Software Quality Paper

Chris O'Brien
0144266

April 29, 2014

1 Introduction

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 connected health solution are the type of medical devices being used, and their exact use within the connected health system. 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 connected health solution that you are cognisant of the classification of each device, especially if you wish to use the solution 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. Medican Devices are categorised based of what risk 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 connection health solution, 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.

In terms of developing a quality plan for a connected health system, its vitally important that these issues are part of any plan. While the how and why of the classification of devices is not an issue within the scope of the plan, how to deal with, manage, and use these devices is very much an issue that needs to be addressed. The range of devices will differ greatly depending on the connected health system, the environment of the system and even on a patient to patient basis, so in this situation, it is important to break down the system to granular devices and ensure compliance.

2.2 Hardware and Software

2.2.1 Software

There are a number of risks associated with the software of a connected health solution. The software will most lightly run on an Operating System (OS) like Windows. The software must have ways of dealing with OS crashes, like 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 from the point of view of HCI. Its important to remember that the end user of a Connected Health System 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 will have to be done on the system. Most Connected Health systems are connecting with custom built hardware. The connectivity between software and hardware needs to be tested to make sure patient data is being 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.

Most Connected Health solutions are web connected, there is a huge security concern here in multiple categories. The security of the system itself is paramount. The communication protocols used must be secure for example HTTPS, 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 (default passwords must be changed, unnecessary ports closed). To make sure that configuration is completed successfully, system admins who are either experienced or extensively trained need to be hired. The solution may need to provide a training course for users of the system. Training is an area that needs great care, training should be directed by a certified professional and at regular intervals to keep employees up to date with the system. The system needs to be tested against the top ten vulnerabilities released by the OWASP Organisation.

The differing levels of authority have to be respected by our system. For example the receptionist should not be able to view sensitive patient data only something like their appointment schedule. 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.

The system must provide documentation and a Help section that can provide users with information/help as the system may not be provided with 24/7 support lines.

One of the most challenging aspects of the system is the concept of interoperability. The system needs to effectively integrate into hospital/GP existing systems. There are a number of challenges here but we can circumvent them with enough access to data. We can provide a combination of APIs and easy export options for data in the system. Integration between 3rd part options and between our system will be difficult but the more access we provide to the data and the more the system integrates with other components then it becomes a possibility.

The system should provide a method of storing hardcopy data from the past. Patient history in combination with the data from the present can lead to a more accurate diagnosis. Manual Data entry as well as batch processing of data from formats such as CSV should be possible. APIs are also useful so if data is already converted to digital format then the data can be entered via an API.

While the system should not have any bugs, software can be complex and bugs happen. When dealing with system errors or bugs, the system 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 the system would be that when a bug is reported silently in the background that when the developers receive the bug report that it is logged automatically in the defect tracking system.

The system should provide a mechanism for developers to update the software remotely. For example Googles 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 the system up to date, that 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 the system with emergency services needs to be investigated. If the connected health solution 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 the system 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 connected health solution. 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 our solution.

2.2.2 Hardware

Installation of hardware should be unobtrusive to the users. Patients of Connected Health systems are typically old people who do not want a disruption to their daily lives

and to their homes. The point of a Connected Health system is to be discrete and not interfere with the day to day lives of the patients.

2.3 Environmental Issues

The location and environment has a huge impact on any system. When developing health care technology, it is not just about the purely technical aspect. (ONeill 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. 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 Connected Health system, rigorous planning must then be needed, as the regulation on each device can be so demanding. There are a number of important issues which must be considered when planning its development.

The system which will be set up in the house 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 you 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. 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 use of mobile phone technology can be utilised in a connected health system. In fact, it has been said that the growth of connected health has coincided with the use of smart-phones 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 connected health solution. Mobile coverage is becoming more widespread as time goes on, but there are still areas where coverage is sparse. 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 could and would be 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 vary 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 you must have a plan in place for how to deal with both at the same time. This could put a strain on the resources even with planning, so being unprepared could cause serious harm.

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 is in the wrong environment then serious errors could occur. An IT worker not trained properly in the health sector could misunderstand the information gathered by the system if it were too medical. 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 you must check how available the broadband is in the location. If the location is remote then you must consider whether you can afford downtime in the case of a broadband failure. Tests must be made prior to the start of the monitoring to ensure you know what you are dealing with. 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 being shut off leads to the risk of unsynchronized information, this could lead to patients taking medication at the wrong time, or being told theyre in danger. If the system is now down, there must a mechanism in place which notifies the staff monitoring. 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 (ONeill 2012). There should also be a way to make another form of connection to the patient so as to not put them in danger.

If there was such a failure, broadband or otherwise, the speed in which the response team make it to the house could potentially be the difference between life and death. Whether the problem is critical or insignificant would not matter, you must still know how fast a team can make it to the location at any time of the day. There is no knowing when an accident may occur. 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

2.5 Quality Models

2.6 Conclusions

References

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.

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

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.

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.