DEVELOPMENT OF A SOFTWARE QUALITY PLAN FOR HOSPITALS

Vispi Shroff, Louise Reid, Sajid Hashmi, Gerard Mulligan, Daniel Sheehy
Keyang Xiang and Ita Richardson
Department of Computer Science and Information Systems, University of Limerick, Limerick, Ireland

Keywords: Hospital software quality plan, Health care software quality.

Abstract: This paper describes research into the development of a quality plan for the management of software in an Irish Hospital. It studies relevant standards, models and legal acts. Synergies between the Irish Health Service Executive's *Quality and Risk Management Standard* and the *Capability Maturity Model Integration* are utilised to build and study a quality plan. While exploring the possibility of utilising software engineering quality standards to improve the quality standards within health care, this has also led to a greater understanding of the interlinked issues within a hospital.

1 INTRODUCTION

The development of high-quality software is an issue of great and growing importance throughout the software industry (Gillies 1992). Medical software in particular, which includes medical devices with embedded software, can have a major impact on the delivery of patient care. A good quality software system accompanied by poor managerial practices cannot provide the required quality of service. Hospitals face challenges in terms of managing software due to size, complexity of practices, parallel management and resistance to change.

Clinicians are heavily dependent on information to inform decision making on the management of patients. Of concern in the Irish setting is the lack of an integrated electronic patient record system. Without quality software in place, there is little hope of patients benefiting "both directly and indirectly from improved data quality since accurate clinical data are a prerequisite for high standards of care and monitoring." (Forster et al. 2008).

The accuracy of data, and consequently, of information, is determined by the quality of the software systems which produce that data. Within Irish Hospitals there are a number of major and minor systems in place. Patients, clinicians, nursing, information technology, administration, data entry personnel, researchers, governing bodies, and external auditors, have different expectations, understanding and requirements. The increasing use of fourth generation databases such as Microsoft Access is allowing staff with little expertise or knowledge of data quality techniques to gather data that is used in the crucial decision making processes along the patient journey.

Current research yields few solutions to the software quality issue. On reviewing the many papers assessing the quality of clinical data there appears to be a lack of recognition of correctness and accuracy of data – which can be provided through the provision of quality software systems.

Our aim is to address these issues by means of some practical solutions. This paper proposes to deliver an implementation of a software quality plan for Irish hospitals through the use of recognised healthcare and software quality models and standards.

1.1 Research Methodology

A literature review of the major databases of journals from 2000 was performed. This gave us the opportunity to investigate quality issues (Brooks 1987) (Fitzgerald et al. 1979) within hospitals. Interviews with hospital clinicians were also carried out to understand the processes involved in the provision of various inpatient services. Also, existing standards for medical devices and health record collection were investigated.

Shroff V., Reid L., Hashmi S., Mulligan G., Sheehy D., Xiang K. and Richardson I..
DEVELOPMENT OF A SOFTWARE QUALITY PLAN FOR HOSPITALS .
DOI: 10.5220/0003172305870591
In *Proceedings of the International Conference on Health Informatics* (HEALTHINF-2011), pages 587-591
ISBN: 978-989-8425-34-8

Comparing this output with existing software standards, we established which software development processes and practices were relevant to the hospital situation.

For the purposes of implementation, we utilised the Quality and Risk Management Standard (HSE 2007) issued by the Irish Health Service Executive, also known as the HSE. The HSE is an executive body with a mandate to run all the public health services in the Republic of Ireland. This standard was mapped against the best practices in selected processes areas in the Capability Maturity Model Integration, also known as CMMI for Development (SEI 2006). The Data Protection Act 1998 and 2003, IEEE Std. 730-2002 - IEEE Standard for Software Quality Assurance Plans, EUROSOCAP (The European Standards on Confidentiality and Privacy in Healthcare) and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 were also taken into account.

1.2 Quality & Risk Management Standard

The QRMS Standard includes a statement of standard and supporting criteria supported by an internal control model (See Figure 1). There are 3 levels to assess compliance with the standard.

- Level 1- The service has approved documentation which describes the process for managing quality and risk.
- Level 2- The service can demonstrate implementation of the approved documentation.
- Level 3- The service can demonstrate that there are processes in place to monitor the overall effectiveness of the approved documentation.

1.3 Capability Maturity Model Integrated (CMMI)

CMMI is a model based on a collection of best practices that assist organisations in the improvement of their software processes. This model was chosen as it is open and freely available for use. It is widely adopted and validated by numerous companies and across various different industries. While it is heavily used in the software industry, there are also case studies available on the implementation of CMMI in the health care services industry (Forrester 2008).

CMMI was found to be the Model that mapped most successfully to the Irish Health Service's Quality and Risk Management Standard.

Levels 1 and 2 in the QRMS map to the Managed & Defined Levels in CMMI respectively.

Level 3 in the QRMS looks at the control and monitoring of the effectiveness of the processes involved. The Quantitatively Managed and Optimising levels in CMMI facilitate that control and drive towards continuous improvement and optimisation.

This intuitive mapping demonstrates the complimentary nature of standards and models and creates a compelling argument for implementation together.

2 QUALITY MANAGEMENT PLAN

Based on the literature review and interviews of clinicians within the hospitals, the following areas of concern were identified. These areas of concern are then addressed with the QRMS and CMMI models guiding the activities to be carried out.

2.1 Project Planning

Within CMMI, the Project Planning and Project Monitoring and Control process areas bring a degree of structure to the hospital software quality plan. (Cooke-Davies 2002) outlined the importance of project and operations management working together to as a critical factor to achieving project success. When developing the hospital quality plan, following a review of CMMI processes, we developed goals, standards and practices. We also developed a system to constantly review and action the findings of the plan.

The HSE provided the following statement of standard which was adopted for this quality plan "Healthcare quality and risk are effectively managed through the implementation of an integrated quality and risk management system that ensures continuous quality improvement" (HSE 2007, p.5).

Within a hospital quality plan, each software system, its type, interfaces, stakeholders and requirements must be defined. A communication strategy for stakeholders must be developed. The potential risks associated with each s system must be identified and rated according to severity and likelihood. A plan generated and implemented to test each system for Integrity and Availability, the use/under use and fit for use of each system must continually be assessed and improved.

2.2 Risk Management

The use of medical devices and health information systems in a hospital are an inherent risk to the patient. Storing patient information on these systems further exacerbates the level of this risk factor (Sicotte et al. 2006). Failure of software in these systems/devices can have potentially catastrophic effects, leading to injury of patients or even death (Burton et al. 2006).

The complexity of software has long been considered a critical IT project risk factor (Sicotte et al. 2006). Risk Management must be an integral part of software project management processes and include proactive risk assessment and reactive incident management to avoid incidents recurring. (Kavaler & Speigel 2003) define risk management as "an organized effort to identify, assess and reduce where appropriate, risk to patients, visitors, staff and organizational assets". These risks can be wide ranging from scheduling and timing risks to personnel management risks. The hospital's software development team can cope with these classes of software risks by applying appropriate systematic risk management activities to the software development process (Galin 2004).

The CMMI divides Risk Management into three main activities - defining a risk management strategy, identify and analysing potential risks and managing and mitigating risks which do take place. Its purpose is to identify potential problems before they occur so that risk-handling activities can be planned and invoked as needed across the life of the project to mitigate adverse impacts on achieving objectives (Dhlamini et al. 2009).

Risk management for software and systems is not just part of a software quality plan, but should be an integral part of the overall risk management plan for the services which hospitals provide.

2.3 Patient Data Security

Storing patient data in electronic form raises concerns about Patient Privacy and Data Security (Haak et al. 2003). To comply with regulations, software systems and medical devices must guarantee adequate protection of the confidentiality integrity and availability of patient information. The framework outlined in this paper assists a hospital to adhere to the HIPAA Standard, EUROSOCAP and the Data Protection Acts of 1998 and 2003. However, having complete protection of patient data in practice may not be feasible or plausible as it may inhibit the doctor's work (Anderson 1996).

There have been many published breaches of patient information in the Irish press that highlight some major security breaches with regard to medical information (O'Hora 2010). These breaches include unauthorized secondary use of patient records, disclosure of patient records by hackers and commercial vendors, and use of patient records by employers (Baumer et al. 2000). Complying with data security law and regulations is a difficult challenge for hospital managers. Hospital workers demand more and easier access to patient information in order to provide the best care to their patients. Also, vendors of healthcare software use words like flexible, easy-to-use, accessible, streamlined, and multidisciplinary to promote their products. This is at odds with principles of data security which talk about privacy and confidentiality (Waldo 1999).

2.4 Integrity & Availability

Quality data can be defined as data which is fit for use or purpose (Bertoni et al. 2009), (de Lusignan 2006). In addition, (Welzer et al. 2002) state that quality data must be accurate, available, have integrity, consistency, timeliness and completeness. In some cases no data is better than inaccurate data. (Welzer et al. 2002) found that data needs to be modeled correctly first and then be correct, adequate and available. It is then necessary to be quality validated again.

(Bertoni et al. 2009) and (Berndt et al. 2001) recognized the importance of placing emphasis on data analysis when designing a database. This is also backed up in the research by (Treweek & Flottorp 2001) pointing to the fact that it is natural that stakeholders would like to make use of available information but that "a major problem, however, is simply getting at the data

2.5 Verification and Validation

Verification and Validation are the processes which determine "whether or not products of a given development or maintenance activity conform to the requirement of that activity and whether or not the final software product fulfils its intended purpose and meets user requirements" (Abran et al. 2004). Our research demonstrates that a software quality plan for a hospital requires that each system is audited regularly to ensure accurate and complete data. It is inevitable that errors or misunderstandings between data providers and database managers will occur in a highly specialized area. Actions must be

put in place to continually improve both the timeliness and accuracy of the reports. The data managers must receive feedback to ensure continuous quality improvement.

Verification and validation are two distinct process areas within the CMMI-Dev model. On a reactive level, validation through CMMI processes ensures that software and systems currently in use actually do perform the activities they were originally intended for. On a proactive level, validation for new systems and software can take place at all levels of creation of the software and systems, be it at the time of design, implementation or verification.

Verification is the other side of the coin. Having ensured that the software or system being built is the right system, verification ensures that what is being built actually meets the requirements originally set out for the software or system.

3 DISCUSSION

During the course of our research we found that there are many problem areas within hospitals which must be addressed to enhance the quality of service. The root causes of many problems lie in the absence or lack of enforcement of standards, legislation and management processes. Additionally, software systems are often not seen as being governed by the existing health standards. For such use, health standards need to be modified to take software standards into account. Existing research on quality in health care has focused on single issues - little has been done to consider quality of service as a whole. In this research, we have tried to address the overall quality issues in hospitals by focusing on software systems and the definition of relevant quality processes. These ultimately will support guidelines that hospitals may follow to improve their quality of service and avoid many hazards. For future research, we recognise that the validation of this approach is very important and we aim to investigate the advantages and disadvantages of using our proposed plan. We are interested in understanding how quality of service is improved through the implementation and improvement of existing software processes.

4 CONCLUSIONS

This study investigated the problems in relation to software quality, to uncover the root causes of information and data which lacks quality, and to propose the suitable strategies to address the issues. Lack of processes and management of systems and software within the hospital environment results in poor quality of service and makes the goal of patient safety more difficult. Different standards, models, and published literature exist at the moment. However, it is impossible to use any single one to solve the existing diverse and complicated problem. Through literature review and interviews with clinicians, we have identified software process requirements for a hospital quality plan and we have proposed some guidelines based on existing health care standards, quality standards and published resources. We could not address all problem areas in detail; instead we emphasized those issues which were reported by existing literature to be the more critical ones.

Quality assurance is an ongoing process which must be monitored and controlled. Quality assurance and improvement is the responsibility of all stakeholders and these must be involved in all iterations of the quality cycle.

ACKNOWLEDGEMENTS

This work is partially supported by Science Foundation Ireland grant 3/CE2/I303_1 to Lero. This work is also partially supported by TRANSFoRm. TRANSFoRm is partially funded by the European Commission – DG INSFO (FP7 247787).

REFERENCES

Abran, A. et al. eds., 2004. SWEBOK - Guide to the Software Engineering Body of Knowledge, *IEEE Computer Society. Available at: http://www.computer.org/portal/web/swebok/html/contents [Accessed July 23, 2010]*.

Anderson, R. J., 1996. Security in clinical information systems. *Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.31.4380&rep=rep1&type=pdf [Accessed July 22, 2010]*.

Baumer, D., Earp, J. B. & Payton, F. C., 2000. Privacy of medical records: IT implications of HIPAA. *SIGCAS Comput. Soc., 30(4), pp.40–47.*

Berndt, D. J. et al., 2001. Healthcare Data Warehousing and Quality Assurance. *IEEE Xplore, pp.56-65.*

Bertoni, M. et al., 2009. A Case Study on the Analysis of the Data Quality of a Large Medical Database. *In DEXA '09: Proceedings of the 2009 20th International Workshop on Database and Expert Systems*

Application. Washington, DC, USA: IEEE Computer Society, pp. 308–312.

Brooks, J., 1987. No Silver Bullet Essence and Accidents of Software Engineering. *Computer, 20(4), pp.10–19.*

Burton, J., McCaffery, F. & Richardson, I., 2006. A risk management capability model for use in medical device companies. *In WoSQ '06: Proceedings of the 2006 international workshop on Software quality. New York, NY, USA: ACM, pp. 3–8.*

Cooke-Davies, T., 2002. The "real" success factors on projects. *International Journal of Project Management, 20(3), pp.185 - 190.*

Dhlamini, J., Nhamu, I. & Kaihepa, A., 2009. Intelligent risk management tools for software development. *In SACLA '09: Proceedings of the 2009 Annual Conference of the Southern African Computer Lecturers' Association. New York, NY, USA: ACM, pp. 33–40.*

Fitzgerald, M., Hanna, F. & Taylor, D., 1979. The use of a microprocessor in routine cardiac assessment. *Journal of Medical Engineering Technology, 3(4), pp.175-80.*

Forrester, E., 2008. CMMI for Services - Overview Presentation. *Available at: https://bscw.sei.cmu.edu/pub/bscw.cgi/d683162/CMMI-SVC%20Health%20Care%20Example%20v3.ppt [Accessed July 22, 2010].*

Forster, M. et al., 2008. Electronic medical record systems, data quality and loss to follow-up: survey of antiretroviral therapy programmes in resource-limited settings. *Bulletin of the World Health Organization, 86(12), pp.939-947.*

Galin, D., 2004. Software quality assurance: From Theory to Implementation *1st ed., Essex, UK: Pearson Education Limited.*

Gillies, A. C., 1992. Software Quality: Theory and Management, *London, UK, UK: Chapman & Hall, Ltd.*

Haak, M. V. D. et al., 2003. Data security and protection in cross-institutional electronic patient records. *International Journal of Medical Informatics, 70(2-3), pp.117 - 130.*

HSE, 2007. Quality & Risk Management Standard. A*vailable at: http://www.hse.ie/eng/About/Who/OQR009_20080221_v3_Quality_and_Risk_Management_Standard.pdf [Accessed July 22, 2010].*

Kavaler, F. & Speigel, A. D., 2003. Risk Management in Health Care Institutions: A Strategic Approach 2nd ed., London: Jones and Bartlett Publishers, I*nc. Available at: http://books.google.com/books?hl=en&lr=&id=5gwsBRhEd70C&oi=fnd&pg=PR19&dq=Risk+management+in+health+care+institutions:+a+strategic+approach&ots=_ypn09BqTP&sig=2lC0a7dJ2UC_xbb-9y_ynzAIabk#v=onepage&q&f=false [Accessed July 22, 2010].*

de Lusignan, S., 2006. The optimum granularity for coding diagnostic data in primary care: Report of a workshop of the EFMI Primary Care Informatics Working Group at MIE 2005. *Informatics in Primary Care, 14(2), pp.133-137.*

O'Hora, A., 2010. Watchdog warns HSE for repeated security breaches of patient data. Irish Independant. *Available at: http://www.independent.ie/health/watchdog-warns-hse-for-repeated-security-breaches-of-patient-data-2131144.html [Accessed July 22, 2010].*

SEI, 2006. CMMI for Development : Version 1.2. *Available at: http://www.sei.cmu.edu/downloads/cmmi/CMMI-DEV-v1.2.doc [Accessed July 22, 2010].*

Sicotte, C. et al., 2006. A Risk Assessment of Two Interorganizational Clinical Information Systems. *Journal of the American Medical Informatics Association, 13(5), pp.557- 566.*

Treweek, S. & Flottorp, S., 2001. Using electronic medical records to evaluate healthcare interventions. *Health Informatics Journal, 7(2), pp.96 -102.*

Waldo, B. H., 1999. Managing Data Security: Developing a Plan to Protect Patient Data. *Nursing Economic$, 17(1), pp.49 - 52.*

Welzer, T. et al., 2002. Medical Diagnostic and Data Quality. *In Proceedings of the 15th IEEE Symposium on Computer-Based Medical Systems. 15th IEEE Symposium on Computer-Based Medical Systems. IEEE Xplore.*