RESEARCH

Assessing a Hospital's Medical IT Network Risk Management Practice with 80001-1

Francis J. Hegarty, Silvana Togneri MacMahon, Patricia Byrne, and Fergal McCaffery

About the Authors

Francis J. Hegarty is with the Medical Physics and Bioengineering Department at St. James Hospital in Dublin, Ireland. E-mail: fhegarty@stjames.ie.

Silvana Togneri MacMahon is with the Regulated Software Research Centre at the Dundalk Institute of Technology in Dundalk, Ireland. E-mail: silvana.macmahon@dkit.ie

Patricia Byrne is with the Medical Physics and Bioengineering Department at St. James Hospital in Dublin, Ireland. E-mail: psbyrne@stjames.ie

Fergal McCaffery is with the Regulated Software Research Centre at the Dundalk Institute of Technology in Dundalk, Ireland. E-mail: fergal.mccaffery@dkit.ie

Abstract

Medical device interoperability has been identified as a key way of decreasing healthcare costs while improving patient care.[1] This has led to a shift toward placing more medical devices onto information technology (IT) networks. However, placing medical devices onto an IT network may lead to additional risks to safety, effectiveness and security of the devices, the network, and the data. ANSI/AAMI/IEC 80001-1 addresses the roles, responsibilities, and activities that need to be carried out when managing these risks. In this article, we describe an exercise undertaken to assess the medical IT network risk management practice implemented within a hospital to control risk associated with a clinical information system (CIS). The level of compliance with the 80001-1 standard was determined using an assessment framework developed by the Regulated Software Research Centre. The purpose of this exercise was to test and inform the development of an assessment method that is part of the assessment framework for this standard. The exercise also sought to identify how the management of such an existing CIS project meets the requirements of 80001-1.

Introduction

Computer-based, clinical information systems (CISs) collect, store, process, and present the clinical information required to deliver patient care. They assist clinical staff in implementing an evidence-based quality improvement process. We assessed the risk management processes used in the management of a CIS implemented in the critical care units in St. James's Hospital in Dublin, Ireland. The robust system covers 40 patient beds. In the 10 years it has been running, there has been very little downtime associated with its use.

To the casual observer, it may appear as if the purpose of the CIS is to integrate data from the physiological monitors, ventilators, dialysis devices, etc., into the critical care electronic patient record. It is true that the electromedical devices at the bedside are interfaced, as are other systems such as laboratory and the radiology information systems. On closer examination, it becomes clear that the computer at the bedside is also used to prescribe and document delivered medications, and is the repository of the medical and nursing notes. The system allows doctors and nurses to combine information from different sources into one

We assessed the risk management processes used in the management of a CIS implemented in the critical care units in St. James's Hospital in Dublin, Ireland.

system, develop and implement bespoke screen configurations, calculate indices, and structure care plans.

The primary aim of implementing the CIS was to deliver an evidence-based and ongoing clinical transformation program. The process is clinically led and under the governance of the director of the intensive care unit (ICU). It would be a mistake to think of the CIS as a technology system that by itself brings benefits. As much consideration and planning was put into the processes that would govern the use of the system and the quality cycle it would support, as the technology itself. The CIS is a sociotechnical system consisting of people, processes, and technology that together deliver a care process that is standardized, measurable, and operates within a quality cycle. In assessing the risk management processes employed in managing such a system, we need to look not only at the technical components, but also the organizational and social issues surrounding the use of these systems.

Risk Management of Clinical Information Systems that Incorporate a Medical IT Network

A CIS brings many benefits; however, it also brings challenges, many of which are new to hospitals. As the clinical care process is predicated on the availability of the CIS, the reliability of the system as a whole needs to be ensured. Therefore, hospital networks, which form part of the CIS infrastructure, become as important to the delivery of patient care as the ventilators at the bedside. Any network outage can have an immediate impact on that care.

Medical devices are regulated stringently prior to being placed on the market, and standards exist to guide those who manufacture and regulate these devices.[2] Similarly, standards exist to guide those who implement and manage information technology (IT) systems.[3] However, in implementing a CIS a hospital will inevitably place a medical device onto an IT network, and this may result in the device not behaving as intended, or the interaction of the device and other elements of the system may result in the system not behaving as expected. Either of these occurrences could have consequences for the safety, effectiveness, and security of the system as a whole. To ensure that these consequences do not occur, a proactive risk management approach, involving all risk management stakeholders, is required throughout the life cycle of the CIS. This approach needs to be informed by both good practice in medical device and IT system design and management.

ANSI/AAMI/IEC 80001-1 (2010)[4] is a standard that details the roles, responsibilities, and activities required to manage the risk of placing a medical device on an IT network. It defines a medical IT network as an IT network that incorporates at least one medical device. Conformance with the standard requires the hospital to take ownership of risk management of a medical IT network. It also requires the hospital to appoint and resource a medical IT network risk manager who shall be responsible for the management and/or execution of the risk management process used to maintain the safety and effectiveness of the medical IT network. This person should manage both internal and external communications. The person's position in the organization should allow him or her to report the result of risk management processes to the hospitals top management,[4] typically the chief executive office. All stakeholders should be partners in ensuring the safety, effectiveness, and security of the medical IT network, sharing the same vision. No method exists to allow hospitals to be assessed against the requirements of the 80001-1 standard.

All stakeholders should be partners in ensuring the safety, effectiveness, and security of the medical IT network, sharing the same vision.

Risk Management of the CIS In St. James's Hospital

The governance and processes used to implement and manage the CIS in St. James's were put in place in 2003 prior to the publication of 80001-1. They have evolved over time in response to both the expansion of the system and the need to deal with issues as they arose.

The system is under the governance of the director of ICU and managed by a multidisciplinary team (MDT) convened by the ICU director. The MDT consists of doctors, nurses, pharmacists, laboratory scientists, IT professionals, and clinical engineers. A multidisciplinary care team is defined as "a group of healthcare workers who are members of different disciplines, each providing specific services to the patient."[5] The only full-time members of the MDT are two nurses who act as custodians of the configuration/application and provide ongoing training, user support, and system administration. The remainder of the team is drawn from their respective departments. Like other clinical care teams, it has a strong bias toward action with contributing staff involved in problem solving and service delivery. The MDT culture is strongly nonhierarchical, with staff members from different backgrounds contributing to the scientific, managerial, and technical tasks, matching the skills available to the tasks at hand at any given time.

The CIS multidisciplinary team has a role in performing risk management over the life of the system. The risk management program of the CIS is concerned with all aspects of the use of the system, not just those associated with the medical IT network upon which the system is built. It meets regularly to try to imaginatively foresee potential hazards and take steps to eliminate them as part of the ongoing system design. Contingency plans are put in place to cover system failures that might occur for unforeseen reasons. Policies regarding user access, passwords, automatic log off, user roles, etc., are strictly enforced, and the usual protection from malware is implemented. The MDT also manages the change control required over the life of the CIS.

As part of the CIS implementation, there is a requirement to ensure the veracity of data supplied from medical devices and other clinical systems.

As part of the CIS implementation, there is a requirement to ensure the veracity of data supplied from medical devices and other clinical systems. During commissioning of the CIS, the interfaces were validated by clinical engineering (CE).[6] For the purposes of this work, validation was considered as the confirmation by examination and the provision of objective evidence that the particular requirements for a specific intended use are fulfilled.[7] Devices and systems were set up to produce a range of values for each particular test. This information was transmitted, and information presented to the end user was evaluated. Evaluation was twofold: verification that content remained unchanged and verification that the message sent had taken the correct information pathway, through the various interfaces and software mapping tools.[8] This validation exercise required the hospital-based staff to work with the suppliers of the different systems to learn the interface pathways and how to assess them independently. This activity promoted the development of a shared vision between the vendors and the hospital as to how to manage risk. Documentation included a description of the interfaces, outline of the testing procedure, testing acceptance criteria, copy of all test data sets used, end-to-end comparison tables, and testing results.

Methodology

The authors from the Regulated Software Research Centre (RSRC) developed an assessment framework that was based not only on the 80001-1 standard, but also on other standards that informed it.[9-15] The resultant framework can be used to assess the performance of risk management activities throughout the life cycle of a medical IT network. This framework includes a process reference model (PRM), a process assessment model (PAM), and an assessment method. To perform an assessment, an interview based upon a set of scripted questions was conducted for each process. On the basis of the responses to these questions, a capability level can be assigned to each process. This allows strengths and weaknesses in current medical IT network risk management processes to be identified. It also allows for recommendations on how to improve the current risk management processes.

The evaluation was conducted over a three-month period and took the form of a series of meetings structured as an assessment. While the assessment method facilitates self-assessment, in this instance the team at the Regulated Software Research Centre (RSRC) that developed the framework undertook the role of assessors. Where there were difficulties in understanding or interpretation, assessment team members from both the RSRC and hospital suspended the assessment process and worked together to clarify the issues. In this way, the governance and management of the CIS was assessed, the assessment method was refined, and the assessment questions that will be used during future assessments were also tailored to improve their suitability.

Results and Discussion

In this paper, we discuss our experiences in using the first draft of a proposed assessment method. When used in isolation, the PAM was found to be difficult to interpret by the hospital team whose work practices are rooted in hospital culture and healthcare technology management.[16] The assessment exercise was very informative both for the hospital and research teams. Using the PAM as a basis for the assessment enabled the hospital team to familiarize itself with practices common in industry and, in turn, learn from and adapt these approaches to the hospital environment.

The assessment took approximately five days to complete. A significant portion of that time was dedicated to learning how to apply the standard and the associated assessment methodology. This aspect of the work was undertaken by the authors. In total, the multidisciplinary team spent approximately one day working through the assessment methodology.

Working closely with the hospital team also allowed the RSRC team to identify and understand the CE team's particular role as risk management stakeholders and how risk is managed when placing a medical device onto the network.

The approach used is based on the concept of the PAM used to facilitate process improvement in industry. Consequently, the terminology adopted was at times unfamiliar to hospital staff. This highlighted the need for more work to be performed to frame the questions in such a way as take cognizance of the hospital practice and culture.

By far, the greatest deficit of the hospital risk management process identified by the PAM was the lack of adequate documentation of policy. When staff members were assigned to the project full time (the application and support nursing staff), the documentation was better. Similarly, processes undertaken as part of commissioning, such as the validation of the interfaces, were also well documented. However, members of the MDT who have primary roles in their own departments and contribute to the CIS management on a part-time basis rarely have time to document the risk management policy. This is not to say that risk management was not performed, rather that the documentation of the process was lacking.

By far, the greatest deficit of the hospital risk management process identified by the PAM was the lack of adequate documentation of policy.

Medical IT network risk management was performed within a wider CIS system risk management process. This wider process rightly prioritizes elimination of hazards that might affect patient care. When it came to assessing hazards associated with the medical IT network, the attention also was focused on the impact to patient care. The probability of occurrence of potential hazards to the medical IT network was usually low compared to other hazards and often impossible for hospital staff to estimate. Consequently, potential hazards were scored on their likely impact on patient care only.

The use of 80001-1 raised awareness of the need for groups within the hospital to come together and address risk-related issues specific to network technology management. The assessment identified a weakness in how medical IT network risk management is managed on an ongoing basis. The management of the computers in the unit and the network was shared between the CE and the IT groups, but the specific roles undertaken by each were not documented clearly. The technical support to these components was delivered by the different departments using different models. The CE Department manages the devices—including the computers, interfaces, and network connections—at the bedside. The IT Department manages the network infrastructure, which is remote from the patient. The IT Department also manages the software on the bedside computer;

The use of 80001-1 highlighted the need to address risk issues associated with the network technology management that had not been identified to date.

however, this is frequently managed remotely. While the two groups work well together, share information, and contribute to the MDT, the management of the IT components would be improved by implementing a single-documented policy defining how both groups work together to manage these devices as a single system.

The use of 80001-1 highlighted the need to address risk issues associated with the network technology management that had not been identified to date. A review of the vulnerability of the network technology to electrical power outage revealed that not all network components were protected by uninterruptable power supplies (UPSs). Where UPSs were in place, their maintenance and quality assurance varied depending upon which group was responsible for them. Arising from this review, a multidisciplinary project was established with input from the IT, facility engineering, and CE groups to upgrade the power management of the network elements and the associated policy for their ongoing management. This project group also included a senior representative of the hospital's risk management team and the hospital's chief operations officer. Although this project was started, it was not complete at the time this paper was written. It is hoped that the inclusion of senior hospital managers in this group will ensure that there is corporate oversight of the importance of the project in ensuring the reliability of the system.

IEC 80001-1 describes specific roles assigned to individuals, such as the medical IT network risk manager. We found that in a number of cases the attributes being assessed were all in place, but responsibility and resources was distributed among a number of individuals who were part of the MDT. This made assessment difficult. However, after detailed discussion it usually emerged that the processes being assessed were in place, but in a different way from that expected by the authors of the PAM. We found that during the planning and commissioning phase, the role of medical IT network risk manager as described in the standard was undertaken by the lead clinical engineer who acted as project manager for the implementation phase. When major upgrades to the system were being undertaken, or the system expanded, this individual again assumed a project manager role. This individual acted not only as project manager but also as the link between the different professional groups contributing to the project (such as medical, nursing, ICT, finance, and procurement), as well as the system and medical device vendors. Consequently, this person fostered a shared vision among all the stakeholders. Within the procurement documentation, there was clear evidence that detailed consideration had been given to risk management of the CIS as a whole and the medical IT network. The risk management process associated with the ongoing development of the application as part of the MDT quality cycle was undertaken by one of the two full-time nursing staff assigned to the project. This lead informatics nurse had risk management of the application named in her job description, and risk management was a recurring agenda item for the MDT, which meets every two weeks.

The standard also highlights the need for clear responsibility agreements to be put in place between the hospital and the vendors who are contracted to supply or support the CIS system. These were in place as a result of the application of standard healthcare technology management practice and took the form of service contracts. The contract with the main system supplier included a provision for the company representative to participate as required in the CIS MDT in giving advice regarding change control and ongoing application and risk management support. Again, this highlighted how the management fostered the development of a shared vision among all stakeholders. The review of compliance with the responsibility agreements prompted a reassessment of the need for internal memorandums of understanding among different departments who contribute to the CIS project. We found that there was a need to formalize the arrangements among different departments within the hospital who contributed to the MDT. Often the activity and responsibility were more closely associated with the individual, rather than the department they represented. This fact posed challenges when staff members changed their roles or left the organization.

Policy	Assessment Result	Recommendation
Risk management	No documented policy in place	Document risk management policy
Risk acceptability criteria	No documented risk acceptability criteria	Establish risk acceptability criteria
Balancing the three key properties with the mission of the responsible organization	Key properties are balanced on a case-by-case basis. No documented policy for balancing the key properties.	Establish policy to balance key properties with mission of the responsible organization.
Resource	**Assessment Result**	**Recommendation**
Provision of adequate resources	Adequate resources employed in multidisciplinary team	Ensure resources continue to be aware of responsibilities
Assignment of qualified personnel	Resources are adequately qualified to represent perspective of all risk management stakeholders	Ensure all stakeholder groups continue to be represented
Appointment of medical IT network risk manager	Role has been informally assumed by clinical engineering	Formalize position as medical IT network risk manager
Enforcement of responsibility agreements	Responsibility agreements in place and functioning well	Continue to monitor performance of responsibility agreements
Risk Management Process	**Assessment Result**	**Recommendation**
Clear connection to other processes	Multidisciplinary team gives oversight of other processes	Use of multidisciplinary team gives connection to other processes
Ensuring continuing stability and effectiveness	Bring emphasis from project to ongoing risk management	Ensure project best practice is used in day-to-day risk management of medical IT network
Reviewing results at defined intervals	Not currently reviewed	Ensure results of risk management processes are reviewed at defined intervals.

Table 1. Assessment Results Summary

The success of the MDT in implementing good risk management processes has resulted in a system that is useful and robust. This system has been achieved as a result of committed individuals who have worked well together to deliver the sociotechnical system. This success masks the need for the institution to invest in a necessary resource to build, maintain, and document the risk management process that such systems clearly require. The standard rightly identifies a role for corporate management in establishing the governance and structures to support this. However, the drivers for these systems are more often than not clinical, and they tend to evolve and grow out of practice at the unit level. To that extent, they develop bottom up, rather than top down—as confirmed by our assessment. The fact that the director of ICU is responsible for risk management of the medical IT network, which is part of the wider hospital network, highlights that in hospitals the necessary changes in governance structures tend to lag behind the development of novel technologies and systems.

Table 1 provides an overview of the results of the assessment performed at St. James's Hospital and lists the recommendations made to address any weaknesses that were identified as a result of performing the assessment. These results are presented in the context of how current risk management processes address the key deliverables identified in the 80001-1 standard.

Following the assessment, a number of improvements have been implemented. The CE and IT groups have completed a shared mapping exercise to clearly identify all technical components of the network and describe how the network is configured. The MDT held formal meetings with the system supplier to review the responsibility agreements and share information pertinent to risk management processes. In general, the risk management of the system is given a higher priority at MDT meeting and processes associated with change control have been reviewed and improved.

Conclusions

ANSI/AAMI/IEC 80001-1 is valuable to hospitals. The standard sets out the people and processes that need to be in place for a hospital to undertake risk management of medical IT networks. It provides a framework for discussion between those who are advocates for risk management of medical IT networks and top management. However, at first reading the specific provisions detailed in the standard may be difficult to map onto existing hospital structures.

The assessment helped the hospital to identify and protect strengths in the current risk management processes and to spot opportunities for improvement and implement them (See Table. 1).

Because compliance with 80001-1 is measured by inspection of the documentation the hospital has in place, it is clear that for hospitals to become compliant, they will have to change how they support such systems to allow for the complete risk management process to be put in place and documented.

Within St. James's Hospital, the MDT provides an excellent forum within which risk management activities can be undertaken. This works best during project phases in which the members concentrate on achieving a particular milestone, and there is a clear project manager who assumes the role of medical IT network risk manager. The assessment highlighted that ongoing risk management of the medical IT network could be improved, but more resources would be needed to deliver this as part of an ongoing process, not just during "go live" to upgrade projects.

The assessment highlighted that ongoing risk management of the medical IT network could be improved, but more resources would be needed to deliver this as part of an ongoing process, not just during "go live" to upgrade projects.

The use of 80001-1 not only raised awareness of the need for groups within the hospital to come together and address issues related to network technology management, but prompted actions that are being implemented.

To meet both of the objectives set out above, those developing CIS systems in a bottom-up fashion and in response to clinical need must act as advocates with corporate management for the necessary resources to adequately manage these systems. This is particularly so as the complexity and prevalence of CISs increase.

The interaction between the RSRC and the hospital teams allowed the questions used in the assessment method to be rephrased in a way that acknowledged the existing hospital processes and culture, and this work is ongoing. One of the authors is the international project leader for a technical report (80001-2-7) that is under development and which contains the assessment method, PRM, and PAM developed as part of this work. This technical report will allow healthcare delivery organizations (HDOs) to self-assess their conformance with 80001-1. The trial period of the assessment method in St. James's Hospital has allowed the researchers to gain an understanding of current risk management practices within an HDO in a specific context. It also has allowed the development of an assessment method that can be tailored to address varying HDO contexts.

Acknowledgments

This research is supported by the Science Foundation Ireland (SFI) Stokes Lectureship Programme, grant number 07/SK/I1299, the SFI Principal Investigator Programme, grant number 08/IN.1/I2030 (the funding of this project was awarded by SFI under a co-funding initiative by the Irish Government and European Regional Development Fund), and supported in part by Lero—the Irish Software Engineering Research Centre (www.lero.ie) grant 10/CE/I1855.

The authors would like to acknowledge the participation of the members of the Clinical Information System Multidisciplinary Team in St. James's Hospital for supporting this research. ■

References

1. **West Health Institute.** The Value of Medical Device Interoperability: Improving Patient Care with More than $30 Billion in Annual Health Care Savings. March 2013.

2. **IEC.** IEC 60601-1 Medical Electrical Equipment - Part 1: General requirements for basic safety and

essential performance. Edition 3.1. International Electrotechnical Commission: Geneva, Switzerland; 2012.

3. **ISO.** ISO/IEC 20000-1:2011, Information technology—Service Management—Part 1: Service management system requirements. Geneva, Switzerland.

4. **IEC.** IEC 80001-1—Application of Risk Management for IT-Networks incorporating Medical Devices—Part 1: Roles, responsibilities and activities. International Electrotechnical Commission: Geneva, Switzerland; 2010.

5. **Mosby.** *Mosby's Medical Dictionary*. 8th edition. Atlanta, GA. Elsevier; 2009.

6. **Hegarty F, Sheahan N, Walsh C, Fanning B, Ryan T.** Validating a New Clinical Information System: Mapping Data Flow between Systems. *European Journal of Medical Physics*. 2001;XVII(3).

7. **DS/EN/ISO/IEC 17025,** General requirements for the competence to testing and calibration laboratories (first edition). 2000:04-27.

8. **Byrne P.** Validation of Clinical Information System Interfaces. Annual Health Informatics Society of Ireland Conference. 2011.

9. **ISO/IEC, ISO/IEC 15504-2:2003** - Software engineering—Process assessmen —Part 2: Performing an assessment. Geneva, Switzerland; 2003.

10. **MacMahon ST, McCaffery F, Keenan F.** Risk Management of Medical IT Networks: An ISO/IEC 15504 Compliant Approach to Assessment against IEC 80001-1. In: ICSSP San Francisco ACM. 2013:156-160.

11. **MacMahon ST, McCaffery F, Keenan F.** Transforming Requirements of IEC 80001-1 into an ISO/IEC 15504-2 Compliant Process Reference Model and Process Assessment Model, in EuroSPI. Dundalk, Co Louth, Ireland. 2013:11.11-11.18.

12. **MacMahon ST, McCaffery F, Keenan F.** The Approach to the Development of an Assessment Method for IEC 80001-1, in Software Process Improvement and Capability Determination, SPICE. 2013: 37-48. Springer: Bremen, Germany.

13. **MacMahon ST, McCaffery F, Lepmets M, Eagles S, et al.** Assessing against IEC 80001-1. *Healthinf.* 2013:305-308. Barcelona, Spain.

14. **MacMahon ST, McCaffery F, Eagles S, Keenan F, et al.** Development of a Process Assessment Model for assessing Medical IT Networks against IEC 80001-1, in Software Process Improvement and Capability Determination, SPICE. 2012:148-160. Springer: Mallorca, Spain.

15. **MacMahon ST, McCaffery F, Keenan F.** Towards a Process Assessment Model for IEC80001-1. *Healthinf.* 2013:301-304. Barcelona, Spain.

16. **AAMI.** ANSI/AAMI EQ 56:2013 Recommended practice for a medical equipment management program. Arlington, VA:AAMI; 2013.