidents as an essential component of their framework for safe use of IT systems.

The Advanced Incident Management System (AIMS)[18] is one such incident reporting system, based on 20 years of research in patient safety, and has been in use since 1998 in more than 1000 facilities in Australia, New Zealand, South Africa, and the United States. In Australia, it is currently in use across the public health system in four of the eight states and territories: New South Wales, Western Australia, South Australia, and the Northern Territory. Additional sites are located in the states of Queensland and Victoria. These jurisdictions account for approximately 60% of the population of Australia and receive high numbers of incident reports per year. For example, New South Wales receives approximately 140 000, and South Australia and Western Australia each receive about 20 000 reports per year. An AIMS incident report consists of a number of structured and free text fields used to describe the incident and its consequences (see online supplementary appendix A, available at www.jamia.org). The incidents studied in this paper were reported using this system.

It is important to note that incident reports do not yield true frequencies of errors or adverse events because they do not capture numerators or denominators, and are subject to bias from a number of sources.[22] However, with large collections of incidents, characteristic profiles may be identified, allowing incidents to be aggregated and analyzed.[23] To do this, it is necessary to 'deconstruct' incidents by systematically identifying contributing factors and consequences, so that the most safety-critical risks can be identified. This process has been undertaken for incidents relating to monitoring equipment and medications.[23 24] The classification developed for AIMS allows incidents to be grouped according to 13 healthcare incident types (HIT), such as 'clinical process/procedure' or 'medication/IV fluid.'[23–25] Computers are listed as an option under the 'medical equipment/device' category within an equipment list that is sourced from the ECRI's Universal Medical Device Nomenclature System (UMDNS).[26]

Recently, a framework for an International Classification for Patient Safety (ICPS) has been agreed to, by a drafting group convened by the World Health Organization (WHO) World Alliance for Patient Safety.[27] The framework is based upon existing classifications such as AIMS, with additional input from international experts in safety, systems engineering, health policy, medicine, and the law.[5 28 29] However, existing classifications, including AIMS and the ICPS,[18] fall short with respect to computer-related incidents as this source of risk has yet to be systematically examined.[20] In this study we thus set out to analyze patient safety incidents associated with computer use to provide the basis for the development of a classification of the problems reported. Such a classification will allow information about computer-related incidents to be collated and classified, providing an objective basis for comparing patterns over time and between settings, and for the development and prioritization of preventive and corrective strategies.

METHODS

Setting

We examined patient safety incidents that were reported by public hospital clinicians to AIMS between 2003 and 2005 across one Australian state. Within this specific state a clinical information system, which contains patient information for all clients, is routinely used in eight major metropolitan public hospitals. Information technology provides clinicians with facilities for electronic ordering, submission of referrals, and recording of consultation notes, with real-time electronic access to integrated patient information including laboratory results, radiology reports, and outpatient appointments.

Search strategy

We searched among the 42 616 patient safety incidents reported between 1 July 2003 and 30 June 2005 by public hospital clinicians to AIMS. Incidents were identified using both the AIMS classification of incidents, as well as additional searches of the free-text incident descriptions. Free-text searches of incident description fields were conducted using a set of keywords generated by the investigators to describe computer hardware, software, or displays based upon knowledge of the clinical information systems deployed in the jurisdiction (box 1).

Classification development

We examined the free-text descriptions of a quarter of the incidents retrieved (25% of 123) to identify 'natural categories' for classification.[30] Where available, AIMS fields such as the medical specialty, time of day, contributing factors, consequences, incident type, ways to prevent the incident, and future risks of a similar incident, were examined. The safety assessment code (SAC) or risk score assigned to each incident was also noted.[31] A simple classification of the reported problems with using computers was developed (figure 1). To account for the main problem described by the reporter, we distinguished human–computer interactions (eg, wrong patient selected) from machine-related problems. Incidents were classified as human- or machine-related, and then subdivided based upon problems at the point of data entry (input), data transfer (transfer) or data retrieval (output). More than one category could be chosen for an incident if multiple problems were identified. A 'general technical' category was included to account for broad hardware and software issues leading to incidents that

Box 1 Keywords used to search free-text descriptions for computer-related incidents

Hardware

- Input devices
  - Keyboard, type, typing, mouse, click, pointer, touch screen, stylus, digitiser/digitizer, scanner, OCR
- Output devices
  - Terminal, screen, VDU
  - Printer, print out, printout
- Networking
  - Internet, web, network, cable, server, system down/unavailable, crash, glitch, bug
- Fixed computers
  - Computer, IT, ICT, information system, workstation
- Mobile devices
  - PDA, handheld, palm, blackberry, personal digital assistant, tablet

Software

- By generic name
  - Prescribing package, CPOE, order entry, PAS, patient administration, LIS, laboratory information system, EMR, EHR, electronic (patient/health) record, patient monitoring system, clinical order module, communication system, electronic transfer, digital imaging system
- By manufacturer
  - Oasis, Medical Director, Kestral, Homer, Hass, Cerner, iSOFT
- By local nomenclature
  - EDIS
- By input feature
  - Pick list, menu, drop down menu
  - Typing, data entry
- By software component
  - Database
  - Knowledge base
  - Decision support
  - Dose suggestion
    - Drug suggestion
    - Warning, alert
- Output/ display
  - Information display/presentation

did not fit into these categories. A category of 'contributing factors' was also included to account for socio-technical contextual variables that contributed to computer-related incidents, such as multi-tasking while using a computer. This was done without reference to AIMS to avoid constraining the range of new categories.

Analyses

Two of the investigators (FM, MO) classified the remaining 75% of incidents (n=123) using the new classification. An inter-rater reliability analysis using the kappa statistic was performed to determine consistency among coders.[32] If an incident was assigned to more than one category, the primary classification was included in the kappa score calculations. When coders disagreed on a primary classification, the event was re-examined and a consensus category assigned. Inter-rater reliability was $\kappa=0.71$ ($p<0.001$), 95% CI 0.06 to 0.80.[32] Free-text incident descriptions were used to assess the direct consequences of incidents on clinical tasks. Descriptive analyses were undertaken for all events to examine the distribution of events by category, medical specialty, time of day, and severity.

RESULTS

Our search strategy retrieved 123 incidents, 23 of which were retrieved using AIMS and the remainder from free-text searches of incident descriptions (see online supplementary appendix B, available at www.jamia.org). We removed four duplicates and eight incidents that did not relate to patient safety, leaving 111 incidents. A medical specialty was recorded in 45 incidents (40%, n=111). Emergency Medicine and Surgery accounted for seven incidents each (15%, n=45), General Medicine for four (8.9%), and Cardiology for three (6.7%) with one or two incidents for each of a further 20 specialties. The time of the incident was provided in 64% (n=71) of reports; three quarters occurred between 07:00 h and 17:00 h (figure 2). Risk scores were available in 68 reports (61%; table 1). The majority were in the medium to low risk categories, SAC 3 (69%, n=47) and SAC 4 (29%, n=20). Only one incident was high risk (SAC 2; see online supplementary appendix C, available at www.jamia.org), and there were no extreme risk cases. While 38% (n=26) of the incidents were reported to have a noticeable consequence but no harm, 34% (n=23) had no noticeable consequence.

Classification of computer-related problems

Of the 111 incidents, eight described an improvement in patient safety due to IT, and four were unresolvable. Examination of the remaining 99 incidents revealed 117 problems. Of these, 55% (n=64) were machine-related problems and 45% (n=53) were problems in human–computer interaction (table 2). Delays in initiating and completing clinical tasks directly related to patient care were a major consequence of machine-related problems (70%, n=39). In contrast, rework was a major consequence of problems in human–computer interaction (78%, n=18). The counts and percentages of incidents for each category in the classification are listed in table 3.

Information input problems

Information input problems were the largest category, accounting for 31% of incidents (n=36). Most were associated with incorrect human data entry (17%, n=20), such as incorrect selection of patient name, diagnosis, diet codes, discharge hospital, and typographical errors. Input errors also resulted from entry into incorrect fields. Equipment problems accounted for only two of these incidents. Although input problems generated errors in the task at hand (eg, 'medication entered for wrong patient', 'x-ray request sent for the wrong patient', 'wrong pathology results posted'), the resulting discrepancies in patient and clinical information were nearly always detected by staff at a subsequent step, usually within that hospital encounter (eg, 'nurse rang pharmacy to intercept discharge script'). Mistakes were sometimes self-detected by staff who took corrective measures themselves (eg, 'call to intercept an incorrect pathology or radiology request'). Some incidents (6.0%, n=7) related to problems in updating data (eg, 'computer system not updated when patient transferred between wards', 'medication lists not updated on admission') and missing data (6.0%, n=7) (eg, 'details of primary care physician not entered in online system'). Overall, input problems were reported to delay care (eg, 'delay in following up abnormal x-ray results received after patient discharged') and resulted in rework to correct mistakes (eg, 'medical registrar called from Emergency to take bloods again', 'extra time taken to trace patient using directory inquiries and other sources').

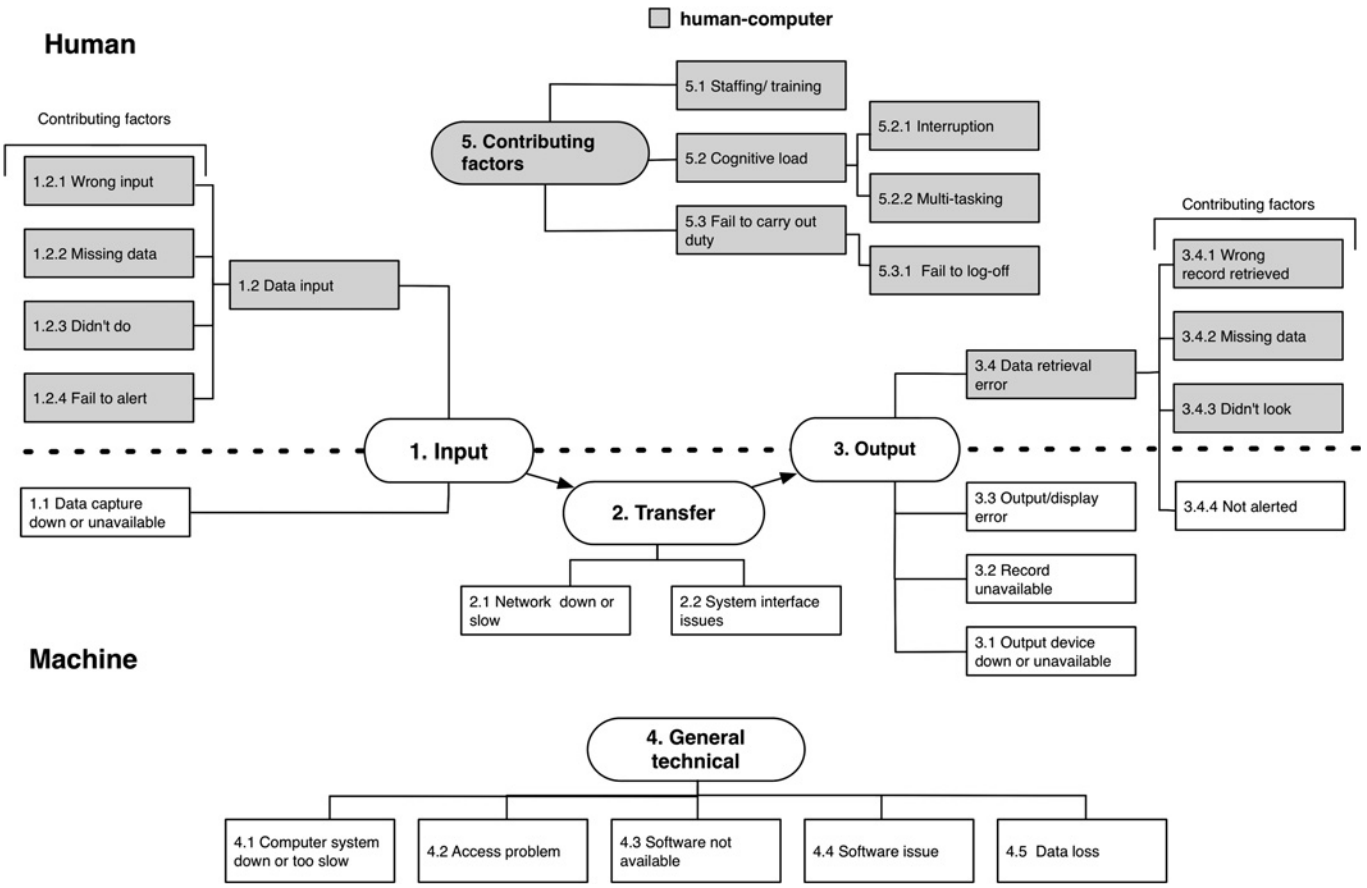

Figure 1 Classification of problems reported in computer-related patient safety incidents (problems relating to human–computer interaction are shaded).

Information transfer problems

Problems in the transfer of information accounted for 20% of all incidents. These were almost evenly attributed to computer network and systems integration issues. While the occurrence of these incidents was generally unpredictable, they were sometimes associated with routine maintenance activities (eg, planned server upgrade) making a range of systems (eg, CPOE, electronic medical records (EMR), Imaging) inaccessible from as little as 15 min to as long as 8 h. No or poor access from peripheral terminals to the computer network made key hospital services inaccessible (eg, 'hospital unable to attend major trauma'; 'patients cannot be admitted', 'can't order investigations', 'can't track location of patients', 'can't get X-rays', 'can't get results', 'paralyzed clinic for whole morning, ultrasound

Figure 2 Distribution of computer-related patient safety incidents by time of day (n=71).

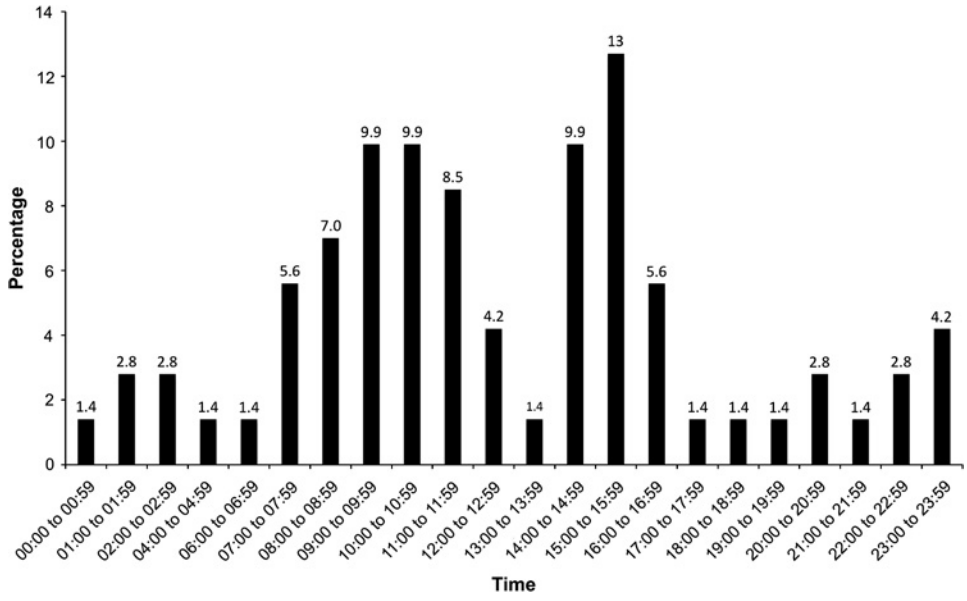

Table 1 Type of computer-related incident by risk category (n=68)

	Risk score*			
AIMS event type	High risk (SAC 2)	Medium risk (SAC 3)	Low risk (SAC 4)	Total (%) (n=68)
Harm to a patient (adverse event)		2		2 (3)
Arrested or interrupted sequence (near miss)		1	2	3 (4)
Incident with noticeable consequence but no harm		17	9	26 (38)
Incident with no noticeable consequence	1	20	2	23 (34)
Hazardous event or circumstance		4	5	9 (13)
Complaint		2	2	4 (6)
Loss		1		1 (1)
Total	1	47	20	

*The Advanced Incident Management System (AIMS) incident monitoring system from which we retrieved reports utilizes a reversed form of the safety assessment code (SAC) where a SAC score of 1 represents extreme risk and low risk is assigned to a SAC score of 4.[38]

results not available offline'), and caused delays (eg, delays admitting 35 patients) often resulting in workarounds supported by paper records and other sources to account for missing information (eg, 'treatment delays resulting from doctors having to access x ray films outside ED', 'prolonged consultation using interpreter', 'incomplete treatment plan', 'missing results', 'extra appointment scheduled').

Systems integration problems (n=11, 9.4%) were reported to be the primary cause for incomplete and lost requests sent to pathology and radiology departments and for missing results. As with computer network problems, these incidents resulted in delays (eg, '3 day delay in placing another order by which time patient could not be located'), often requiring rework (eg, '93-year-old patient stuck with needle for unnecessary repeat specimen') and additional phone calls to follow up requests and results (eg, 'unit must telephone pathology to receive results').

Information output problems

Information output problems accounted for 20% of incidents (n=23) caused by malfunctioning peripheral devices (n=13, 11%; eg, printers and monitors). Problems in human–computer interaction (n=10, 8.5%) included errors in the interpretation of printed and online information due to poor quality or misleading presentation. For example, key information such as abbreviations, name, and dose were unclear in computer generated medication printouts and electronic displays (eg, 'to view the drug levels for any particular client one most scroll downwards and then one of those rows of dates is no longer visible, the one that is not visible is the only relevant one'). Data retrieval errors were another type of output problem (eg, receptionist relied on date-of-birth search to identify records with similar sounding names). Use of hybrid paper–electronic systems sometimes resulted in omission errors where clinicians were not notified about results (eg, 'doctor/hospital team not notified about abnormal results from private abdominal ultrasound scan available on computer system, results available online but not sent to doctor as requested'). Failed output devices prevented access to results. As with data retrieval problems, these incidents were generally detected by staff at a subsequent stage (eg, 'error intercepted by nurse and patient, medications delayed till the next morning', 'treatment halted, patient re-assessed, treatment corrected and completed without complications'). Notification problems delayed treatment and were reported to be a source of frustration for staff who needed to act upon test results.

Table 2 Causes and consequences of 117 problems in 99 computer-related incident reports

Problems		Consequences	
	n=117 (%)	Delay n=56 (%)	Rework n=23 (%)
Human	53 (45)	17 (30)	18 (78)
Machine	64 (55)	39 (70)	5 (22)

Table 3 Classification of 117 problems reported in 99 computer-related patient safety incidents

		Consequence	
(Type) Problem	Frequency n=117 (%)	Delay n=56 (%)	Rework n=23 (%)
1. Information input problems	36 (31)	10 (18)	11 (48)
1.1 (Machine) Data capture device down or unavailable, eg digitizer not working	2 (2)	2	
1.2 (Human) Data input (communication error)			
1.2.1 Wrong input	20 (17)	4	9
1.2.2 Missing data	7 (6)	1	
1.2.3 Fail to update data	7 (6)	3	2
1.2.4 Fail to communicate/ carry out task			
2. (Machine) Information transfer problems	23 (20)	19 (34)	3 (13)
2.1 Network down or too slow	12 (10)	10	
2.2 Systems integration problem	11 (9)	9	3
3. Information output problems	23 (20)	8 (14)	5 (22)
3.1 (Machine) Output device down or unavailable	5 (4)		
3.2 (Machine) Record unavailable			
3.3 (Machine) Output/display error	6 (5)	1	
3.4 Data retrieval error			
3.4.1 (Human) Wrong record retrieved	5 (4)	2	4
3.4.2 (Human) Missing data (ie, did not look at complete record)			
3.4.3 (Human) Did not look	5 (4)	3	1
3.4.4 (Machine) Not alerted	2 (2)	2	
4. (Machine) General technical	28 (24)	17 (30)	2 (9)
4.1 Computer system down or too slow	11 (9)	8	
4.2 Software not available	1 (2)		
4.3 Access problem (ie, user unable to login)	6 (5)	4	
4.4 Software issue (ie, system does not allow data entry)	8 (7)	5	1
4.5 Data loss	2 (2)		1
5. (Human) Contributing factors	7 (6)	2 (4)	2 (9)
5.1 Staffing/ training	2 (2)	1	1
5.2 Cognitive load	1 (1)		
5.2.1 Interruption			
5.2.2 Multi-tasking	1 (1)	1	1
5.3 Fail to carry out duty			
5.3.1 Fail to log-off	3 (3)		

General technical

General technical problems accounted for 24% of the incidents (n=28). Problems ranged from slow performance or failure of a single computer workstation (9.4%, n=11) to software-related issues where software was not available at a particular workstation, was not accessible, did not have the correct settings (eg, date), or behaved in an unexpected manner preventing data entry or causing data loss (eg, 'patient discharged from computer system prior to specimen arrival in Tx department'). Software-related errors were detected by vigilant staff and required rework to correct mistakes (eg, 'letters needed to be re-done'). As with network problems, poor performance or failure of a single workstation prevented staff from carrying out tasks (eg, 'nurses unable to access results and complete handovers', 'clinician unable to access care plan for frequently presenting patient who required treatment within 30 min in Emergency'), caused delays and were reported to be a source of significant frustration. Workarounds and re-organization were the most common strategies to cope with general technical problems which prevented access to patient and clinical information (eg, 'staff required to compile manual lists resulting in delays', 'doctors must leave the ED to view x-rays', 'clinicians making decisions without radiology results', 'major trauma redirected to another hospital').

Contributing factors

A number of human factors (n=7, 6.0%) were reported to directly lead to patient safety incidents. The presence of a hybrid electronic—paper system meant that not all staff were trained to access the computer system (eg, 'ward clerk not available to access EMR').

Multitasking was reported to be a contributing factor in one high-risk (SAC 2) incident in which a wrong blood test request form was picked up from a printer out-tray. In this case the nurse was aware that the printer was slow so they decided to start dialysis while waiting, meanwhile another request form was printed leading to a mix-up. While there was no delay in treatment, the mix-up was reported to delay blood results as staff firstly called the laboratory to cancel tests, then blood was taken again from the patient. Potential and actual breaches of patient privacy were reported to be the consequence of printouts left at patients' bedsides as well as failure to log-off the computer system.

Improved patient safety

Although not included in the initial draft of our classification, we report incidents in which IT played a role in improving patient safety. Examination of these incidents (n=8) revealed that the availability and sharing of electronic health records (EHR) aided detection of drug—drug interactions (eg, warfarin—tramadol), duplicate medication orders and MRSA infection risk, assisted checking and correction of dialysis treatment, found discrepancies in antenatal paper records, and provided up-to-date contact details. In one case a discrepancy in the ABO blood group was identified by a transfusion computer program that was used to cross-check records maintained at multiple sites.

DISCUSSION

Main findings and implications

This is the first study we are aware of which examines computer-related patient safety incidents reported by health professionals to a state-wide system in order to develop categories to provide the basis for a classification. While the causes, consequences, and outcomes of several types of patient safety incidents have been previously reported,[18] the few studies of computer-related incidents in hospital settings have generally been restricted to specific areas of activity such as medication incidents.[17]

Reporting and analyses of IT safety incidents

We found only 99 patient safety incidents out of 42 616 (0.2%) that were related to IT. Possible contributing factors to this low overall proportion of computer-related incidents include: the system used (AIMS) does not specifically elicit information about IT incidents, which may have inhibited reporting (most incidents in our analysis were retrieved from free-text descriptions); reporters may be unaware of this emerging class of incident, and so under-reported it; and healthcare workers may have low expectations of the reliability of computers and IT systems, and regard problems as being 'business-as-usual' and not worth reporting.

Most incidents reported were fairly mundane from the patient safety perspective, but quite disruptive to workflow and frustrating for healthcare professionals. This is consistent with findings in other patient safety domains where mundane adverse incidents predominate (eg, falls, poor pain management). Nevertheless, they account for about 60% of incident-related resource consumption.[30] The vast majority of computer-related incidents, although often delaying clinical work and creating rework, did not directly harm patients. This is an important message, as it helps shape research and policy to deal with what is important 'on the ground' as opposed to what might be technically interesting or newsworthy.

Learning from incidents

Incident reports are useful for learning even when no actual harm resulted, when clinicians feel that there has been a near miss or that a catastrophic outcome could have resulted. While the multitude of small errors in the system seldom result in patient harm—Reason's Swiss cheese model is a nice metaphor for this[33]—the types of error are finite in number and, when systematically identified and addressed, can lead to improvements in patient safety.

The main purpose of our study was to identify categories to populate a classification of IT problems that will provide a clinically useful, comprehensive means of eliciting information about, and collating and classifying computer-related patient safety incidents. We believe that such a scheme needs to reflect the natural categories that arise from real-world reports,[30] as well as being shaped by top-down classes that place IT incidents in the overall context of patient safety.[28] With a sound classification, mechanisms can be established to improve reporting by better eliciting information from reporters, and we will then be better able to identify the profile of computer-related incidents and the implications for patient safety.

Identifying the natural categories of safety incidents has been the method used for creating the AIMS classification, which is the starting point for expanding the ICPS.[18 30] We propose that a further health incident type (HIT) for the ICPS be developed for IT related problems, incorporating the categories identified here (table 3, figure 1). This will be further expanded by a comprehensive search of the literature and by extracting IT incidents from other databases. For example, information about computer-related problems will have specific categories in the US 'common formats'.[34]

Factors contributing to incidents

We found that technical issues relating to computer hardware, software, or networking infrastructure accounted for over half the problems reported (55%), with human factors reported to be the primary cause in the remaining 45%. The nature of our study does not allow us to determine which of these problems would also have occurred with paper records. However, the fact that they did occur is of relevance to the development of healthcare IT systems. Six out of 10 problems in human—computer interaction related to data entry (64%), and retrieval of clinical and patient data was also problematic.

Specific contributing factors were cited for only 6% of problems. This reflects the manner in which the reporting system was used, and has been the subject of comment elsewhere.[35] Factors reported including the lack of training, failure to carry out a duty, high cognitive workload, and the effects of multi-tasking. Observer studies have confirmed that multi-tasking and interruptions are ubiquitous in clinical work.[36] A factor in the low rate of reporting is that multi-tasking and interruptions seem generally accepted by staff as an inevitable part of clinical work and may not be recognized or reported as explicit contributing factors. There are plans to elicit such information by reporting to call centers with operators who may prompt the reporters. However, observer studies, ideally combined with interviews, may well represent a better method for capturing information of this type.[36]

Consequences of incidents

Delays in initiating or completing clinical tasks were reported to be a major consequence of the computer-related incidents we examined, and were associated with 70% of machine-related problems. Rework was associated with 78% of problems in human–computer interaction (table 2). Overall, the negative impact of computer-related incidents on patient safety is small but noticeable. Twelve incidents in our dataset were associated with an adverse event or a near miss (see online supplementary appendix C), with actual or potential patient harm.

Improving the safety of clinical IT

Ongoing vigilance (staff detecting mistakes) was highly effective in preventing incidents from turning into adverse events (with harm to patients). However, self-detection and correction of mistakes was not supported by the existing technology, for example staff could not easily cancel a request and needed to contact the intended recipient by telephone or face-to-face to intercept incorrect pathology or radiology orders. A separate communication channel was also useful in tracing missing pathology or radiology requests. This highlights the importance of staff training and the development of protocols for the safe use of health IT.

Our results also underscore the fundamental importance of basic technical infrastructure in supporting safe care. It is essential that staff have access to, and smooth functioning of, their hardware (eg, computer workstations including peripheral devices such as printers and scanners) and networking infrastructure. Lack of access to the computer system (eg, EHR) often resulted in workarounds relying on paper-based records, which were often inefficient and ineffective. It is also essential that scheduled and unscheduled interruptions to service trigger a switch to a reliable and up-to-date backup system. Software must be also be accessible and up to date, with accurate local settings such as date and time. Where required, reliable software interfaces for communicating with other systems should be provided.

While dual paper and electronic systems may be unavoidable initially, work processes where staff must update two sets of records may introduce new opportunities for error. On the other hand, the redundancy provided by a dual system was sometimes reported to be useful in verifying and correcting irregularities. Our results also indicate a critical need for specific safety features within user interfaces to minimize selection errors. While hard-stops (not allowing users to proceed beyond a certain point without correcting mistakes) are useful, they can probably only be applied very selectively, for example when critical data are incorrect and/or missing. The broad-brush use of such strategies may not be acceptable to staff. Similarly, alerts can notify staff when critical tasks are not completed. While standardization of design features to improve retrieval and accurate presentation of electronic records is currently being explored (eg, the Microsoft Common User Interface initiative), there is little evidence that these strategies reduce the risks associated with human–computer interaction. An evidence-based approach to design that is based on examining the effectiveness and long-term use of specific safety features for data entry and retrieval is urgently needed.

Comparison with the literature

Patient safety incidents associated with computer use have not been extensively investigated. Building on previous approaches to examining healthcare IT incidents, our categorization expands the two high-level categories of human–computer and machine-related problems identified by others.[1 8] Two of our main categories map to the high-level error classes first identified by Ash *et al*.[1] 'Information input problems' and 'information output problems' correspond to errors in 'entering and retrieving information', and 'information transfer problems' correspond to 'communication and co-ordination'. We have expanded these categories to identify specific manifestations of these problems and added two general categories to account for technical problems and contributing factors described by reporters.

Consistent with previous analyses of IT incidents involving medications, we found a range of human–computer interaction errors related to selection of patient and clinical information, and display errors. The consequences of IT problems, including delays and rework, were also similar. Some specific effects such as dispatch of medications to the wrong room, were also common. In contrast to the MEDMARX data, we found a larger proportion of incidents related to computer system failures (2.8% MEDMARX vs 9.4%).[17] Fewer mismatches between actual clinical workflow and the system model were reported in comparison to Koppel *et al*'s mixed method study, most likely representing a narrower focus on the part of clinicians forwarding incidents.[8] Such inferences may indeed be better drawn from mixed method studies.

Limitations of this dataset

The incidents studied here are based on self-reports provided to a voluntary incident reporting system, with all the inherent limitations of such a system, such as a bias toward reporting incidents which appear interesting or unusual.[22] Another limitation is that the dataset used, from one Australian state, has limitations imposed by the education provided and practices which evolved in that state with respect to incident reporting. Inefficiencies in providing detail about contributing and contextual factors have been identified, and a two-level system is being proposed (basic and detailed, bringing in information from all available sources) to better elicit information in the future.

However, the incidents analyzed were reported over a significant period, providing sufficient data for some quantitative and qualitative analyses. As we have shown in other domains, such incident reports are useful in providing a profile of the nature of the problems encountered, and this profile has generally been shown to be consistent until interventions are introduced to address problems identified.[22] Although no cause and effect relationships can be reported with confidence, changes in the profile of what goes wrong over time can suggest the elimination of some old problems and the emergence of some new ones.[37] A major strength of reporting systems is the potential to learn from the collective experience of others. There is sufficient evidence to suggest this is going to be extremely important in designing and implementing healthcare related IT systems. To this end, we propose to use the categories identified here as the basis of the WHO International Classification for Patient Safety which is currently under development.

The computer-related problems we have identified are limited to the types of IT systems in use at the time and represent only a small proportion of the kinds of problems that might be encountered. For instance, other well-known problems previously identified in the literature, for example failure to update rules for decision support systems,[38] are not represented here. Incident reports are one source among an array of information repositories (eg, the literature, existing registries for equipment failure and hazards, medical record review, complaints, and medico-legal investigations[39]) that need to be brought together to provide a more comprehensive understanding about the nature, causes, consequences, and outcomes of IT problems in healthcare.

CONCLUSION

Only 0.2% of all incidents reported were computer related. Machine-related problems (software- and hardware-related) accounted for more than half of the problems, with most of the remainder attributed to problems with human–computer interactions. The vast majority of computer-related incidents, although often delaying clinical work and creating rework, did not directly harm patients; ongoing staff vigilance was highly effective in preventing harm. Voluntary incident reports are useful, as in other spheres of activity, in identifying the nature and consequences of some of the problems of using IT in routine clinical settings. Further work is required to expand our classification using incident reports and other sources of information about IT problems in healthcare nationally and internationally. Evidence-based approaches to designing safer user interfaces are needed and must focus on features for the safe entry and retrieval of clinical information, and support users in detecting and correcting errors and malfunctions.

Acknowledgments The authors wish to thank Dr P Hibbert for his assistance in retrieving incident reports.

Funding This research is supported in part by grants from the Australian Research Council (ARC) (LP0775532 and DP0772487) and NHMRC Program Grant 568612. FM is supported by an ARC APDI Fellowship and the University of New South Wales, Faculty of Medicine. MO is supported by an ARC APA(I) Scholarship.

Competing interests None.

Provenance and peer review Not commissioned; externally peer reviewed.

REFERENCES

1. **Ash JS,** Berg M, Coiera E. Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. *J Am Med Inform Assoc* 2004;**11**:104–12.
2. **Coiera E,** Westbrook J, Wyatt J. The safety and quality of decision support systems. *Methods Inf Med* 2006;**45**(Suppl 1):20–5.
3. **Ammenwerth E,** Schnell-Inderst P, Machan C, *et al*. The effect of electronic prescribing on medication errors and adverse drug events: a systematic review. *J Am Med Inform Assoc* 2008;**15**:585–600.
4. **Runciman WB,** Merry AF. Crises in clinical care: an approach to management. *Qual Saf Health Care* 2005;**14**:156–63.
5. **Runciman W,** Hibbert P, Thomson R, *et al*. Towards an International Classification for Patient Safety: key concepts and terms. *Int J Qual Health Care* 2009;**21**:18–26.
6. US Office of the National Coordinator for Health IT, HIT Policy Committee, Adoption/Certification Workgroup meeting 2010. http://healthit.hhs.gov/.
7. US Joint Commission on Accreditation of Healthcare Organizations [Internet] 2010. http://www.jointcommission.org/SentinelEvents/SentinelEventAlert/sea_42.htm (accessed Dec 2008).
8. **Koppel R,** Metlay JP, Cohen A, *et al*. Role of computerized physician order entry systems in facilitating medication errors. *JAMA* 2005;**293**:1197–203.
9. **Ash JS,** Sittig DF, Dykstra R, *et al*. The unintended consequences of computerized provider order entry: findings from a mixed methods exploration. *Int J Med Inform* 2009;**78**(Suppl 1):S69–76.
10. **Campbell EM,** Sittig DF, Ash JS, *et al*. Types of unintended consequences related to computerized provider order entry. *J Am Med Inform Assoc* 2006;**13**:547–56.
11. **Weiner JP,** Kfuri T, Chan K, *et al*. "e-Iatrogenesis": the most critical unintended consequence of CPOE and other HIT. *J Am Med Inform Assoc* 2007;**14**:387–8; discussion 9.
12. **Nebeker JR,** Hoffman JM, Weir CR, *et al*. High rates of adverse drug events in a highly computerized hospital. *Arch Intern Med* 2005;**165**:1111–16.
13. **Han YY,** Carcillo JA, Venkataraman ST, *et al*. Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. *Pediatrics* 2005;**116**:1506–12.
14. **Sittig DF,** Ash JS, Zhang J, *et al*. Lessons from "Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system". *Pediatrics* 2006;**118**:797–801.
15. **Horsky J,** Kuperman GJ, Patel VL. Comprehensive analysis of a medication dosing error related to CPOE. *J Am Med Inform Assoc* 2005;**12**:377–82.
16. **Singh H,** Mani S, Espadas D, *et al*. Prescription errors and outcomes related to inconsistent information transmitted through computerized order entry: a prospective study. *Arch Intern Med* 2009;**169**:982–9.
17. **Zhan C,** Hicks RW, Blanchette CM, *et al*. Potential benefits and problems with computerized prescriber order entry: analysis of a voluntary medication error-reporting database. *Am J Health Syst Pharm* 2006;**63**:353–8.
18. **Runciman WB,** Williamson JA, Deakin A, *et al*. An integrated framework for safety, quality and risk management: an information and incident management system based on a universal patient safety classification. *Qual Saf Health Care* 2006;**15** (Suppl 1):i82–90.
19. **Samore MH,** Evans RS, Lassen A, *et al*. Surveillance of medical device-related hazards and adverse events in hospitalized patients. *JAMA* 2004; **291**:325–34.
20. **Walker JM,** Carayon P, Leveson N, *et al*. EHR safety: the way forward to safe and effective systems. *J Am Med Inform Assoc* 2008;**15**:272–7.
21. **Sittig DF,** Classen DC. Safe electronic health record use requires a comprehensive monitoring and evaluation framework. *JAMA* 2010;**303**:450–1.
22. **Runciman WB,** Kluger MT, Morris RW, *et al*. Crisis management during anaesthesia: the development of an anaesthetic crisis management manual. *Qual Saf Health Care* 2005;**14**:e1.
23. **Symposium.** The Australian Incident Monitoring System. *Anaesth Intensive Care* 1993;**21**:501–695.
24. **Australian Medication Safety Working Group.** Towards the safer use of drugs and blood products in Australia. *J Qual Clin Pract* 1999;**19**:1–72.
25. **Runciman WB,** Roughead EE, Semple SJ, *et al*. Adverse drug events and medication errors in Australia. *Int J Qual Health Care* 2003;**15**(Suppl 1):i49–59.
26. Emergency Care Research Institute (ECRI) [Internet] 2010. http://www.ecri.org (accessed Nov 2008).
27. International Classification for Patient Safety[Internet] 2010. http://www.who.int/patientsafety/en/ (accessed Feb 2010).
28. **Sherman H,** Castro G, Fletcher M, *et al*. Towards an International Classification for Patient Safety: the conceptual framework. *Int J Qual Health Care* 2009; **21**:2–8.
29. **Thomson R,** Lewalle P, Sherman H, *et al*. Towards an International Classification for Patient Safety: a Delphi survey. *Int J Qual Health Care* 2009;**21**:9–17.
30. **Runciman WB,** Edmonds MJ, Pradhan M. Setting priorities for patient safety. *Qual Saf Health Care* 2002;**11**:224–9.
31. Safety Assessment Code (SAC) Matrix. [Internet]. http://www.va.gov/ncps/matrix.html (accessed Dec 2008).
32. **Landis JR,** Koch GG. The measurement of observer agreement for categorical data. *Biometrics* 1977;**33**:159–74.
33. **Reason J.** *Human error*: New York: Cambridge University Press, 1990.
34. **Agency for Healthcare Research and Quality.** Common formats. Rockville, Maryland: US Department of Health and Human Services [Internet]. http://www.pso.ahrq.gov/formats/commonfmt.htm (accessed Mar 2010).
35. **Schultz T,** Hannaford N, Runciman B, *et al*. *Improving learning from patient safety incidents: patient identification and clinical handover. Final report prepared for the Australian Commission on Safety and Quality in Health Care*. Adeliade: Australian Patient Safety Foundation, 2009.
36. **Westbrook JI,** Woods A. Development and testing of an observational method for detecting medication administration errors using information technology. *Stud Health Technol Inform* 2009;**146**:429–33.
37. **Runciman WB.** Iatrogenic harm and anaesthesia in Australia. *Anaesth Intensive Care* 2005;**33**:297–300.
38. **Sittig DF,** Singh H. "Eight rights of safe electronic health record use". *JAMA* 2009;**302**:1111–13.
39. **Runciman WB,** Merry A, Walton M. *Safety and ethics in healthcare: aguide to getting it right*. Aldershot: Ashgate Publishing, 2007.

An analysis of computer-related patient safety incidents to inform the development of a classification

Farah Magrabi, Mei-Sing Ong, William Runciman, et al.

J Am Med Inform Assoc 2010 17: 663-670
doi: 10.1136/jamia.2009.002444