Using IEC80001-1 to assess a hospital's Medical IT- Network risk management practice.

F. Hegarty [1], S.T. MacMahon [2],P. Byrne [1] and F.McCaffery[2].

[1]. Medical Physics & Bioengineering Department, St James's Hospital, Dublin, Ireland.
[2]. Regulated Software Research Centre, Dundalk Institute of Technology, Dundalk, Ireland

Abstract.

Medical device interoperability has been identified as a key way of decreasing healthcare costs while improving patient care [1]. This has lead to a shift towards placing more medical devices onto IT networks. However, placing medical devices onto an IT network may lead to additional risks to the safety, effectiveness and security. 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 a Clinical Information Systems level of compliance with the IEC 80001-1 standard using an assessment framework developed by the Regulated Software Research Centre (RSRC). The purpose of this exercise was, to test and inform the development of an assessment method which is part of the assessment framework for this standard, and also, to identify how the management of such an existing Clinical Information Systems (CIS) project meets the requirements of IEC 80001-1.

Introduction.

CISs are computer-based systems which collect, store, process and present the clinical information required to deliver patient care. They assist clinical staff in delivering an evidence based quality improvement process. We assessed the risk management processes used in the management of a CIS implemented in a 40 bed critical care unit in St James's Hospital in Dublin, Ireland. This system is well regarded in Ireland as a good example of how to structure and implement a CIS. It is robust and in the ten years it has been running, there has been very little downtime or harm 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 electro-medical 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 the doctors and nurses to combine information from different sources into one system, develop and implement bespoke screen configurations, calculate indices, and structure care plans.

The primary aim of the CIS project was to deliver an evidence based and on-going clinical transformation programme. The project is clinically led and under the governance of the Director of ICU. It would be a mistake to think of CIS as a technology system which in itself brings benefits. As much consideration and planning was put into the processes which would govern the use of the system and the quality cycle it would support, as the technology itself.

The CIS is a socio-technical system consisting of people, processes and technology that together deliver a care process that is standardised, measurable and operates within a quality cycle. In assessing the risk management processes employed in managing such a system, we need to not only look at the technical components but also the organizational and social issues surrounding the use of these systems.

Risk management of clinical information systems that are built of Medical IT networks.

A CIS brings many benefits however it also brings challenges, many of which are new for hospitals to deal with. As the clinical care process is predicated on the availability of the CIS, the reliability of the system as a whole needs to be assured. 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 stringently regulated prior to being placed on the market, and standards exist to guide those who manufacture and regulate these devices [1]. Similarly standards exist to guide those who implement and manage information technology systems [2]. 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 and having unanticipated consequences for the safety, effectiveness and security of the network. To ensure that these consequences do not occur, a proactive risk management approach, involving all risk management stakeholders, is required throughout the lifecycle of the CIS and this approach needs to be informed by both good practice in Medical Device and IT System design and management.

IEC 80001-1 (2010) [3] 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 required 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 report to the Top Management and manage both internal and external communications. All stakeholders should be partners in ensuring the safety, effectiveness and security of the Medical IT Network and there should be a shared vision between them all. No method currently exists to allow hospitals to be assessed against the requirements of IEC 80001-1 standard.

Risk management of the clinical information systems 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 IEC 80001-1. They have evolved over time in response to both the expansion of the system and the need to deal with difficulties as they arose.

The system is under the governance of the Director of ICU and managed by a multidisciplinary team (MDT). The MDT consists of doctors, nurses, pharmacists, laboratory scientists, IT and Clinical Engineers. A multidisciplinary care team is defined as "a group of health care workers who are members of different disciplines, each providing specific services to the patient" [4] and this accurately describes the activity. The only full time members of the MDT are two nurses who act as custodians of the configuration/application and provide on-going training, user support and system administration. The remainder of the team are drawn from their respective departments. The MDT is convened by the Director of ICU. Like other clinical care teams, it has a strong bias towards action with contributing staff involved in problem solving and service delivery. The MDT culture is strongly non-hierarchical, with staff from different backgrounds contributing to the scientific, managerial, and technical tasks, matching the skills available to the tasks in hand at any given time.

The CIS MDT has a role in performing risk management over the life of the system. The risk management programme 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 and imaginatively foresee potential hazards and take steps to eliminate them as part of the on-going system design. Contingency plans are put in place to cover system failures that might occur for unforeseen reasons. Policies regarding user access, use of passwords, automatic log off, user roles etc. are strictly enforced and the usual protection from malware attack is implemented. The MDT also manages the change control required over the life of the CIS.

Methodology.

The authors from the Regulated Software Research Centre (RSRC) team developed an assessment framework which was based not only on the IEC 80001-1 standard but also the other standards which informed it [5-11]. The resultant framework can be used to assess the performance of risk management activities through-out the lifecycle of a Medical IT Network. This framework includes a Process Reference Model (PRM), a Process Assessment Model (PAM) and an assessment method. In order to perform an assessment , an interview based upon a set of scripted questions was conducted for each process area. 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 risk management processes to be identified and recommendations to be provided for actions to be implemented in order 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 RSRC team who developed the framework undertook the role of assessors. Where there were difficulties in understanding or interpretation, both the RSRC and Hospital groups 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 questions which 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. On its own the PAM was difficult in interpret for those whose work practices are routed in hospital culture and based on Healthcare Technology Management [12]. The assessment exercise was very informative both for the hospital and research teams. Using the PAM as a basis for the assessment forced the hospital team to familiarise themselves with practices common in industry and in turn learn from and, adapt these approaches to the hospital environment.

Working closely with the hospital team also allowed the RSRC team to identify and understand the Clinical Engineering team’s particular role as risk management stakeholders and how risk management is currently performed when placing a medical device onto the network, within the hospital culture.

The approach used is based on the concept of the Process Assessment Model 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 cognisance of the hospital practice and culture.

By far the greatest deficit of the hospital risk management process identified by the process assessment model was the lack of adequate documentation. Analysis revealed this was due to lack of protected resources assigned within the hospital to implement CIS projects. Where staff were assigned to the project full time (the application and support nursing staff) the documentation was better. 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 activities associated with the support of the CIS. This is not to say that the risk management processes are not being followed, often excellent processes were in place; however they were often based on an individual's enthusiasm and acumen and not documented within an agreed system.

The Medical IT Network risk management was being undertaken within a wider CIS system risk management process. This wider process rightly prioritises elimination of hazards that might impact on patient care. When it came to assessing hazards associated with the Medical IT Network the same focus on the impact to patient care was evident. 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.

IEC 80001-1 describes specific roles prescribed 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 distributed among a number of individuals who were part of the MDT. This made assessment difficult, although 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. Where major upgrades to the system were being undertaken, or the system expanded, this individual again assumed a project manager role. Being an experienced Clinical Engineer this individual was perfectly placed to understand both the clinical and technical challenges that come with such a system. They acted not only as project manager but also as the synergist between the different professional groups contributing to the project (medical, nursing, ICT, finance and procurement) and also the system and medical device vendors. In doing so, they fostered the shared vision between all the stakeholders which is one of the requirements of IEC 80001-1. Within the procurement documentation, there was clearly evidence that detailed consideration had been given to risk management of the Medical IT Network. However, the risk management process associated with the on-going 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 assessment identified a weakness in how the risk management of the Medical IT Network is managed on an on-going basis. The management of the computers in the unit and the network was shared between the clinical engineering group and the ICT department but there was little clarity around this.

Often the risk management associated with these elements happened within different departments and consequently was not supported by a single overarching policy.

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 provision for the company representative to participate as required in the CIS MDT in the provision of advice regarding change control and on-going application and risk management support. Again this highlighted how the management fostered the development of a shared vision between all stakeholders. Although outside of the scope of IEC 80001-1, the review of compliance with the responsibility agreements prompted a review of the need for internal Memorandums of Understanding between different departments who contribute to the CIS project. We found that there was a need to formalise the arrangements between different departments within the hospital who contributed to the MDT. Often the activity and responsibility was more closely associated with the individual rather than the department they represented and this posed challenges when staff members changed their role or left the organisation.

The success of the MDT in implementing good risk management processes has resulted in a system which is useful and robust. This has been achieved as a result of committed individuals who have worked well together to deliver the socio-technical system. This success masks the need for the institution to invest in a necessary resource to build, maintain and document the risk management process which such systems clearly require. The standard rightly identifies a role for Top 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. The assessment helped us to identify this. 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 tends to lag behind the development of novel technologies and systems.

Following the assessment a number of improvements have been implemented. The Clinical Engineering and ICT 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 that system supplier to review the responsibility agreements and also 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

IEC 80001-1 is valuable to hospitals. It set 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 identify opportunities for improvement and implement these improvements.

The interaction between the RSRC and 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 on-going.

The MDT provides an excellent forum within which the risk management activities can be undertaken. This works best during project phases where 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 on-going risk management of the Medical IT Network could be improved but this would require more resources to deliver this as part of an on-going process, not just during go live to upgrade projects.

Since compliance with IEC 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.

To meet both of the objectives set out above, those developing CIS systems in a bottom up fashion and in response to clinical need, will need to act as advocates with top management for the necessary resources to adequately manage these systems. This is particularly so as the complexity and prevalence of Clinical Information Systems increases.

References

1.IEC, *IEC 60601-1 Medical Electrical Equipment - Part 1: Genaral requirements for basic safety and essential performance*. Edition 3.1 2012, International Electrotechnical Commission: Geneva, Switzerland.

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

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

4. Mosby's Medical Dictionary, 8th edition. © 2009, Elsevier.

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

6. MacMahon, S. T., Mc Caffery, F. & Keenan, F. (2013). Risk Management of Medical IT Networks: An ISO/IEC 15504 Compliant Approach to Assessment against IEC 80001-1. In: *ICSSP San Francisco* ACM. 156 - 160.

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

8. MacMahon, S.T., F. Mc Caffery, and F. Keenan, The Approach to the Development of an Assessment Method for IEC 80001-1, in Software Process Improvement and Capability Determination, SPICE 2013. 2013, Springer: Bremen, Germany. p. 37-48.

9. MacMahon, S.T., F. Mc Caffery, M. Lepmets, S. Eagles, A. Renault, and F. Keenan, Assessing against IEC 80001-1, in Healthinf 2013. 2013: Barcelona, Spain. p. 305 to 308.

10. MacMahon, S.T., F. McCaffery, S. Eagles, F. Keenan, M. Lepmets, and A. Renault, Development of a Process Assessment Model for assessing Medical IT Networks against IEC 80001-1, in Software Process Improvement and Capability Determination, SPICE 2012. 2012, Springer Mallorca, Spain. p. 148 to 160.

11. MacMahon, S.T., F. Mc Caffery, and F. Keenan, Towards a Process Assessment Model for IEC80001-1, in Healthinf 2013. 2013: Barcelona, Spain. p. 301 to 304.

12. ANSI/AAMI EQ 56:2013 Recommended practice for a medical equipment management program. 2013 AAMI, Arlington, USA

Acknowledgements.

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 Science Foundation Ireland 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 (http://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 supporting this research.

1. West Health Institute, *The Value of Medical Device Interoperability - Improving patient care with more than $30 billion in annual health care savings*. 2013.