An Exploration of Software Quality Issues in a Connected Health Solution

Chris O'Brien, Shane Whelan, Cian Scanlon, Brian O'Donoghue

May 2, 2014

1 Introduction

This paper examines Connection Health Solutions (CHS) and areas in which software quality issues may occur. This paper is a result of four students with experience in software, but with no experience of its application within the medical field. The areas examined within this paper are those which were of most interest. This paper focuses on the examination of their contribution to the integrity of a CHS.

The research methodology used for this paper, and accompanying software quality plan, was problem based learning (PBL). PBL suggests that for "effective acquisition of knowledge, learners need to be stimulated to restructure information they already know" (Kilroy 2004). This is used to gain new knowledge and learning, which was reinforced in this process by the discussion and exploration of new ideas within a group setting, with the assistance of a person with considerable knowledge in the area.

2 Research

2.1 Medical Devices

One aspect that needs to be considered as part of any CHS are the type of medical devices being used, and their exact use within the CHS. Failures within these devices fall into both hardware and software areas, with software failures rising due to "the rapid increase of software in medical devices" (Wallace and Kuhn 2001). The amount of software within consumer products is now doubling every two to three years (Gibbs 1994).

There are a number of regulations that govern the classification of medical devices. It is important that when designing a CHS to be cognisant of the classification of each device, especially the solution could be deployed in multiple jurisdictions. The classification process in the US, regulated by the Food and Drub Administration (FDA), has been characterized as "slow, risk-aversive and expensive" (Kramer, Xu, and Kesselheim 2012). Conversely, the European Union (EU) process "has drawn criticism for conflicts of interest in its evaluation process" (Kramer, Xu, and Kesselheim 2012). This was highlighted by a recent scandal involving medical devices sold within the EU (Gallagher 2012).

The European Union requirements for classification of medical devices are set out in Annex IX of the Council Directive 93/42/EEC, while the FDA is responsible for this in the United States. In Canada, the Medical Devices Bureau of Health Canada is responsible, while section 41BD of the Therapeutic Goods Act 1989 and Regulation 3.2 of the Therapeutic Goods Regulations 2002 outlines the usage of such devices in Australia, and is under the control of the Therapeutic Goods Administration. Medical Devices are categorised based on level of risk that is attached to its usage.

Class I is a low risk device, Class II is medium risk, Class IIb is higher risk and Class III is highest risk. There are a number of rules which aid the classification of a device. Rules 1 through 4 identify a non-invasive device. An example of this would be a hearing aid. Rules 5 to 8 refer to invasive devices, which is any device intended, by the manufacturer, to be used, in whole or part, to penetrate the body of a human being through a body orifice or through the surface of the body. A key example of this would be an injection. Rules 9-12 cover what are called Active Devices. These refer to devices that are active and implantable. A pacemaker would be an example of an active device. Rules 13 through 18 are special rules. These deal with devices that cover a range of possibilities:

- Devices incorporating integral medicinal substances liable to act in an ancillary

way on the human body;

- Devices used for contraception or prevention of STDs;
- Devices for disinfecting medical devices;
- Devices for recording X-Ray diagnostic images;
- Devices using non-viable animal tissues or derivatives;
- Blood bags;

With the usage of medical devices within a CHS, there needs to be established procedures on how to deal with their handling, storage, disposal, and any training that may be needed by the user, or given to the user. An obvious example is any situation dealing with bladder problems the patient may have a drainage bag and catheter. There would need to be awareness of how to correctly prepare these devices on a patient, and to ensure their proper installation, usage and disposal, and any lack of attention to these areas would lead to high risk of infection.

The ability of medical devices to accurately identify medical incidents was also highlighted as a concern when speaking with a nurse (JH) who works with a CHS. There was concern expressed that there may be events, such as silent seizures, that "technology isn't going to pick up. Maybe if it was more advanced, it might but it's not at that level at the moment" (JH 2014). In this regard, it is important that the CHS suits the medical situation and is not used "to save money on staff" (JH 2014) by introducing the potential for high risk situations.

It is important to ensure that the devices used within the solution are documented, and their regulatory status tracked. Devices may be recalled due to issues discovered after their approval. This will happen when a "medical device is defective, when it could be a risk to health, or when it is both defective and a risk to health" (FDA 2012). A process, such as the Risk Management Capability Model (RMCM), as proposed by Burton, McCaffery, and Richardson 2006 that is used by a medical device manufacturer would be a good indication as to the quality of their medical devices.

2.2 Hardware and Software

2.2.1 Software

Software for connected health is a complicated and diverse field which is lacking in vast research and standardisation. It is also a field that has issues still occurring every day. The importance of security was reinforced this week when Scott Erven's research into the vulnerability of a hospital was widely reported on. His research is unpublished as of time of writing but has been presented at the THOTCON conference. The presentation outlined how Scott was given access to a hospital to run a penetration test as a white-hat hacker. Scott had many disturbing findings such as drug infusion pumps which freely allow hackers to manipulate dosage amounts; Bluetooth enabled defibrillators that can be hacked to deliver random shocks; and medical records that could be altered for malicious means. Scott also found devices with default passwords such as "admin" or "1234" (Zetter 2014). The fact that this research has findings as severe as these in 2014 shows that there is a major clean-up operation to be executed on existing devices and an even bigger change to software process. Software engineers cannot let our profession be tarnished by these schoolboy errors. In this paper we define what we consider to be basic software quality requirements.

Most CHSs are web connected or enabled; this alone is a major security concern. The security of the system itself is vital. The communication protocols utilised must be secure, for example, HTTPS [although older

OpenSSL versions are not secure (OpenSSL 2014)], otherwise patient data could be intercepted in transmission. The database, whether local or remote, must be protected from unauthorised access. A large proportion of security vulnerabilities are due to misconfiguration of the server and the network itself. Examples are the use of default passwords which must be changed and any unnecessary network ports closed. to make sure that configuration is completed successfully, system administrators who are either experienced or extensively trained need to be hired. Potential CHSs may need to provide a training course for users of the system. Training is an area that needs great attention; training should be directed by a certified professional and at regular intervals to keep employees up to date with the system. A CHS needs to be tested against the top ten vulnerabilities released by the OWASP organisation.

There are a number of risks associated with the software development of a CHS. The software will most lightly run on an Operating System (OS) like Windows. The software must have ways of dealing with OS crashes, such as start on reboot and reloading to the same state. The software must take care not to attract attention of antivirus programs which can interrupt and disrupt the functionality of the connected health devices. The software may be evaluated form the point of view of HCI. Its important to remember that the end user of a CHS is going to be a Nurse or Doctor not a programmer. The UI must follow best practices of design to allow for ease of use. Patients themselves may also have to enter data in some solutions, this falls under the same category. Extensive testing should be executed on the system. Most CHSs are connecting with custom built hardware. The connectivity between software and hardware needs to be tested to make sure patient data is entered correctly. There are severe repercussions for saving an incorrect reading from a hardware interface. The system should fail gracefully with human readable error messages if there is a connectivity issue between software and hardware.

The differing levels of authority have to be respected by CHSs. For example the receptionist should not be able to view sensitive patient data, only their appointment schedule or other less sensitive data. Doctors and nurses must have full access. With automated logout activating after a period of inactivity. Two-factor authentication is a must with some form of key card or physical token to authorise users. In a Q&A session where a developer of a CHS and a clinical audit lead from a local hospital were present, it was revealed that password sharing of hospital IT systems is a key issue. It was further discussed that one of the only effective ways to solve the issue is introducing a process for logging in and out; this process is then heavily audited with repercussions for staff if they fail to use the correct login credentials. This is an example of where the software itself can only be so cautious, needing a defined process to actually implement a system.

A CHS should also provide easy to use documentation and a “Help” section that can provide users with information/help as systems may not provide 24/7 support lines. One of the most challenging aspects of the system is the concept of interoperability. Potential systems need to effectively integrate into hospital/GP existing systems some of which are legacy systems that cannot be upgraded. CHSs should provide a combination of APIs and easy export options for data in the system. Integration between 3rd party solutions and between new systems can be challenging but with easy access provided to the data and simplified integration with other components then it becomes a possibility.

The system should provide a method of storing hard copy data from the past. While some hospitals do not have the resources to digitise their paper based records, the option

should be provided for hospitals that do. Patient history in combination with the data from the present day can lead to a more accurate diagnosis or for trends to be spotted. Manual data entry as well as batch processing of data from formats such as CSV should be possible. APIs are also useful for converting data from old systems to new.

While the system should not have any bugs, software can be complex and bugs happen. How a CHS deals with bugs and patch them is important. When dealing with system errors or bugs, systems should notify the user of the error in plain English and log and report the error over the Internet to the developers silently. An ideal implementation of a system is that when a bug is reported silently in the background, developers receive the bug report and it is logged automatically in the defect tracking system.

A CHS should provide a mechanism for developers to update the software remotely. For example Google's Chrome browser updates silently in the background on a reboot of the software, this can go unnoticed to the user. Non-technical people should not be in charge of keeping their systems up to date, this would be ineffective and confuse users.

An assessment will have to be carried out by an IT professional about the eligibility of such a system for patients. Patients may live in rural areas where connectivity and broadband bandwidth may not be as competent as urban areas. An agreement will have to be signed by the patient to allow systems to be installed in their homes.

The possibility of integrating CHSs with emergency services needs to be investigated. If a CHS detects an emergency then the appropriate emergency services need to be notified on a 24/7 basis. Sometimes there can be loss of Internet connectivity but the phone lines still works. On loss of connectivity a CHS should have an emergency backup of dialling a phone number to alert the monitor of a loss in connection. Some patients may be interested in contacting Nurses/Doctors through their CHS. For the patients who can use a computer the system should provide a communication protocol such as video calling or emailing. While this is something that would have a low usage it would be a helpful element of a potential solution.

2.2.2 Hardware

Installation of hardware should be unobtrusive to the users. Patients using a CHS are typically old people who do not want a disruption to their daily lives and to their homes. The point of a CHS is to be discrete and not interfere with the day to day lives of the patients.

Failure of medical devices is of huge concern to the industry. In a general scope, the failure of hardware devices is well documented, with cases such as Amazons hardware failure in 2011 that resulted in their web services going off-line for 48 hours (Wainewright 2011). This was coupled with a previous failure in 2010 where a failure occurred during a peak shopping time in the Christmas period (BBC 2010). In the medical device sector, however, failure is far more serious. Research has been published on the amount of recalls for medical devices; the following figures are just recalls alone and not general faults.

The statistics from research by Wallace and Kuhn 2001 are:

- For the Fiscal Years 1983-1991, there were 2,792 quality problems that resulted in recalls of medical devices, including devices that do not contain software.
- Of those, 165, or 6%, were related to computer software.

The research went on to document the increase in failures related to software, theorising that these failures are as a result of

the increase of devices in the industry. The idea of a rigid software process that follows a framework - such as the framework provided by Shroff, Reid, and Richardson 2011 can be applied to hardware development processes too. In the era of "the internet-of-things" hardware devices should be careful how they expose themselves to failure and hacking. For example, former vice president of the USA Dick Cheney had the Bluetooth feature of his pacemaker disabled to prevent terrorist attacks (Franzen 2013); a rigid hardware and software process should have been in place to prevent issues like this.

2.3 Environmental Issues

The location and environment has a huge impact on any system. When developing health care technology, it is not purely about the technical aspect (O'Neill et al. 2012). There is an emphasis on the human factors, such as usability. Usability of a system relies not just on the interface, but also its situation within an environment. Usability is "a quality attribute that assesses how easy user interfaces are to use" (Nielsen 2003). Nielson describes usability as being made up of five attributes: Learnability, Effciency, Memorability, Errors and Satisfaction (Nielsen 1994). The resources needed and the resources available vary between places, and so this must be taken into account when planning a system. In the case of a CHS, rigorous planning must then be undertaken, as the regulations on each device can be quite demanding. There are a number of important issues which must be considered when planning the development of the CHS.

The system which may be deployed in a patient's residence must be non-invasive, but provide sufficient monitoring so as to ensure its accuracy and integrity. If the equipment set up is extremely complex and difficult to use we must consider who will be available to operate it. In the case of information logging by the patient into the system manually, they are likely to require training. The development of wearable devices could help keep invasiveness to a minimum, using a ring or wristband to monitor the health of the patient (Korhonen, Parkka, and Van Gils 2003). There must be some way to ensure that the information being put through is accurate. Is this the responsibility of the patient or of the system to catch any potential errors? Or should there always be a nurse on-call? What is the level are training required to use the system? These are questions which we must take into account.

The application of mobile phone technology can be utilised in a CHS. In fact, it has been said that the growth of connected health has coincided with the use of smartphones in telehealth. "This trend coincides with the explosion of consumer digital and mobile products" (Landers 2013). This means that the availability of phone coverage is a factor when considering a location of a CHS. Mobile coverage is becoming more widespread as time goes on, but there are still areas where coverage is sparse. It must also be noted that while an area may have strong coverage, it may not have the correct level of coverage to provide acceptable internet speeds. For example, 2G connectivity provides speeds of up to 236kbit/s, where 3G can provide a minimum of 2000kbit/s. A system being set up where the coverage is sparse could mean poor communication between staff and patient. The house itself will also affect the coverage, as thick walls affect phone signal. It is not uncommon that houses have walls thick enough to interfere with this signal, so it is important to be aware of this.

The availability of staff is affected by the location of the patient. If the patient is far away in a remote area the travel time could be quite high. This could mean the difference between being on-call and being on-site in the case of a problem. The types of problems could vary depending on the capabilities

of the system. That is why on-site or on-call will differ from system to system. This must be taken into account when planning the resources needed for staffing. If a member of staff is dedicated to more than one location in the event of an accident, there must be a plan in place for how to deal with both locations at the same time. This could put a strain on the resources even with planning, so being unprepared could cause serious harm. The effect of longer hours due to travelling needs to be taken into account as well. Studies have shown that "the likelihood of making an error increased with longer work hours and was three times higher when nurses worked shifts lasting of 12.5 hours or more" (Rogers et al. 2004).

The level of expertise needed to operate the system must be planned. The users monitoring the system and reading the data must be sufficiently trained. If the wrong staff are in the wrong environment then serious errors could occur. An IT worker not trained properly in the health sector could misunderstand information gathered by the system, considering the medical nature of that data. The location of each staff worker must then be considered. The level of expertise needed to operate the system in the house should be much lower than that of the monitoring system to help minimize risk.

The physical location of the house can have an impact on the system. If broadband is an essential part of the system then the availability of broadband in the area must be investigated. If the location is remote, the risk of downtime to the system must be assessed with regard to patient welfare. Tests must be made prior to the start of the monitoring to ensure that the outcome is in line with exceptions (O'Neill et al. 2012). In the event of a power outage there must be a safety procedure in place. This could include additional resources for the patient or a backup energy source for the crucial systems. A system or device that is rendered inoperable leads to the risk of unsynchronized information. This could lead to patients taking medication at the wrong time, or the system inaccurately assessing the patients situation. If the system is offline, there must a mechanism in place which notifies the staff monitoring the patient. A proposed solution for this could be to have "support contact details mounted on all the relevant devices which will be forwarded to either the in-situ support manager or an answering machine which has to be checked at regular intervals" (O'Neill et al. 2012). A facility should be in place in order to provide an alternative communication link between those monitoring the CHS, and the patient being supported by the system.

If there was such a failure, broadband or otherwise, the speed in which the support team responds to a system alert could potentially be the difference between life and death. Whether the problem is critical or insignificant would not matter, how fast a team can make it to the location at any time of the day must be known. If a monitor goes down in the house of the patient it is far less critical than if a server goes down. The risks must be taken into account and categorized according to their severity. Staff must be available to respond at various levels of speed depending on the severity of the error. Again this reiterates the point that the management of staff and resources available must take into account the potential risks that may occur.

2.4 Data Privacy

When dealing with a CHS there are a lot of concerns with data privacy and the confidentiality of that information. Doctors, Nursing staff and patients must be able to use and trust these electronic medical devices to store and transfer their sensitive information.

"Electronic medical records and other clinical applications, data repositories and analytic tools, connected biomedical devices and

telehealth collaboration technologies all enable connected health. Most importantly, those solutions must rest on a foundation of technology and data standards and security that ensures the confidentiality of personal health information" (Accenture 2012).

As mentioned in the previous medical device section, a medical device data system is any hardware or software product that transfers, stores, convert formats or display medical data and are classified as class 1 medical devices. The Devices must follow standards such as the LEC 62034 Standard which provides a framework of software development lifecycle processes for the safe design and maintenance of medical device software.

One risk associated with the use of a CHS is the actual information captured by the system. Electronic entry of patient notes via manual input or sensors must be transferred securely. The patients personal security number and other confidential information must be encrypted. If the data is in a hospital the data must be maintained correctly. There must be preventions against unauthorised access of user information. The ISO/IEEE 11073 is one such standard which deals with health device communication between medical devices and with external computers. The use of fingerprint, biometrics, passwords and security cards can be used as a safety measure for accessing such data.

How is the data on these medical devices stored and is it secure? Wilcox et al. 2006 have categorised the following architectural models for medical devices which store data as the centralized model, the federated model and the hybrid model.

1. The centralized model is when patients medical data is collected from local sources but stored in a central repository. All information exchanges are routed through the central repository;
2. The federated model: In this model, also called the decentralized model, individual organizations or sub-systems have control of the healthcare record. The individual systems are linked through record locator services that enable them to exchange information;
3. The hybrid model: This model is a mix of the centralized and federated architecture. The patient medical data is usually stored and managed at organizational or regional levels, but information exchange is enabled through a central hub;

Medical devices which are used at the home are constantly in use transferring and receiving information through internet protocols such as HTTPS. The information being transferred must be secure and the correct preventions must be in place in the event of data loss or device malfunction.

A new wireless medical standard, IEEE 802.15.6, was recently developed for a personal area or body area network to be operated at low frequencies over very short range, with long battery life and high data rates. Proponents anticipate that the technology will be used for a very small unobtrusive body-worn device for the exchange of medical information between an implant and a wristwatch receiver.

Other areas that must be considered are the patients privacy rights. The following are the 8 Data Protection Act Principals obtained from the Data Protection Act 1998 (Parliament 1998) which must be considered when dealing with sensitive data:

1. Processed fairly and lawfully;
2. Obtained for specified and lawful purposes;
3. Adequate, relevant and not excessive;
4. Accurate and up to date;

5. Not kept any longer than necessary;
6. Processed in accordance with the "data subjects" (the individuals) rights;
7. Securely kept;
8. Not transferred to any other country without adequate protection;

"The principles of information security require that all reasonable care is taken to prevent inappropriate access, modification or manipulation of data from taking place. In the case of the NHS, the most sensitive of our data is patient record information" (DataProtectionCommissioner 2012).

These principles of information security have identified three main area of concern:

- Information must be secured against unauthorised access - **confidentiality**
- Information must be safeguarded against unauthorised modification - **integrity**
- Information must be accessible to authorised users at times when they require it - **availability**

Over the last fifteen years, IEC 62304 has became the benchmark standard for the development of medical device software, whether standalone software or otherwise, in both the EU and the US. The software in medical devices must adhere to their specific standards to ensure the safety of its users. Patients must also trust these devices and software and have the correct level of usability.

"The privacy issue, too long seen as a barrier to electronic health information exchange, can be resolved through a comprehensive framework that implements core privacy principles, adopts trusted network design characteristics, and establishes oversight and accountability mechanisms" (McGraw et al. 2009).

2.5 Further Research

This paper has discussed a number of issues relating to a CHS. Other aspects, such as Usability, a more in depth look at Risk Management, a closer examination of Software Quality Processes, such as the CMMI and ISO15504, and Training procedures are equally important to a CHS.

2.6 Conclusions

In this paper we have examined 4 key areas that relate to improving the software quality of a CHS. The connected health field of research is a relatively young field with ample scope for further research. Unfortunately this industry doesn't have the luxury of time, therefore many devices are on the market which do not meet the standards for use on humans. As an industry we need to work towards the goal of dependable, usable and precise medical devices.

References

Accenture (2012). *Connected Health: The Drive to Integrated Healthcare Delivery*. URL: http://www.himss.eu/sites/default/files/Accenture-Connected-Health-Global-Report-Final-Web.pdf (visited on 04/30/2014).

BBC (2010). *Amazon knocked offline by 'hardware failure'*. URL: http://www.bbc.com/news/technology-11980125 (visited on 04/27/2014).

Burton, John, Fergal McCaffery, and Ita Richardson (2006). "A risk management capability model for use in medical device companies". In: *Proceedings of the 2006 international workshop on Software quality*. ACM, pp. 3–8.

DataProtectionCommissioner (2012). *The Data Protection Rules*. URL: http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/responsibilities/3bii.htm&CatID=54&m=y (visited on 04/30/2014).

FDA (2012). *What is a Medical Device Recall?* URL: http://www.fda.gov/MedicalDevices/Safety/ListofRecalls/ucm329946.htm (visited on 04/20/2014).

Franzen, C (2013). *Dick Cheney had the wireless disabled on his pacemaker to avoid risk of terrorist tampering*. URL: http://www.theverge.com/2013/10/21/4863872/dick-cheney-pacemaker-wireless-disabled-2007. (visited on 05/01/2014).

Gallagher, James (2012). *PIP breast implants: European Commission says reform needed*. URL: http://www.bbc.com/news/health-16543321 (visited on 04/25/2014).

Gibbs, W Wayt (1994). "Software's chronic crisis". In: *Scientific American* 271.3, pp. 72–81.

JH (2014). private interview.

Kilroy, DA (2004). "Problem based learning". In: *Emergency medicine journal* 21.4, pp. 411–413.

Korhonen, Ilkka, Juha Parkka, and Mark Van Gils (2003). "Health monitoring in the home of the future". In: *Engineering in Medicine and Biology Magazine, IEEE* 22.3, pp. 66–73.

Kramer, Daniel B, Shuai Xu, and Aaron S Kesselheim (2012). "Regulation of medical devices in the United States and European Union". In: *New England journal of medicine* 366.9, pp. 848–855.

Landers, Steven H. (2013). "The case for connected health at home". In: *Cleveland Clinic Journal of Medicine* 80.e-Suppl 1, e–S27.

McGraw, Deven et al. (2009). "Privacy as an enabler, not an impediment: building trust into health information exchange". In: *Health Affairs* 28.2, pp. 416–427.

Nielsen, Jakob (1994). *Usability engineering*. Elsevier.

– (2003). *Usability 101: Introduction to usability*.

O'Neill, Sonja A et al. (2012). "Evaluation of connected health technology". In: *Technology and Health Care* 20.3, pp. 151–167.

OpenSSL (2014). *TLS heartbeat read overrun*. URL: https://www.openssl.org/news/secadv_20140407.txt (visited on 04/20/2014).

Parliament, Irish (1998). *Data protection act of 1998*.

Rogers, Ann E et al. (2004). "The working hours of hospital staff nurses and patient safety". In: *Health affairs* 23.4, pp. 202–212.

Shroff, Vispi, Louise Reid, and Ita Richardson (2011). "A Proposed Framework for Software Quality in the Healthcare and Medical Industry". In:

Wainewright, P (2011). *Lightning strike zaps EC2 Ireland*. URL: http://www.zdnet.com/blog/saas/lightning-strike-

zaps - ec2 - ireland / 1382 (visited on 05/01/2014).

Wallace, Dolores R and D Richard Kuhn (2001). "Failure modes in medical device software: an analysis of 15 years of recall data". In: *International Journal of Reliability, Quality and Safety Engineering* 8.04, pp. 351–371.

Wilcox, Adam et al. (2006). "Architectural strategies and issues with health information exchange". In: *AMIA Annual Symposium Proceedings*. Vol. 2006. American Medical Informatics Association, p. 814.

Zetter, K. (2014). *Its Insanely Easy to Hack Hospital Equipment*. URL: http://www.wired.com/2014/04/hospital-equipment-vulnerable/. (visited on 04/25/2014).