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

Francis Hegarty[1], Silvana Togneri MacMahon[2], Patricia Byrne[1] and Fergal 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 safety, effectiveness and security of the devices, the network and the data. 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. The level of compliance with the IEC 80001-1 standard was determined 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 that is part of the assessment framework for this standard, and also, to identify how the management of such an existing Clinical Information System (CIS) project meets the requirements of IEC 80001-1.

Introduction.

CISs are computer-based systems that 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 a 40 bed critical care unit in St James's Hospital in Dublin, Ireland. The system is robust and in the ten 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 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 implementing the CIS was to deliver an evidence-based and on-going clinical transformation programme. The process 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 that in 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 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 incorporate a 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 [2]. Similarly standards exist to guide those who implement and manage information technology 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 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) [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 and position in the organization should allow them to be able to report the result of risk management processes to the hospitals Top Management [4], typically the CEO. 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 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 Director of ICU. The MDT consists of doctors, nurses, pharmacists, laboratory scientists, information technology professionals 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" [5] 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 is drawn from their respective departments. 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 multidisciplinary team 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.

As part of the CIS implementation there is a requirement to assure the veracity of data supplied from medical devices and other clinical systems. During commissioning of the CIS the interfaces were validated by clinical engineering [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 setup 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 two fold; Verification that content remained unchanged and verification that the message set 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 system to learn the interface pathways and how to independently access them. This activity promoted the development of shared vision between the vendors and the hospital as to how risk would be managed. Documentation included a description of the interfaces, outline of the testing procedure, testing acceptance criteria, copy of all test data sets used, End/End comparison tables and testing results.

Methodology.

The authors from the Regulated Software Research Centre (RSRC) team developed an assessment framework that was based not only on the IEC 80001-1 standard but also on the other standards that informed IEC 80001-1[9-15]. 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 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. 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 [16]. 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.

The assessment took approximately five days to complete. A significant portion of that time was spent in learning about 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 clinical engineering team's particular role as risk management stakeholders and how risk is managed 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 of policy. Where staff 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 the risk management was not being undertaken, rather that the documentation of the process was lacking.

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. Consequently potential hazards were scored on their likely impact on patient care only.

The use of 80001 raised awareness of the need for groups within the hospital to come together and address risk issue related specifically to network technology management. 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 information technology department but the specific roles undertaken by each were not clearly documented. The technical support to these components was delivered by the different departments using different models. Clinical engineering manage the devices at the bedside including the computers, interfaces and network connections. The information technology department manage the network infrastructure which is remote from the patient. They also manage the software on the bedside computer however this is more often than not done remotely. While both groups work well together, share information and contribute to the MDT, the management of the information technology components would be improved by implementing a single documented policy that set out how both groups would work together to manage these devices as a single system.

The use of 80001 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 Uninterupable Power Supplies (UPS). Where UPS 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 information technology, facility engineering and clinical engineering groups to upgrade the power management of the network elements and the associated policy for their on going management. This project group also included a senior representative of the hospitals risk management team and the hospital Chief Operations Officer. While this project is started at the time of writing it is not complete. 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 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. 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 that 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. 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 standard also highlights the need for clear Responsibility Agreements [4] 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. 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 that 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 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. 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 tend to lag behind the development of novel technologies and systems.

The following table shows an overview of the results of the assessment performed in St. James's Hospital and lists the recommendations made to address any weaknesses which 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 IEC 80001-1 standard.

Policies:		
Policies for:	**Assessment Result:**	**Recommendations**
Risk Management Process	No documented policy in place	Document risk management policy
Risk Acceptability Criteria	No documented risk acceptability criteria	Establish risk acceptability criteria
Balancing the 3 key Properties with the mission of the Responsible Organisation	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 RO.
Resources:		
Resources for:	**Assessment Result:**	**Recommendations**
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	Formalise 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		
Risk Management Process:	**Assessment Result:**	**Recommendations**
Clear Connection to other processes	Multidisciplinary team gives oversight of other	Use of Multidisciplinary team gives connection to

	processes	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

Following the assessment a number of improvements have been implemented. The clinical engineering and information technology 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 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 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 identify opportunities for improvement and implement these improvements (Fig. 1).

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.

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 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.

The use of 80001 not only raised awareness of the need for groups within the hospital to come together and address issue related to network technology management but prompted actions which are currently 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, will need to 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 Clinical Information Systems increases.

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. One of the authors is the international project leader for a technical report (IEC 80001-2-7) which is currently under development which contains the assessment method, PRM and PAM developed as part of this work. This technical report will allow Healthcare Delivery Organisations to self assess their conformance with IEC 80001-1. The trialing of the assessment method in St James's Hospital has allowed the researchers to gain an understanding of current risk management practices within a Healthcare Delivery Organisation in a specific context and has allowed the development of an assessment method that can tailored to address varying Healthcare Delivery Organisation contexts.

References.

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

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

3. 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. 2010, International Electrotechnical Commission: Geneva, Switzerland.

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

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 Vol.XVII No. 3 Jul 2001.

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 assessment — Part 2: Performing an assessment. 2003: Geneva, Switzerland.

10. 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.

11.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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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 St James's Hospital for supporting this research.