12-3-2014

Avoiding epic fails: software and standards directions to increase clinical safety

Patricia A H Williams
Edith Cowan University, trish.williams@ecu.edu.au

Vincent B. McCauley
Medical Software Industry Association, vincem@mccauleysoftware.com

DOI: 10.4225/75/57982c3331b49
3rd Australian eHealth Informatics and Security Conference. Held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.

AVOIDING EPIC FAILS: SOFTWARE AND STANDARDS DIRECTIONS TO INCREASE CLINICAL SAFETY

Patricia A H Williams[1] Vincent B McCauley[2]
[1]eHealth Research Group, School of Computer and Security Science
Edith Cowan University, Perth, Western Australia
[2,]Medical Software Industry Association
[1]trish.williams@ecu.edu.au, [2]vincem@mccauleysoftware.com

Abstract

The safety issues related to IT and software are gaining more exposure within the Healthcare industry. While software and computing was seen as a panacea to a range of preventable clinical errors, the introduction of healthcare IT has of itself presented patient safety issues. It is the inherently complex nature of healthcare, and its delivery, that creates increasing patient safety concerns in the application of IT and software. This position paper provides a collation of current work in international standards and highlights the drivers for the necessary change required to address patient safety in the use of healthcare IT software and systems. Software development and deployment has already altered and standards to oversee these are only just catching up. The need to revise such standards has been recognised and is underway, however a clash of cultures is delaying the emergence of Standards traditionally developed and governed by Standards Development Organisations (SDOs). The impact of this is that whilst standards are being informed by current software trends, the standards developers themselves are struggling to assimilate the rapid changes in the market. Whilst SDOs are cooperating more closely, there is an increased need for the involvement of the healthcare software development community and e-health informaticians in the standards process to narrow the gap in standards relevance. Such involvement would expand the currently narrow field of experts with the appropriate skills, background, knowledge, and experience in healthcare software risk analysis, security, privacy, and standards development.

Keywords
Health Software, Patient Safety, Standards, E-health, Health Informatics, Standards, Information Security.

INTRODUCTION

Contact with the healthcare system is a risky activity (Leape et al., 2009), and indeed, it has been shown to have a parallel risk to mountain climbing but with 99,900 more deaths per year (AHRQ, 2005). In the past 15 years, the implementation of information technology in healthcare has advanced rapidly. Whilst adoption and use of electronic record storage has occurred, the developments in established information exchange, telemedicine, and remote patient monitoring have not developed as rapidly as anticipated (Knaup et al., 2014). It is not a lack of technical solutions, but the organisational and ethical issues that have prevented the depth and breadth of development and adoption (Black et al., 2011). However, the increased use of information technology in healthcare has seen major improvements in reducing information based and clinical errors (Ammenwerth et al., 2014; Ammenwerth, Schnell-Inderst, Machan, & Siebert, 2008). These improvements relate to the impact on patient safety, medical errors, quality assurance and improvement, and risk management (Stroetmann, Thierry, Stroetmann, & Dobrev, 2007).

Patient safety impacts refers to an event that could have resulted, or did result, in unnecessary harm to a patient (Runciman et al., 2009; Sherman et al., 2009). However, it has also introduced a new set of problems related to the impact of IT and ICT applications on patient safety, The unintended consequences of using ICT in healthcare, which is a complex socio-technical environment, is a growing area of interest (Black et al., 2011; Magrabi, Li, Day, & Coiera, 2010).

Research on health information technology (HIT) system failures is difficult to acquire. To date, the majority of research is through analysis of reporting systems on patient safety such as the Food and Drug Administration (FDA) in the US (Magrabi, Ong, Runciman, & Coiera, 2010, 2012; Magrabi, Ong, Runciman, & Coiera, 2011). Consistently the majority of these errors concern medication errors (Ammenwerth et al., 2014; Magrabi et al., 2011). Unfortunately, reporting of errors is generally a voluntary activity, which leads to an inevitable underestimation of the scope of the problem. Further, where this specifically relates to the use and integration of HIT, the problems are compounded because of the difficulty in detecting and recognising such errors. Therefore, the research classification and identification of HIT patient safety issues primarily relates to post event notification. This paper explores the issues from perspectives of the development of HIT solutions, specifically

software, and the international work addressing patient safety concerns. An explanation of each health software safety issue, together with the current approaches to this, are presented. The clash of culture that this creates when addressing patient safety concerns from the software development perspective is also explored. Subsequently, the related challenges and drivers for safer software and the broader challenges that the healthcare environment presents, form the discourse in this paper.

WHAT IS EHEALTH SOFTWARE SAFETY AND WHAT ARE THE ISSUES?

Whilst having the potential to provide significant benefits in relation to patient safety, when health information systems and their associated software are designed without cognizance of potential patient safety concerns, they themselves pose risks to patient safety (Ash, Berg, & Coiera, 2004). It is imperative to understand the nature of the problems, as well as contributing factors and subsequent safety implications in order to address patient safety issues (Goodman et al., 2011). Interestingly, and incorrectly, the recent Ebola crisis in the US saw the blame for a patient death aimed at the EPIC electronic medical record (EMR) system (Dvorak, 2014; "Kalorama: EMR System Unlikely to Blame for Ebola-Related Care Mistakes," 2014). This accusation was a simplistic and reactionary response. It was clear to those in the discipline of ehealth informatics, that this was a significantly more complex problem.

Identification of the Issues

The classification of HIT problems related to software, as described by Magrabi, Ong, Runciman and Coiera (2011) suggests that the software issues relate to functionality, system configuration, device interface, and network configuration. Whilst this research focuses on parameters to improve reporting, they do suggest areas that software development can investigate to improve safety of software. However, it is clear that the information on reported incidents, which relates to technical issues with software hardware, and networking infrastructure, only provide an overview of the relationship of HIT systems to patient safety incidents. What is not ascertainable is when software related errors are clearly identified as the root cause as distinct from incidents caused by mis-configuration, slow system performance, network problems, and human error in software use. Whilst the latter are important to developing interventions to mitigate such problems, they do not assist in identifying underlying software development errors. Hence, both identification and subsequent reporting of 'software' errors is problematic. With a distinct lack of evidence, the standards community is left with no choice but to take a risk approach to the development of software and its potential patient safety concerns.

Addressing the Issues Through Standards

There is significant recent history of adopting a risk approach to safety. The medical IT network configuration has been the subject of standardisation since 2005 with the development of the *ISO/IEC 62A 80001 application of risk management to information technology networks incorporating medical devices,* series of standards. However, it is the delineation between medical device software and stand-alone health software, which is causing controversial debate. This has led to an evident clash of culture between two diverse development areas in healthcare IT. The classification of what patient safety means within risk assessment of health software, has traditionally been based on the severity of harm. However, as is reflected in the definitions of patient safety (Runciman et al., 2009), it is now moving to assessment based on traditional security reasoning and likelihood of occurrence (Williams & McCauley, 2013). Standards that address the areas of health software development and patient safety include:

- *ISO/TR 27809:2007 Health Informatics – measures ensuring patient safety of health software;* and
- *ISO/IEC 82304-1 Healthcare software systems – Part 1: General requirements for product safety* (under development).

However, the increasing integration and convergence of technology with software, is presenting significant challenges in developing standards to address patient safety within software systems.

Clashing of Cultures: Merging of Healthcare Safety Standards with Medical Devices and Health IT-Networks

The development of consensus can only occur where there is a shared understanding. With the convergence of technology and software, the convergence of standards is inevitable. It is this convergence and the subsequent indeterminate delineation between originally distinct entities, such as hardware and standalone medical devices, healthcare software, and IT networks supporting health care computing, that is presenting a significant challenge

in the standards development community and for the SDOs. The difficulties lie in the necessity for adaptation of the existing administrative working group structures as well as a mental/conceptual shift for those immersed in their individual discipline areas. An example of this is the collaboration between technical committees for ISO TC215 (Health Informatics) and IEC SC62A (Common aspects of electrical equipment used in medical practice) as an ISO Joint Working Group (JWG7) to integrate the standards on health software safety. The largest group of participants are medical device manufacturers, with only a few software developers, (mainly from Australia), and only one medical practitioner/Health Informatician (again from Australia). The close relationship between the development of *IEC 62304:2006 Medical device software -- Software life cycle processes* and ISO 82304 has led to considerable effort in educating the medical device participants in contemporary software techniques, and terminology. On the other side of the coin, the Medical Device safety community have provided education to the ISO participants in electrical and engineering risk analysis techniques. There are significant challenges in collaboration between these disparate international groups, such as understanding and agreement on basic terminology and concepts, the clash of development cultures, and semantic interpretation of common English language.

The increasing acceptance that software can no longer be considered distinct from the device on which it is running, (or in the case of medical devices embedded into), is reflected in the transfer and transformation of IEC 62304 (under IEC 62A jurisdiction) to *ISO/IEC 62304 Health software lifecycle process* (under joint ISO/IEC jurisdiction). This transfer includes a change of scope from 'medical device software' to 'health software'. These changes are driven by the acceptance that the separation between medical devices with medical software and health software is no longer sustainable. Indeed, to go further than this, the ISO/IEC Joint Working Group Final Report specifically identifies that risk management in the complex socio-technical environment in healthcare cannot be restricted to the health software itself but must encompass the users, the infrastructure (including security, databases and integration of systems) and environment of operation (JWG7, 2014).

The distinction and separation between the hardware and standalone medical devices, healthcare software, and IT networks supporting health care computing areas is largely from the perspectives of legacy systems, as there are no products being developed in the software field that do not encompass some aspects of traditional medical devices and health IT networks. However, it is taking time for the standards to catch up, and subsequently the revision of existing standards is going through a rigorous process to move the two cultures of medical devices and health software forward in tandem. Indeed, the addition of regulation around medical devices further complicates these issues as well as the formulation of a consistently widely accepted definition of health software. However, in the work on ISO 82304, great emphasis has been placed on the context in which the standard is to be used, to ensure an optimum fit with market need. Consequently, it has attracted strong interest in domains such as the EU, Japan, USA, and China, where regulatory developments are high on the agenda. For instance, the International Medical Device Regulators Forum (IMDRF) published "Software as a Medical Device: Possible Framework for Risk Categorisation and Corresponding Considerations (SaMD)" for comment. Despite worldwide input from many diverse stakeholders including software developers, the definition of what constitutes SaMD is still, highly, medical device centric.

A broader challenge is in the developing area of mobile health, more commonly known as mhealth, which adds a further level of complexity in a growing application and services oriented environment. The divergent but emerging areas in mhealth, trending towards consumer based wellness applications and the other applications supporting the efficient delivery of services and healthcare surveillance, present a new challenge for the standards community (Williams & McCauley, 2013). The mix of consumer health with medical devices is the cause of much discussion and consternation where there is insufficient delineation and separation of broad reference architectures. The past year has seen an abundance of feedback, comment, and disagreement at the highest level of abstraction of what exactly constitutes a medical device, and therefore a cascading failure to be able to define and differentiate between 'traditional' medical devices and other 'mobile' applications.

To overcome the challenges that this produces, particularly in testing, maintenance and accreditation, in addition to development processes, we are seeing further refinement of software development techniques, where products consist of highly specialised modules and sophisticated interfaces that support rich interoperability as well as external data exchange. Some manufacturers are less enthusiastic about external data exchange!

THE NECESSITY FOR HIGHLY SPECIALISED, MODULAR HEALTH SOFTWARE

The impact of the crossover and integration of medical devices, healthcare software, and IT networks supporting health care computing, is that software development has to become more adaptable whilst considering many more factors in its development and deployment. Driving this impact are factors that include safety, accreditation, market agility, configurability, and deployment. At the same time, there are a number of associated

enabling influences to support the development of the necessary move to specialised modular health software, such as technical developments and the increasing adoption of Service Oriented Architecture (SOA) for integration and deployment.

Drivers

Safety: There is a requirement in software development and deployment to ensure that all constituents of the information system are well tested and proven in operation as well as functionality. This demands that it is possible to isolate modules of code, undergoing rapid change due to changing environments, operating systems, and changes to external services (e.g. national identification systems, terminology services, EHRs) to which they interface.

Accreditation requirements: This requires that components subject to accreditation (and regulation) are isolated in modules and are tested individually. Such modules typically undergo a slow rate of change, consistent with the resourcing costs associated with repeated external accreditation. Examples of this include the Australian National Association of Testing Authorities (NATA) accredited testing of the Health Identifiers (HI) Service interface, and in the US context the Office of the National Coordinator for Health Information Technology (ONC) accreditation for meaningful use requirements (CMS.gov, 2014).

Market agility: The ability to bring new user functionality to market rapidly is important for software manufacturers. This functionality encompasses the ability to utilise new capabilities in operating systems, cloud services, hardware, medical devices, and integrated third party software products, so that software can track the latest trends and healthcare best practice. For instance, the ability to correctly deal with new epidemics and to change the software to give more clinical prominence to travel history, as in the case of the recent Ebola event in Dallas (Dvorak, 2014), was critical to patient outcomes. This event has driven rapid change in EMR systems to flag and alert users where specific clinical symptoms and patient circumstances may point to potential Ebola infected patients (Beck, 2014). There is an increasing need for software and EMR systems to respond to clinical requirements, new clinical best practice, incorporation of guidelines, and new deployment of national and local infrastructure. Specialised modular health software allows development in new areas that encompass rapid change whilst maintaining stability in the rest of the product. This has provided an additional driver to the move to data driven software functional configuration and away from traditional code development, in order to satisfy these needs in a timely and cost-effective manner

Configurability: The ability of a single product to address a wider market, and organisational and user requirements, from a single stable code base through extensibility and configuration, contributes to commercial success. Increasingly we are seeing the monolithic products losing market share, giving way to modern technology.

Deployment: Increasingly software developers and manufacturers are looking at zero/small footprint deployment (deployment in a standard web browser or similar interface), where the majority of all functions are web or cloud based with little or no local code. Modular software enables such a gradual transition from thick to thin client and zero footprint deployment. This is becoming a more popular option because of the reduced cost of deployment, reduced costs of maintenance, and timeliness of updates.

Associated Enablers:

A number of technical developments, most notably the increased adoption of SOA, has supported the development of specialised modular health software. Other enablers include software as a service, licencing becoming mainstream (Microsoft and other non-health specific vendors), an increasingly regulated healthcare software environment, and increasing development and testing costs as software and systems complexity continues to follow Moore's law.

The power of, and the ubiquity in, a computing environment that has a range from small cheap portable pc's to smart phones, and the merging of the two technologies, creates an array of opportunities for software development. The next five years will see an even bigger change in this development and operating environment, with mobile applications for health (Barton, 2012). Another powerful enabler is the number of platforms on which software can be deployed. For instance, mobile applications running as desktop programs provide an even larger market for such software. Indeed, clinicians are looking to have the same software capabilities on their phone as their personal computing platform, as well as their hospital and clinical platforms, with transparent data accessibility and automatic user credentialing.

Inevitably, the standards related to healthcare devices, healthcare software and IT networks must undergo a parallel transition and merging with the development of ISO 82304 (health software) and its close relationship to

IEC 62304 (medical device) and ISO 80001 (IT network). We are seeing a convergence, which has recently been crystallised into the report at ISO TC215 on how these standards fit into a unified picture (figure 1). Current developments of these standards are moving them all towards a common approach to health software safety.

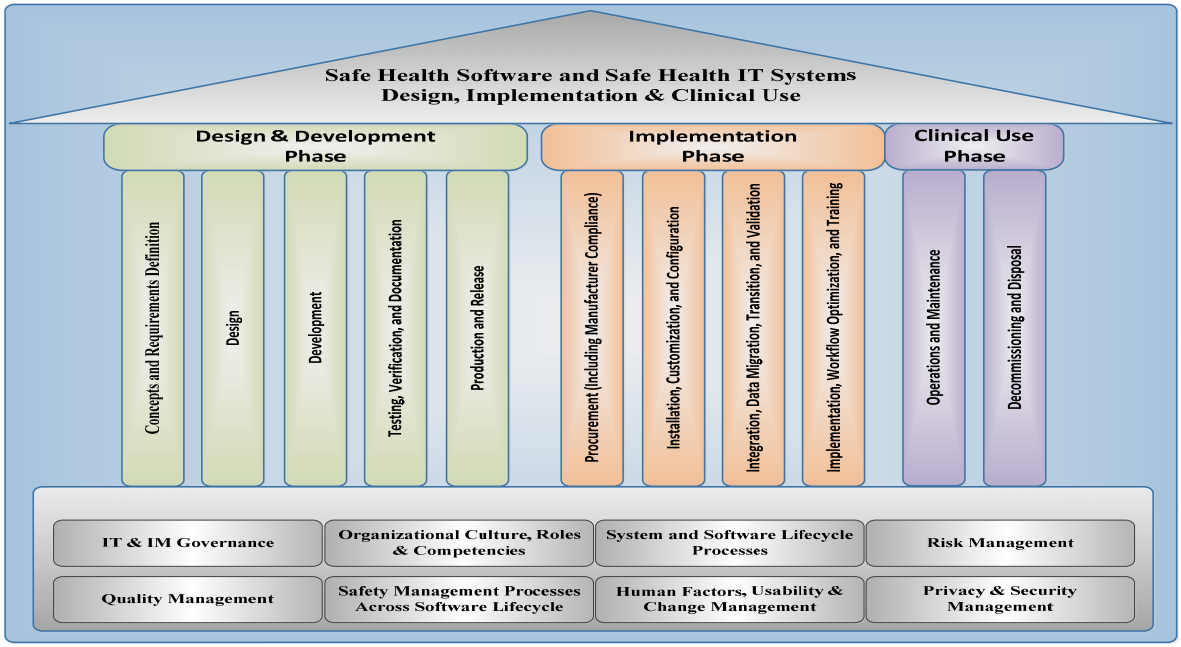

Figure 1 Component model for health software safety standards (JWG7, 2014).

CONCLUSION

The standards community recognises the urgency and importance of guidance and solutions for addressing the risks that HIT poses to patient safety. The current work on ISO/IEC 62304 and ISO/IEC 82304 together with new proposals such as the development of a 'Framework of Event Data & Reporting Definitions for the Safety of Health Software', demonstrates the seriousness with which patient safety resulting from HIT is being considered. The direction that health software is heading (modular, specific, networked) may cause more patient safety concerns in the future. As software becomes more complex, driven by the merger of medical devices, healthcare software, and IT networks supporting health care, errors may be more difficult to detect and examine and root cause analysis of failures extremely difficult. Healthcare information systems already consist of multiple disparate components, and as this increasingly becomes the norm for software, the increased interaction required between these components has the potential to be problematic if not disastrous. It has already been demonstrated that individual software components interacting in ways that were not in the original design can cause patient safety events (McCauley & Williams, 2011).

Ultimately, international standards increasingly need the engagement of all stakeholders and wider collaboration between SDOs. The SDOs are addressing this with new bilateral collaboration agreements forged (IHE and HL7, HL7 and TC215, IHE and TC215, IHTSDO & HL7), demonstrating a new interest in cooperation as the apparent merging of foci occurs. Examples of this are terminology with software modelling, and terminology and deployment and interoperability testing. However, on an individual standards development level, there is still some ground to cover in engaging clinicians, to be gatekeepers in interpreting that the output is both clinically appropriate and safe. This is reflective of the disparate entities currently in the health software development arena.

Software development and deployment has already changed, and standards are just catching up. The need to revise existing standards and develop new ones is recognised, but the clash of cultures is delaying the emergence of standards traditionally developed and governed by separate peak bodies such as IEC and ISO. The impact of this is that whilst standards are being informed by current software trends, standards developers are struggling to assimilate the rapid changes in the market. The disruptive but necessary changes occurring in the health software environment can only be incorporated when the SDOs cooperate more closely, and understand the increased

need for involvement of the software development community in the health software standards processes to narrow the gap in standards relevance. Given the narrow field of experts with appropriate skills, background, knowledge, and experience in software, healthcare, risk analysis, security, privacy, and standards development, the national and international standards development bodies need to ensure that appropriate expert engagement is promoted and supported to lessen the potential for epic failures in patient safety due to healthcare software.

REFERENCES

AHRQ. (2005). *National healthcare quality report 2005*. Agency for Heal;thcare Research and Quality. Retrieved from http://archive.ahrq.gov/qual/nhqr05/nhqr05.htm

Ammenwerth, E., Aly, A. F., Bürkle, T., Christ, P., Dormann, H., Friesdorf, W., . . . Criegee-Rieck, M. (2014). Memorandum on the use of information technology to improve medication safety. *Methods of Information in Medicine, 53*(5), 336-343. doi: http://dx.doi.org/10.3414/ME14-01-0040

Ammenwerth, E, Schnell-Inderst, Petra, Machan, Christof, & Siebert, Uwe. (2008). The effect of electronic prescribing on medication errors and adverse drug events: a systematic review. *Journal of the American Medical Informatics Association : JAMIA, 15*(5), 585-600. doi: http://dx.doi.org/10.1197/jamia.M2667

Ash, J S., Berg, M, & Coiera, E. (2004). Some unintended consequences of information technology in health care: The nature of patient care information system-related errors. *Journal of the American Medical Informatics Association, 11*(2), 104-112.

Barton, A J. (2012). The regulation of mobile health applications. *BMC Medicine 2012, 10*(46). doi: 10.1186/1741-7015-10-46

Beck, M. (2014, Nov 04). The Ebola battle: Hospital records adapt to flag Ebola, *Wall Street Journal,* p. 9. Retrieved from http://ezproxy.ecu.edu.au/login?url=http://search.proquest.com/docview/1619403476?accountid=10675

Black, A D., Car, J, Pagliari, C, Anandan, C, Cresswell, K, Bokun, T & Sheikh, A. (2011). The impact of ehealth on the quality and safety of health care: A systematic overview. *PLoS Medicine, 8*(1), e1000387. doi: 10.1371/journal.pmed.1000387.

CMS.gov. (2014). 2014 Definition Stage 1 of Meaningful Use. Retrieved from http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html

Dvorak, K. (2014). Texas Health backtracks on statement that Epic EHR led to release of Ebola patient. Newton: Questex Media Group LLC.

Goodman, K W., Berner, E S., Dente, M A., Kaplan, B, Koppel, R, Rucker, D, . . . Winkelstein, P. (2011). Challenges in ethics, safety, best practices, and oversight regarding HIT vendors, their customers, and patients: a report of an AMIA special task force. *Journal of the American Medical Informatics Association : JAMIA, 18*(1), 77-81. doi: http://dx.doi.org/10.1136/jamia.2010.008946

JWG7, ISO/IEC. (2014). Health Software Ad hoc group final report: Health software safety standards. Future state, architecture/framework and roadmap IEC collaboration tools.

Kalorama: EMR system unlikely to blame for Ebola-related care mistakes. (2014, Oct 15). *PR Newswire*. Retrieved from http://ezproxy.ecu.edu.au/login?url=http://search.proquest.com/docview/1611733632?accountid=10675

Knaup, P, Ammenwerth, E, Dujat, C, Grant, A, Hasman, A, Hein, A, . . . Haux, R. (2014). Assessing the prognoses on health care in the information society 2013 - thirteen years after. *Journal of Medical Systems, 38*(7), 1-73. doi: http://dx.doi.org/10.1007/s10916-014-0073-6

Leape, L., Berwick, D., Clancy, C., Conway, J., Gluck, P., Guest, J., . . . Isaac, T. (2009). Transforming healthcare: a safety imperative. *Qual Saf Health Care, 18*(6), 424-428. doi: 10.1136/qshc.2009.036954

Magrabi, F., Li, S. Y. W., Day, R. O., & Coiera, E. (2010). Errors and electronic prescribing: a controlled laboratory study to examine task complexity and interruption effects. *J Am Med Inform Assoc, 17*(5), 575-583. doi: 10.1136/jamia.2009.001719

Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E. (2010). An analysis of computer-related patient safety incidents to inform the development of a classification. *J Am Med Inform Assoc, 17*(6), 663-670. doi: 10.1136/jamia.2009.002444

Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E. (2012). Using FDA reports to inform a classification for health information technology safety problems. *J Am Med Inform Assoc, 19*(1), 45-53. doi: 10.1136/amiajnl-2011-000369

Magrabi, F., Ong, Ms, Runciman, W., & Coiera, E. (2011). Patient safety problems associated with heathcare information technology: An analysis of adverse events reported to the US Food and Drug Administration. *AMIA Annu Symp Proc, 2011*, 853-857.

McCauley, V, & Williams, P A H. (2011). Trusted interoperability and the patient safety issues of parasitic health care software. In P. A. H. Williams (Ed.), *9th Australian Information Security Management Conference* (pp. 189-194). Perth: secau- Security Research Centre, Edith Cowan University.

Runciman, W, Hibbert, P, Thomson, R, Van Der Schaaf, T, Sherman, H, & Lewalle, P. (2009). Towards an international classification for patient safety: Key concepts and terms. *International journal for quality in health care : Journal of the International Society for Quality in Health Care / ISQua, 21*(1), 18-26. doi: http://dx.doi.org/10.1093/intqhc/mzn057

Sherman, H, Castro, G, Fletcher, M, Hatlie, M, Hibbert, P, Jakob, R, . . . Virtanen, M. (2009). Towards an international classification for patient safety: The conceptual framework. *International Journal for Quality in Health Care, 21*(1), 2-8. doi: http://dx.doi.org/10.1093/intqhc/mzn054

Stroetmann, V N, Thierry, J-P, Stroetmann, K A, & Dobrev, A. (2007). *eHealth for safety: Impact of ICT on patient safety and risk management in healthcare* (pp. 70). Retrieved from http://www.ehealth-for-safety.org/news/documents/eHealth-safety-report-final.pdf

Williams, PAH, & McCauley, V. (2013, 2nd-4th December, 2013). *A rapidly moving target: Conformance with e-health standards for mobile computing.* Paper presented at the 2nd Australian eHealth Informatics and Security Conference, Edith Cowan University, Perth, Western Australia.