Classifying Health Information Technology patient safety related incidents – an approach used in Wales

D. Warm; P. Edwards

Nursing and Social Care Information Directorate, NHS Wales Informatics Service, Pencoed, Wales

Keywords

Medical informatics; Patient Safety; Risk Management; Incident Reporting; Wales

Summary

Interest in the field of patient safety incident reporting and analysis with respect to Health Information Technology (HIT) has been growing over recent years as the development, implementation and reliance on HIT systems becomes ever more prevalent. One of the rationales for capturing patient safety incidents is to learn from failures in the delivery of care and must form part of a feedback loop which also includes analysis; investigation and monitoring. With the advent of new technologies and organizational programs of delivery the emphasis is increasingly upon analyzing HIT incidents.

This thematic review had two objectives, to test the applicability of a framework specifically designed to categorize HIT incidents and to review the Welsh incidents as communicated via the national incident reporting system in order to understand their implications for healthcare. The incidents were those reported as IT/ telecommunications failure/ overload. Incidents were searched for within a national reporting system using a standardized search strategy for incidents occurring between 1st January 2009 and 31st May 2011.

149 incident reports were identified and classified. The majority (77%) of which were machine related (technical problems) such as access problems; computer system down/too slow; display issues; and software malfunctions. A further 10% (n = 15) of incidents were down to human-computer interaction issues and 13% (n = 19) incidents, mainly telephone related, could not be classified using the framework being tested.

On the basis of this review of incidents, it is recommended that the framework be expanded to include hardware malfunctions and the wrong record retrieved/missing data associated with a machine output error (as opposed to human error).

In terms of the implications for clinical practice, the incidents reviewed highlighted critical issues including the access problems particularly relating to the use of mobile technologies.

Correspondence to:

Daniel Warm
Nursing and Social Care Information Directorate
NHS Wales Informatics Service
10–11 Old Field Road
Bocam Park
Pencoed
CF35 5LJ
Wales
E-mail: daniel.warm@wales.nhs.uk

Appl Clin Inf 2012; 3: 248–257
doi:10.4338/ACI-2012-03-RA-0010
received: March 27, 2012
accepted: June 10, 2012
published: June 27, 2012
Citation: Warm D; Edwards P: Classifying health information technology patient safety related incidents – an approach used in Wales. Appl Clin Inf 2012; 3: 248–257
http://dx.doi.org/10.4338/ACI-2012-03-RA-0010

1. Introduction

Interest in the field of patient safety incident reporting and analysis with respect to Health Information Technology (HIT) (also known as information management and technology or informatics in some health environments) has been growing over recent years as the development, implementation and reliance on HIT systems becomes ever more prevalent within healthcare settings [1]. A recent Institute of Medicine report [2] called for greater transparency and reporting of patient safety incidents related to the use of HIT, which is reflective of the hypothesis that an increase in the deployment of information technology within healthcare systems will potentially lead to patient safety incidents [3].

In Wales (UK) the responsibility for the strategic development of HIT sits with the NHS Wales Informatics Service (NWIS). As part of its governance structure NWIS has a formal Clinical Risk Management Process which drives the proactive assessment of the clinical risks for any HIT it develops or procures on behalf of the NHS in Wales. As part of this process the organization horizon scans for and reviews patient safety incidents that have been reported involving HIT through the National Reporting & Learning System (NRLS) and other mechanisms such as helpdesks. This information is used to inform the development, implementation and upgrading of HIT in Wales.

One of the rationales for capturing incidents is to learn from failures in the delivery of care and must form part of a feedback loop which also includes analysis; investigation and monitoring [3, 4]. With the advent of new technologies and the organizational delivery of HIT, the emphasis is increasingly upon analyzing patient safety related incidents [2]. Whilst incident reporting does not provide the whole picture of the risk and harm associated with HIT deployments, it can potentially contribute by enabling those who design and deploy HIT in the clinical area to be aware of some of the problems the implementation of HIT can introduce. Further, the use of incident reporting can be used to help develop safer systems [3]. Evidence does suggest that even in healthcare environments with a high dependency on new technologies, the levels of reported incidents resulting in severe harm are relatively low [5]. This may be due to an actual low level of harm or a low level of reporting incidents. Evidence suggests that the usage and attitudes towards incident reporting can differ by professional grouping such that a multi-disciplinary approach to incident reporting is advocated in order to improve both understanding of the importance of reporting incidents and the actual reporting of incidents [6].

Many countries and healthcare systems across the world including the NHS in England and Wales have a national incident reporting mechanism. In the UK the National Reporting and Learning System (NRLS)[1] was established in 2003 and enables anonymized patient safety incidents to be reported by NHS organizations to a national database. The database holds 5 million reports of patient safety incidents ranging from access to healthcare through to death of a patient due to the wrong intervention being applied. The data is analyzed nationally to identify hazards, risks and opportunities to improve the safety of patient care. In the NRLS a patient safety incident is defined as "Any unintended or unexpected incident that could have or did lead to harm for one or more patients receiving NHS-funded healthcare. *The terms 'patient safety incident' and 'patient safety incident (prevented)' will be used to describe 'adverse events' / 'clinical errors' and 'near misses' respectively*" [7]. For each incident the NRLS contains data fields such as date of incident, location, specialty, category (type of incident e.g. medication error) and a free text description of the incident and is completed by the reporter of the incident. The NRLS is in general a voluntary reporting system and any member of staff can report incidents to their local reporting system. In recent years the NHS in England has mandated that all incidents resulting in permanent harm or death are reported. This move was in response to the fact that there is significant under reporting of patient safety incidents [8]. As with any method of incident reporting there are always inherent advantages and disadvantages to the extent to which latent errors can be identified given the potential bias of incidents actually reported [9].

Parallel to the growing body of evidence of HIT incidents as reported through systems such as the NRLS there has been limited published evidence of the development of investigative frameworks to

[1] http://www.nrls.npsa.nhs.uk/

help categorize and understand the nature of the incidents. A recent example of an HIT orientated classification framework is one developed and enhanced by Magrabi et al [10, 11]. The framework itself is based on incidents reported in Australia and was further developed using information based on incidents drawn from reports submitted to the US Food and Drug Administration Manufacturer and User Facility Device Experience (MAUDE) database.

The applicability of the Magrabi framework has not been explored extensively within the context of national reporting systems and as such needs to be tested. In order to learn from the data received so far from the NRLS, NWIS conducted a thematic review of 29 months worth of data using the Magrabi framework as a basis for classification. The objectives were two-fold: to test the applicability of the Magrabi classification framework to categorize data collected within Wales as reported via the NRLS; and to review the incidents reported via the NRLS in order to understand their implications for the NHS in Wales.

2. Methods

Under an existing data-sharing agreement with the current administrators of the NRLS (National Patient Safety Agency), NWIS receives data from patient safety incidents reported from the NHS in Wales (both primary and secondary care) on a quarterly basis. In order to elicit relevant incident reports, the NRLS uses standardized incident coding for IT incidents (including clinical systems). Those used for this thematic review were IT/ telecommunications failure/ overload. The incidents extracted include the following standardized details: incident identification number; the location, service and specialty in which the incident occurred; the date; the type of incident; the degree of harm; and a free text description of the incident.

For the purposes of this thematic review, whereby incidents are analyzed which present common characteristics or themes [12], the authors categorized all incidents occurring in Wales between 1st January 2009 and 31st May 2011, and reported to the NRLS by September 2011.

Using the classification framework developed by Magrabi et al [10, 11] all reported incidents returned following the search were reviewed by the two authors both of whom have experience of thematic analysis. Each incident was independently reviewed and where differences were found in the categorization a discussion took place between the authors in order to achieve consensus.

The basis for the framework is to categorize incidents using a binomial classification of human or machine related categories and a series of sub-categories including input; transfer; out-put; general technical; and contributing factors (►Fig. 1). The rationale of such a thematic framework is to ensure a consistent approach to reviewing incidents.

3. Results

In total 149,532 patient safety incidents were reported across Wales in the period of the thematic review, of these 228 incidents were identified using the search strategy for HIT related incidents. Following the removal of duplicate reports and incidents that on discussion the authors did not believe related to HIT, 149 incidents remained. Duplicates were identified where the incident report was identical in every field e.g. location, specialty, free text. Where reports were similar e.g. could have been the same incident but reported by two different members of staff, these were considered to be separate incidents for the purposes of this analysis as the authors could not ensure they were actually the same incident.

Of these 149 incidents 69 occurred in acute/general hospital; 43 in community nursing, medical and therapy service (including community hospital); 21 in community and general dental services; 15 in mental health services; and 1 in general practice.

According to the attributed level of harm as allocated by the original reporter for all 149 incidents; no evidence exists of permanent harm or death, 99 incidents (66%) resulted in no harm to the patient and 50 (34%) were reported as low harm (e.g. an incident that required extra observation or minor treatment) [7].

3.1. Classification

Using the framework described by Magrabi et al [10, 11] each of the 149 incidents were allocated to one of the two high-level classifications, namely machine-related (where the incident is directly related to technical problems) and human-computer interface related (those incidents where there is an element of human interaction with systems). Of these 115 (77%) were classified as being machine-related and 15 (10%) were human-computer interface related. Nineteen incidents (13%) could not be classified using the framework as these were related specifically to the breakdown of hardware (i.e. the hardware itself does not work) which is not included as a category within the framework. All incidents were allocated to one category only. The percentages for each of the categories are listed in ▶Table 1.

3.2 Sub-categorization of incidents

The following analysis is categorized according to the sub-divisions within the framework of Magrabi et al [11] under machine related and human-computer interaction.

3.2.1 Machine related incidents

This is where an incident is directly related to technical problems.

3.2.1.1 General Technical incidents

This category of incidents within the framework is designed to capture general hardware and software related incidents and accounted for 56% (n = 83) of the total incidents reported. Within this category poor access, particularly from mobile devices accounted for 38 of the incidents, the computer system being unavailable accounted for a further 22 of incidents and software issues such as software configuration in 18.

Examples of this category of incidents are the inability to use the system whether due to lack of access to the network or the actual system being down meant that patients records could not be viewed to aid clinical decision making (such a x-ray images). Therefore the ability to add to patients records in a timely manner was inhibited and in some cases patient appointments were either cancelled or moved to other sites.

An example of an incident with respect to access issues from the NRLS database was "*Consultant had problems with viewing patient from archive. Whilst problem trying to be repaired remotely….. the remote server crashed which meant that there was no access to images*".

3.2.1.2 Information output incidents

Sixteen percent (n = 25) of the total number of incidents identified concerned information output incidents and these were only related to machine-related problems. Half of the incidents related to the displaying of dental radiological images from the wrong patient, this was noted to be a known and recurrent problem with the system. An exemplar of this is "*On patients…. file there are three xrays that do not belong to the patient*". Four other incidents were individual incidents related to Picture Archive and Communication System (PACS) images where PACS are used to manage the storage, retrieval, distribution and presentation of images including X-rays, ultrasound, CT and MRI scans.

3.2.1.3 Information transfer incidents

The smallest number of incidents within this group of reports related to the transfer of information where it accounted for the 5% (n = 7) of the total. Of these four incidents related to network issues such as slow connection speeds whilst three related to system interface issues such as information not being delivered to the designated destination.

3.2.2 Human-computer interaction

This is an incident where there is an element of human interaction.

3.2.2.1 Information input incidents

This was the only category where human-computer related incidents were reported and accounted for 10% (n = 15) of the total, three had the wrong information inputted, one was due to missing data, and the last one was related to an action not being undertaken. The remaining 10 incidents were related to where the system was available but would either not allow the user to record details or access specific details of a given patient.

3.2.3 Incidents unable to be categorized

Thirteen per cent (n = 19) of incidents did not relate to the categories set out in the Magrabi framework [11]. Of these 15 were related to the breakdown of telephone systems. The remainder were associated with hardware failures where the computer itself crashed or was not functioning, for example *"Image disc and computer failed, tried reformat, failed parts ordered to arrive next day"*.

4 Discussion

4.1 Critique of the applicability of the framework

Whilst the use of different framework types within patient safety are not uncommon [13, 14] the framework suggested by Magrabi et al [10, 11] is one that focuses specifically on health information technology. The development of this framework is dependent on the original data used to construct it. The testing of the applicability of any framework such as that developed by Magrabi et al is also dependent on the results used to test it and in this case the number of results generated using the search strategy. For this thematic review the 149 incidents clearly related to the technical aspects of the incident rather than the clinical and patient safety issues which could have been explored using a different search strategy.

The clinical relevance of some incidents could not be captured using the framework, however the framework does not set out to do this, instead it is intended to aid the development and prioritization of preventative and corrective strategies. It is suggested that a different approach may be needed to explore the clinical implications of incidents more appropriately within the context of a thematic framework.

Although the original authors of the framework mention hardware as an issue, the general technical classifications only covers software related issues. Those incidents which were due to hardware malfunction e.g. the computer itself was broken, could not be classified. The thematic review authors suggest that the framework could be expanded to include a further sub section of 4 (General technical) to include hardware malfunction. Sixteen out of the 19 incidents that were not able to be classified would fall into this new proposed category. Due to the nature of the incidents included in the sample there were several incidents related to the breakdown of phones and bleep systems which could not be classified. Further our analysis also suggests that there are two types of machine output / display errors which have the contributory factor of wrong record retrieved (n = 7) and missing data (n = 4).

The authors had some discussion over the difference between access problems and transfer problems due to the network being down or slow, as a network problem can prevent access, rather than being a contributory factor towards the transfer of data. In our analysis we allocated; 'access' to problems whereby the clinician could not open an application or system, transfer due to the network as those whereby information had been inputted but could not be uploaded to the system.

4.2 Learning from Incidents

A vast majority of the incidents reviewed were access issues, mainly due to mobile technology which did not feature in the Magrabi et al [11] framework. This needs to be considered during the implementation of systems used in community settings including patients' homes. This is particularly pertinent in rural areas/settings where there is often an emphasis on the development in relation to the use of mobile devices, and with respect to web based technology in telehealth/telecare/telemedicine projects. With respect to Wales specifically, reviewing the incidents gives the authors responsibility to follow-up and action areas of concern. This is potentially both with the developers of systems as well as the end users of those systems as appropriate.

The implementation of health information technologies particularly those pertinent to the correct identification of the patient is fundamental to improving patient safety. Mytton et al [15] however highlights the importance of monitoring new technologies in particular as they introduce new risks that are not always predicted. The ongoing reviews of incidents will enable organisations such as NWIS with responsibilities for the development and implementation of HIT to monitor whether their risk assessments and predictions were sound and help inform the assessment of future developments. Whilst the actual incidents of failure of HIT cannot be accurately quantified using incident reporting it can help identify if a failure has happened in the past so moving from the theoretical to an actual risk. To ensure lessons are learnt the ongoing review of patient safety incidents should result in some level of feedback to staff to ensure changes are made [16], particularly if they are being encouraged to report all incidents. This should be aimed at multiple levels of stakeholders from designers of systems through to users of those systems, specifically through training.

4.3 Limitations

The data reviewed covered all aspects of IT within the healthcare setting, not just clinical systems which would normally be considered Health Information Technology (HIT). This would explain why the authors were unable to use the Magrabi framework to categorize all incidents e.g. bleep and telephone incidents. Further the data as provided by the NRLS did not allow the identification of the actual type of HIT in a majority of cases e.g. electronic health records, decision support software, which would have enhanced the analysis.

The data reviewed was reported as low or no harm, again this may be due to the technical nature of the reports received. Incidents related to permanent harm or death of the patient would potentially be reported as clinically rather than technically related. It is possible that technology could have been a contributory factor. The data reviewed was also limited to the account provided by the reporter and no investigation or root causes for the incident was available for analysis. This will have potentially affected the allocation of categories by the authors as the cause and effect cannot be established with the data provided e.g. mobile connectivity may have been due to the laptop or the network provider.

The analysis identified very few human error incidents (n = 15); this may have been due to the nature of the dataset reviewed. Human error type incidents would probably be reported in other NRLS categories which reflect the outcome / affect on the patient rather than a technical incident which may have been the root cause. For example a medication administration error may have been due to a missing data inputted into a record, therefore reported as a medication incident rather than a data capture incident.

This was a limited and specific dataset and a wider search of the NRLS would be beneficial to truly test the framework and learn from HIT related patient safety incidents.

5. Conclusions

It is the intention of the authors to continue to use the framework to analyze all patient safety reports in the future as it proved appropriate and applicable to the data regularly analyzed. To ensure that all HIT incidents can be categorized using the Magrabi framework [10, 11] the authors would recommend some small adaptations including; hardware malfunction, and the wrong record retrieved/ missing data associated with a machine output error (as opposed to human error). The majority of the incidents reported and reviewed were machine related, with access to the systems dominating the results. Within this dataset very few human related issues were identified, but this may be due to the reporting process. This was a limited and specific dataset and a wider search of the NRLS would be beneficial to truly test the framework and learn from HIT related patient safety incidents.

The lack of frameworks that classify the clinical impact of incidents is an area that could be considered for future development.

6. Clinical Relevance Statement

The reviewing of health information technologies related incidents within the development, deployment and use of clinical systems is essential to ensure patient and clinical safety, and clinicians are critical to this process. The use of a framework such as that suggested by Magrabi et al [10, 11] is important in helping clinicians understand the types of incidents relating to the ever increasing use of health information technologies. Learning from the incidents reported here show that factors such as understanding the use of mobile technologies is vital particularly with respect to ensuring network coverage so that clinicians are able to access information in a timely and appropriate manner.

Conflicts of Interest

The authors declare that they have no conflicts of interest in the research.

Protection of Human and Animal Subjects

Human and/or animal subjects were not included in the project.

Acknowledgements

The authors would like to thank the National Patient Safety Agency for access to the data through the data sharing agreement, and to Farah Magrabi for allowing us to use and reproduce the diagrammatical representation of her framework. The authors would also like to thank Beverley Thomas (NWIS Director for Nursing and Social Care Information) for her insightful comments on the manuscript.

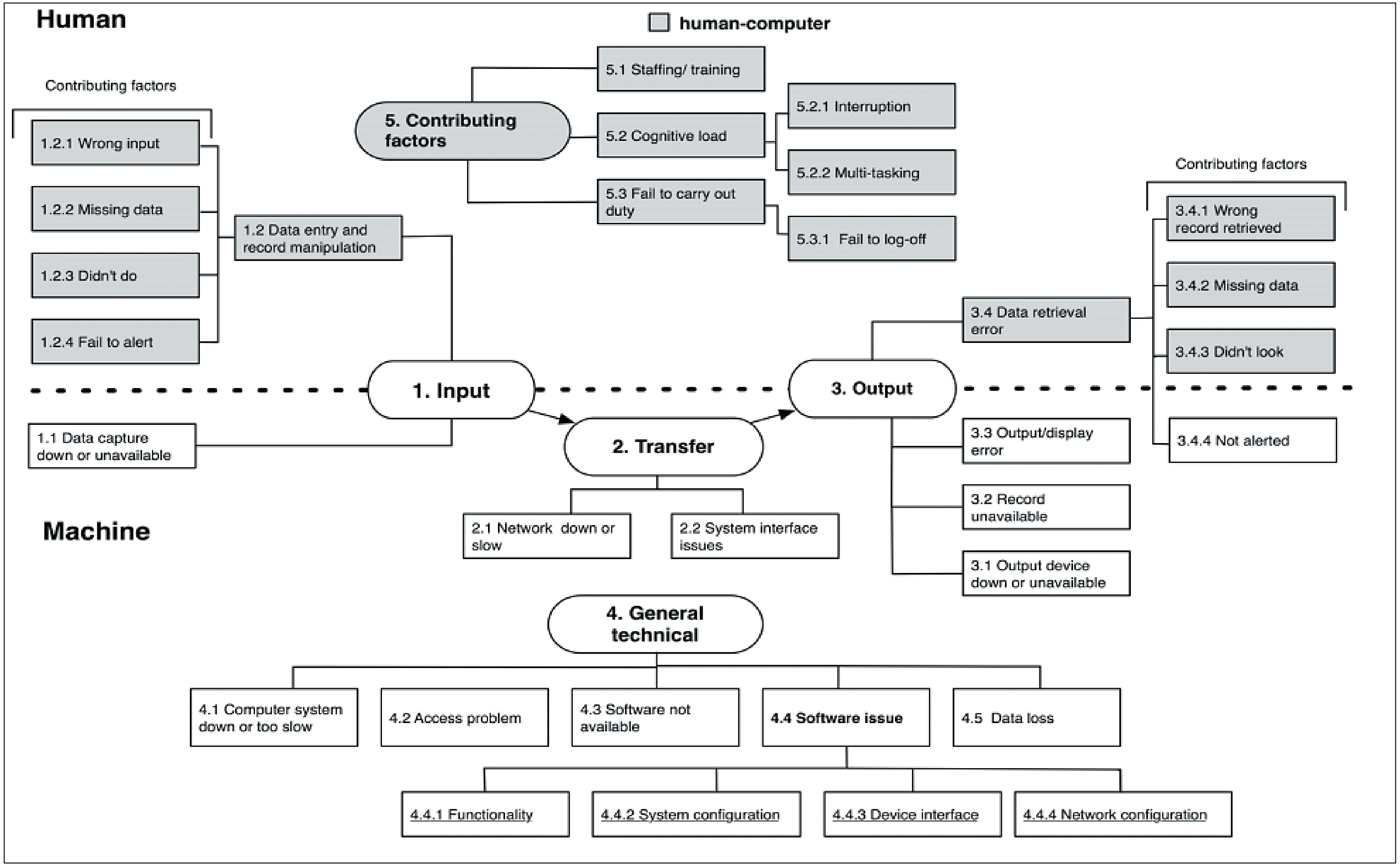

Fig. 1 Magrabi framework used for classification of 149 incidents reported to the NRLS as IT /telecommunications failure / overload in Wales

Table 1 Classification of 149 incidents reported to the NRLS as IT / telecommunications failure / overload in Wales using the Magrabi [11] framework.

	Category	Sub-category	Number	%
Machine related	General Technical	Access problem	38	26
		Computer system down or too slow	22	15
		Data loss	3	2
		Software issue	18	12
		System configuration	1	1
		Not able to classify	1	1
		TOTAL	83	56
	Information output	Record unavailable	1	1
		Output device down or unavailable	9	6
		Output/Display error	15	10
		TOTAL	25	16
	Information transfer	Network down or slow	4	3
		System interface issue	3	2
		TOTAL	7	5
Human – computer interaction	Information input	Data capture down or unavailable	10	7
		Data entry and record manipulation (Human related)	5	3
		TOTAL	15	10
Not able to classify			19	13
Grand Total			149	100

References

1. Sittig D, Classen D. Safe electronic health record use requires a comprehensive monitoring and evaluation framework. JAMA 2010; 303: 450–451.
2. Institute of Medicine. Health IT and Patient Safety: Building Safer Systems for Better Care. Washington, DC: The National Academies Press; 2012.
3. Myers R, Jones S, Sittig D. Review of reported clinical information system adverse events in US food and drug administration databases. App Clin Informatics 2011; 2: 63–74.
4. Benn J et al. Feedback from incident reporting: information and action to improve patient safety. Qual Saf Health Care 2009; 18: 11–21.
5. Newton RC et al. Making existing technology safer in healthcare. Qual Saf Health Care 2010; 19: i15-i24.
6. Braithwaite J, Westbrook M, Travaglia J. Attitudes towards the large-scale implementation of an incident reporting system. Int J Qual Health Care 2008; 20: 184–191.
7. National Patient Safety Agency. Seven Steps to Patient Safety. London: NPSA; 2004.
8. National Audit Office. A safer place for patients, Learning to improve patient safety. London: The Stationary Office; 2005.
9. Shojania K. The elephant of patient safety: what you see depends on how you look. The Joint Commission Journal on Quality and Patient Safety 2010; 36: 399–401.
10. Magrabi F, Mei-Sing O, Runciman W, Coiera E. An analysis of computer-related patient safety incidents to inform the development of a classification. J Am Med Inform Assoc 2010; 17: 663–670.
11. Magrabi F, Mei-Sing O, Runciman W, Coiera, E. Using FDA reports to inform a Classification for health information technology safety problems. J Am Med Inform Assoc 2011; 19: 45–53.
12. Aronson J. A pragmatic view of thematic analysis. The Qualitative Report 1994; 2.
13. Pfeiffer Y, Manser T, Wehner T. Conceptualising barriers to incident reporting: a psychological framework. Qual Saf Health Care 2010; 19: e60.
14. Reiman T, Pietikäinen E, Oedewald P. Multilayered approach to patient safety culture. Qual Saf Health Care 2010; 19: e20.
15. Mytton O et al Introducing new technology safely. Qual Saf Health Care 2010; 19: i9-i14.
16. Wallace L et al. Improving patient safety incident reporting systems by focusing upon feedback – lessons from English and Welsh trusts. Health Serv Manage Res 2009; 22: 129–135.