Received May 17, 2023, accepted March 12, 2024, date of publication March 25, 2024

# Healthcare Providers' Readiness to Address Medical Device Cybersecurity within the Irish Healthcare System

By Dara Keeley

Biomedical & Clinical Engineering Association of Ireland

## ABSTRACT

Medical devices that can diagnose and treat critically ill patients have become sophisticated and complex. Device manufacturers have been developing these systems to meet market requirements as technology evolves. Combining medical devices and ICT into a distributed medical device IT system can be a solution to incorporating continuous monitoring from the patient bedside to interoperability with a clinical information system. These technology innovations aim to manage patient data and configure medical devices into networked systems that can provide functionality and safety. The implementation of a medical device network solution allows a healthcare provider to take advantage of managing the flow of information to improve clinical work practices and implement a system that can be interoperable with other clinical information systems.

International Electrotechnical Commission (IEC) 80001-1 was developed to assist healthcare providers in identifying and managing the risks associated with medical devices sharing the same IT network with other systems and software. This standard defines roles, responsibilities, and activities in relation to the management of risk with medical devices on an IT network.

This study aims to determine if the standard International Electrotechnical Commission (IEC) 80001-1 is being implemented and determine familiarity with regulations and appropriate standards and guidance for an effective medical device security risk-management program with Irish healthcare providers.

A literature review highlighted the restrictions healthcare providers face in adopting and implementing IEC 80001-1 and the security threats and risks present when integrating medical devices and IT networks. The study research was conducted with clinical engineering members of the Biomedical and Clinical Engineering Association of Ireland (BEAI). This survey targeted BEAI members due to their wealth of experience, knowledge, and skill level in supporting complex medical device systems. An online anonymous survey was created to determine knowledge, awareness, and familiarity with IEC 80001-1 and other medical device security risk-management guidelines.

The study research results revealed low knowledge, awareness, and familiarity among research participants with IEC 80001-1 and guidelines on medical device security risk management. These results were consistent with the literature review that a key to the success of standard adoption is collaboration between stakeholders and a multidisciplinary approach to compliance.

**Keywords** – *Vital Signs, Physiological Monitor, Medical Device, NEWS, Vital Signs Automation, Medical IT Network, Patient Safety, Cybersecurity Risks, IEC 80001:1 Standard, NIST, AAMI TIR57, NIS Directive, ENISA.*

## INTRODUCTION

Physiological monitoring technology has advanced in the last few years, enabling these devices to be incorporated into healthcare providers' networks. This system can provide real-time centralized management of patient monitors, with patients' vital signs being supervised by clinicians, allowing them to recognize and immediately react to clinical conditions through alarm notifications.[1] This clinical information system can be integrated with other hospital information systems, including a laboratory information system (LIS), patient administration system (PAS), and radiology information system (RIS). The greater automation of a provider's information system can be associated with reductions in patient mortality, complications and costs.[2]

The International Electrotechnical Commission (IEC) developed and released a standard to address risks associated with medical devices that share the same IT network with other peripheral devices and software applications. The standard IEC 80001-1, "Application of risk management for IT networks incorporating medical devices – Part:1 Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software", defines roles, responsibilities, and activities that are necessary for risk management, before during and after connecting medical devices to IT infrastructure.[3] The objective of this standard is to prevent adverse incidents and patient harm in three areas - Safety, Effectiveness, and Security, and requires that a comprehensive risk management program be implemented.

### Study Aims

This research study aimed to determine knowledge and awareness of the following within Irish healthcare:

- IEC 80001-1 standard – Application of risk management for IT networks
- incorporating medical devices, defining roles, responsibilities, and activities.
- The restrictions prohibit the adoption of IEC 80001-1 standard and a medical device security risk-management program.
- National Institute of Standards and Technology (NIST) guidelines to secure network-connected medical devices.
- Association for the Advancement of Medical Instrumentation (AAMI) guidance for effectively implementing a medical device security risk-management program.
- A medical device security risk management program.
- Responsibility for implementing and managing a risk management program relating to medical devices incorporated into medical IT networks.
- The National Early Warning Score (NEWS) and the criteria included to calculate the score.
- A digital initiative called Vital Signs Automation (VSA) to capture physiological parameters and automatically calculates the NEWS.

### Literature Review

Medical devices have developed over time to become sophisticated and complex systems that can be incorporated into medical IT networks. This digital transformation can provide benefits to a healthcare provider but can also have the potential to be open to cybersecurity threats that can compromise patient safety.[4] In the European Union, medical devices are strictly regulated by safety protocols; however, when a medical device is integrated into an IT network, it becomes a medical IT network.[5] The standard IEC 80001-1 was developed in 2010 to identify and address inherent risks and to assist with managing these risks. It received several iterations to reduce understanding complexity and enable healthcare providers to engage with implementation. The most recent release is IEC 80001-1:2021, which includes significant technical changes to the application of risk management.

### Search Strategy

A literature review was undertaken to inform the subject matter and develop a substance review for this thesis. The search criteria are outlined in Table 1.

**TABLE 1.** Electronic Search Criteria

| Criteria | English Language |
|---|---|
| Databases | UCD library OneSearch, PubMed, Science Direct, Google, and Google Scholar. |
| Type | Journals, Books, Websites, Standards, Reports, White Papers, Government Publications and Academic Papers. |
| Key Words and "Terms" searched | Vital Signs, Physiological Monitor, Medical Device, NEWS, Vital Signs Automation, Medical IT Network, Patient Safety, Cybersecurity Risks, IEC 80001:1 Standard, NIST, AAMI TIR57, NIS Directive and ENISA. |

## Physiological Monitor

The World Health Organisation (WHO) defines a medical device as, "a*ny instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination for a medical purpose*,"[6] for prevention and screening, diagnose illness, monitor treatments, assist disabled people and to intervene and treat illness, both acute and chronic.

The European Medicines Agency (EMA) defines medical devices as "*products or equipment intended for a medical purpose. In the European Union (EU) they must undergo a conformity assessment to demonstrate they meet legal requirements to ensure they are safe and perform as intended*."[7]

Two new EU laws were enacted in April 2017 relating to medical device regulations (MDR) 2017/745 and in vitro diagnostic medical devices (IVDR) to replace the previous medical device directives. These new regulations aim to address the weaknesses of the previous directives and provide a secure, consistent regulatory framework across all medical devices in the EU market. Clearly defined requirements and specific obligations on stakeholders throughout the supply chain are the main points that stand out with the new regulations.[8]

Patient physiological data from a bedside monitor can be routed to a central station monitor for display, printing, and alarm monitoring. The importance of this workstation cannot be underestimated in allowing clinicians to respond to adverse patient events, reviewing alarm history, and analyzing trend data for research.[9]

The increasing complexity of medical devices, mainly physiological monitors, comes with the ability to monitor multiple vital sign parameters simultaneously with each parameter having the ability to have individual alarms and complex software that can include sub-screens for the clinician to navigate to other devices[10] and systems that include a RIS and LIS.

Clinicians can perform tasks and manage admitting, transferring, and discharging patients, changing alarm limits, storing and retrieving parameter values and trends, and monitoring remote patients.[11] These systems are interoperable with modern electronic health records, enabling patient data to be transferred and populated in real-time.

## IEC 80001-1 Standard

The standard IEC 80001-1:2021, "Application of risk management for IT networks incorporating medical devices – Part:1 Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software", defines roles, responsibilities, and activities that are necessary for risk management, before during and after connecting medical devices to IT infrastructure.[3] The standard applies to responsible organizations, medical device manufacturers, and information technology providers. First published in 2010, with the latest revision released in 2021, the standard was considered too complex and complicated to implement and was revised as a process-based approach to overcome reported barriers, such as a lack of alignment between IT and clinical engineering departments within hospitals and a lack of motivation from management to implement the standard.[12] ISO/IEC/TR 80001, under the general title Application of Risk Management for IT Networks Incorporating Medical Devices are outlined in Table 2.

The role of clinical engineering (CE) / Health Technology Management (HTM) departments will have to evolve to meet the needs of healthcare technology risks and needs, in line with objectives and policies. Alwi et al, found that one of the key elements for successfully implementing this standard was the collaboration between CE / HTM and IT departments.[13]

**TABLE 2.** Application of Risk Management

| Part 1 | Roles, Responsibilities, and Activities |
|---|---|
| Part 2-1 | Step-by step risk management of medical IT networks, practical applications, and examples. |
| Part 2-2 | Guidance for the communication of medical device security needs, risks, and controls. |
| Part 2-3 | Guidance for wireless networks. |
| Part 2-4 | General implementation guidance for Healthcare Delivery Organisations. |
| Part 2-5 | Application guidance for distributed alarm systems. |
| Part 2-6 | Application guidance for responsibility agreements. |
| Part 2-7 | Guidance for Healthcare Delivery Organisations (HDOs) on how to self-assess their conformance with IEC 80001-1. |
| Part 2-8 | Application guidance on standards for establishing the security capabilities identified in IEC 80001-2-2. |

The risk management process has three main phases (Table 3).

**TABLE 3.** Risk Management Process

| | |
|---|---|
| Phase 1 | Risk assessment to identify application hazards and assess risk for each. |
| Phase 2 | Risk evaluation and control to mitigate identified risk and re-evaluate and develop a report. |
| Phase 3 | Post project and operation to continuously monitor and reassess risk. |

With the implementation of this standard's risk management framework, there is a reliance on IT best practices and increasing CE / HTM and IT department convergence. This collaboration is key to ensuring the safe management of medical device IT networks to benefit staff and patients.[13] ISO published a technical report in 2015, ISO/TR 80001-2-7:2015, guidance for healthcare providers to self-assess conformance to the standard. This includes a Process Reference Model (PRM) and Process Assessment Model (PAM) with assessment questions to assist with identifying strengths and weaknesses of the risk management process.[14] In 2016, a technical report, IEC TR 8001-2-8:2016, was developed to guide healthcare providers and medical device manufacturers in identifying security controls and addressing each security capability for the risk management process.[15]

## Standards and Risk Management

The NIST developed a cybersecurity framework (CSF) to enable organizations to protect themselves and continue business operations during an attack. The CSF allows organizations to manage and mitigate cybersecurity risk based on existing standards, guidelines, and practices.[16] As seen in Table 4, CSF is organized into five core functions.

**TABLE 4.** NIST Cybersecurity Framework

| | |
|---|---|
| 1. | Identify physical assets and information to establish a risk management strategy that is tailored to an organisations business function. |
| 2. | Protect the assets and data from malicious attacks or unintentional compromise. |
| 3. | Detect and monitor the environment for security incidents and events. |
| 4. | Respond to attempted or successful attacks. |
| 5. | Recover from the attack and adjust security policies in retrospect. |

The NIST CSF guides healthcare organizations in managing assets, defining their vulnerabilities, and assisting with fending off a growing number of malicious attacks as new digital transformation projects are incorporated.[17]

In 2016, the AAMI published Technical Information Report 57 (TIR57) to provide guidance and assist medical device engineers in integrating cybersecurity risk management into the development of the device so potential threats can be identified and mitigated before placing on the market. TIR focuses on cyber risks and provides steps for identifying and evaluating threats and vulnerabilities, as well as security risk controls and monitoring the ease of use of these controls. The FDA have recognized and approved this standard, reflecting on the requirement for the protection of medical devices as we move toward the transition to digital healthcare.[18]

In 2016, the EU enacted cybersecurity legislation in the form of the Network and Information Systems (NIS) Directive 2016/1148 to enhance cybersecurity across member states. As shown in Table 5, NIS has three parts.

**TABLE 5.** NIS Directive

| | |
|---|---|
| Phase 1 | Risk assessment to identify application hazards and assess risk for each. |
| Phase 2 | Risk evaluation and control to mitigate identified risk and re-evaluate and develop a report. |
| Phase 3 | Post project and operation to continuously monitor and reassess risk. |

The European Network and Information Security Agency (ENISA) is responsible for cybersecurity and implementing the NIS directive to assist member states in identifying good practices, supporting the EU-wide cybersecurity incident reporting process, guidance with common approaches and procedures, and assisting member states in addressing common cybersecurity issues.[19] ENISA has developed good practice guidelines to manage cybersecurity threats with medical devices.

The National Electrical Manufacturers Association (NEMA) developed a voluntary standard in 2008, the Manufacturer Disclosure Statement for Medical Device Security (MDS2), to assist appropriate and responsible persons in assessing security risks in managing medical device security issues. This form allows medical device manufacturers to answer a series of questions covering relevant security capabilities about a medical device and is shared with a healthcare provider.[20]

IEC 27001:2022 was developed for Information Security Management Systems (ISMS) and provided a systematic and comprehensive approach to managing and protecting sensitive information. The standard outlines several requirements that organizations must meet that including developing security policies, performing risk assessments, defining information security roles, managing and maintaining an inventory of assets, training staff to be security aware, developing a business continuity plan, ensuring compliance with GDPR, developing an incident response plan, monitoring the performance of ISMS and restricting access to information to authorized personnel only.[21]

The EU Medical Device Coordination Group developed guidance on cybersecurity for medical devices in 2019 to guide manufacturers on fulfilling all Annex I MDR 745/2017 requirements and IVDR 746/2017 about cybersecurity. Manufacturers must develop products that consider risk-management information security principles and set out minimum requirements concerning IT security measures, including protection against unauthorized access.[22]

Argaw et al. found that building and improving the cyber resilience of a healthcare provider is vital and a shared responsibility. Clinicians and administration staff should be provided with training and practice digital hygiene, while decision-makers should enforce policies that include cybersecurity when making purchasing decisions. Information security teams in hospitals should upkeep security tools to safeguard the provider and patients.[23]

## RESULTS AND ANALYSIS

### Method

The purpose of this project is to conduct research and determine if the standard IEC 80001-1 "Application of risk management for IT networks incorporating medical devices" is being implemented and determine familiarity with regulations as well as appropriate standards and guidance for an effective medical device security risk-management program with Irish healthcare providers. The online questionnaire was hosted by Qualtrics, which could generate a report based on individual feedback on each question posed.

### Question 1, Position

Participants were asked to provide an outline of this current position within clinical engineering, whether working within a hospital setting or working for private enterprise.

| Response | Count | Percentage |
|---|---|---|
| Working within a healthcare provider | 31 | 79 |
| Working for a private company | 8 | 21 |
| Total | 39 | 100 |

### Question 2, Experience

Participants were asked if they had any prior experience integrating medical devices with medical IT networks.

| Response | Count | Percentage |
|---|---|---|
| Yes | 35 | 92 |
| No | 3 | 8 |
| Total | 38 | 100 |

### Question 3, Support

This question asked participants whether they support medical devices integrated with medical IT networks.

| Response | Count | Percentage |
|---|---|---|
| Yes | 36 | 95 |
| No | 2 | 5 |
| Total | 38 | 100 |

### Question 4, Clinical Engineers

Clinical engineers' skills, abilities, and knowledge have expanded to support medical systems that have become more complex with hardware and software technology.

| Response | Count | Percentage |
|---|---|---|
| Strongly disagree | 3 | 8 |
| Somewhat disagree | 1 | 3 |
| Neither agree nor disagree | 4 | 10 |
| Somewhat agree | 7 | 18 |
| Strongly agree | 24 | 61 |
| Total | 39 | 100 |

### Question 5, Responsibility

Who maintains and supports your organization's medical device systems and IT networks?

| Response | Count | Percentage |
|---|---|---|
| Clinical Engineering | 3 | 8 |
| IT Department | 4 | 11 |
| Both Clinical Engineering and IT | 29 | 81 |
| Total | 36 | 100 |

### Question 6, Standards

The importance of standards cannot be underestimated, particularly as they relate to healthcare and patient safety.

| Response | Count | Percentage |
|---|---|---|
| Strongly disagree | 5 | 14 |
| Somewhat disagree | 0 | 0 |
| Neither agree nor disagree | 2 | 6 |
| Somewhat agree | 4 | 11 |
| Strongly agree | 25 | 69 |
| Total | 36 | 100 |

### Question 7, IEC 80001-1

Participants were asked to indicate knowledge and awareness of IEC 80001-1 standard – "Application of risk management for IT networks incorporating medical devices, defining roles, responsibilities and activities."

| Response | Count | Percentage |
|---|---|---|
| Not at all aware | 7 | 19 |
| Slightly aware | 9 | 25 |
| Moderately aware | 17 | 47 |
| Very aware | 1 | 3 |
| Extremely aware | 2 | 6 |
| Total | 36 | 100 |

### Question 8, NIST Guidelines

Participants were asked to indicate familiarity with NIST guidelines to secure network-connected medical devices.

| Response | Count | Percentage |
|---|---|---|
| Not at all familiar | 13 | 36 |
| Slightly familiar | 5 | 14 |
| Moderately familiar | 13 | 36 |
| Very familiar | 2 | 6 |
| Extremely familiar | 3 | 8 |
| Total | 36 | 100 |

### Question 9, AAMI Guidelines

Participants were asked to indicate their level of knowledge and awareness of The AAMI guidance for implementing an effective medical device security risk-management program.

| Response | Count | Percentage |
|---|---|---|
| Not at all aware | 8 | 22 |
| Slightly aware | 12 | 33 |
| Moderately aware | 11 | 31 |
| Very aware | 2 | 6 |
| Extremely aware | 3 | 8 |
| Total | 36 | 100 |

### Question 10, Security

Participants were asked whether a medical device security risk-management program concerning a medical IT network was implemented within your organization.

| Response | Count | Percentage |
|---|---|---|
| Yes | 8 | 22 |
| No | 13 | 36 |
| Don't know | 15 | 42 |
| Total | 36 | 100 |

### Question 11, Implementation

Participants were asked if IEC 80001-1 standard – "Application of risk management for IT networks incorporating medical devices" was implemented within your organization.

| Response | Count | Percentage |
|---|---|---|
| Yes | 4 | 11 |
| No | 10 | 28 |
| Don't know | 22 | 61 |
| Total | 36 | 100 |

### Question 12, Responsibility

Participants were asked who is responsible for implementing and managing a risk management program for medical devices incorporated into medical IT networks.

| Response | Count | Percentage |
|---|---|---|
| Clinical Engineering | 1 | 3 |
| IT Department | 3 | 10 |
| Both Clinical Engineering and IT | 12 | 39 |
| Multidisciplinary Team | 15 | 48 |
| Total | 31 | 100 |
| Total | 36 | 100 |

### Question 13, Restrictions

Participants were asked what they feel are the restrictions prohibiting the adoption of IEC 80001-1 standard and a medical device security risk-management program. Three responses were categorized from research as the main barriers and restrictions to adopting this standard.

| Response | Strongly disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly Agree | Total |
|---|---|---|---|---|---|---|
| Standard is complicated to understand | 0 | 5 | 13 | 11 | 2 | 31 |
| Lack of management support to provide resources | 1 | 2 | 4 | 16 | 8 | 31 |
| Clinical Engineering and IT Department are not aligned | 1 | 1 | 0 | 16 | 14 | 32 |

### Question 14, NEWS

Participants were asked to indicate their level of knowledge and awareness of the NEWS and the criteria included to calculate the score.

| Response | Count | Percentage |
|---|---|---|
| Not at all aware | 6 | 19 |
| Slightly aware | 6 | 19 |
| Moderately aware | 7 | 24 |
| Very aware | 6 | 19 |
| Extremely aware | 6 | 19 |
| Total | 31 | 100 |

### Question 15, Digital NEWS & VSA

Participants were asked to indicate knowledge and awareness of a digital initiative called VSA to capture physiological parameters such as oxygen saturation, blood pressure, pulse rate, heart rate and temperature by automatically calculating the NEWS used to track whether a patient's condition is deteriorating.

| Response | Count | Percentage |
|---|---|---|
| Not at all aware | 10 | 32 |
| Slightly aware | 5 | 16 |
| Moderately aware | 8 | 26 |
| Very aware | 2 | 7 |
| Extremely aware | 6 | 19 |
| Total | 31 | 100 |

## CONCLUSION

### Strengths

A benefit of the survey would be generating a greater awareness among the participants that standards are available for cybersecurity risk management of medical devices and a national initiative, digital NEWS – VSA, being implemented across acute hospital settings—confirmation of the barriers to adopting IEC 80001-1 correlated with the study results.

### Implications of the Research Study

Highlighted by the research findings were the barriers to implementing this standard, with participants surveyed agreeing that the lack of management support to provide resources and a lack of alignment of the clinical engineering and IT departments were the main restrictions to adoption. The literature review highlighted the inherent cybersecurity threats when integrating a medical device into a medical IT network. Healthcare providers and appropriate stakeholders must adopt and implement a cybersecurity risk management program, mainly IEC 80001-1, and ensure compliance to minimize an adverse event or incident.

### Recommendations and Future Research

The research study results highlight the lack of knowledge, awareness, and adoption of standard IEC 80001-1 "Application of risk management for IT networks incorporating medical devices" and a low level of familiarity with regulations as well as appropriate standards and guidance for an effective medical device security risk-management program with Irish healthcare providers. The following recommendations are required at the local

healthcare provider, regional hospital group, and national level for adoption and implementation to be successful:

- Education with the appropriate internal and external stakeholders on the importance of standards and their adoption, focusing on IEC 80001-1. The development of a training resource and identifying with the Health Service Executive (HSE) and healthcare providers management to provide resources in the development of expertise and coordinate the availability of personnel to provide education.
- Enable adoption and implementation of IEC 80001-1 more easily by removing the historical barriers to adoption. HSE management provides guidance and governance to healthcare providers, enabling a simple pathway to compliance.

Increased and close collaboration between all stakeholders is essential for standard adoption and implementation success.

## Conclusion

Medical devices integrated into healthcare providers' IT networks have become more prevalent over the last few years, specifically physiological monitoring. This integration and converging of medical systems with traditional IT networks have transformed the IT architecture and introduced additional risks that may have a bearing on the safety and security of this medical IT network. This was highlighted recently in the HSE with WannaCry ransomware attack in May 2017, and the major ransomware cyberattack suffered in May 2021, causing all the IT systems nationwide to be shut down.

IEC 80001-1 standard was developed to assist healthcare providers in applying risk management and system security to minimize patient safety and infrastructure threats by defining roles, responsibilities, and activities. The NIST provides guidelines to secure network-connected medical devices. The AAMI guides healthcare providers in implementing an effective medical device security risk-management program. This study research highlights the barriers to adoption of IEC 80001-1. It makes recommendations to ensure compliance with the implementation of this standard, particularly with the increasing number of digital transformation projects being realized across acute hospital settings in Ireland.

## REFERENCES


1. KNiubó I and Cartaya M. Implementation of the Multiprocessing in a Central Monitoring Station with 16 Patient Monitors'. World Congress on Medical Physics and Biomedical Engineering, September 7 - 12, 2009, Munich, Germany, Berlin, Heidelberg, 2009: Springer Berlin Heidelberg, 100-103.
2. Amarasingham R, et al. (2009) 'Clinical Information Technologies and Inpatient Outcomes: A Multiple Hospital Study', Arch Intern Med 2009;169(2):108–114.
3. Subhan A. ISO/IEC 80001. Risk Management of Medical Devices on a Network. J Clin Engineer 2016;41(3).
4. Sherman C, Schiano S, Balaouras S, et al.. Best Practices: Medical Device Security. Forrester's Official Website; 2021. Available at: https://reprints2.forrester.com/#/assets/2/1730/RES132003/report.
5. Janssen M and Schrenker R. Guidelines From 80001: Maintaining a Medical IT Network. Biomed Instrumental Tech 2022;45(4):295–9.
6. WHO. Medical Devices. World Health Organisation's Official Website; 2022. Available at: https://www.who.int/health-topics/medical-devices#tab=tab_1.
7. EMA. Medical Devices. European Medicines Agency's Official Website; 2022. Available at: https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices.
8. DOH. Medical Device Regulations (EU) 2017/745 and In Vitro Diagnostic Medical Devices Regulations (EU) 2017/746. Department of Health's Official Website; 2021. Available at: https://www.gov.ie/en/publication/da0cd-medical-device-regulations-eu-2017745-and-in-vitro-diagnostic-medical-devices-regulations-eu-2017746/.
9. Miodownik S. 88 - Intensive Care', in Dyro, J.F. (ed.) Clinical Engineering Handbook. Burlington: Academic Press 2004;373-376.
10. Phillips J, Sowan A, Ruppel H, and Magness R. Educational program for physiologic monitor use and alarm systems safety. Clin Nurse Spec 2020;34(2):50–62.
11. Subramanian S. 98 - Physiologic Monitoring and Clinical Information Systems', in Dyro, J.F. (ed.) Clinical

Engineering Handbook. Burlington: Academic Press; 2004:456-463.

12. MacMahon ST, Cooper T. and McCaffery F. Revising IEC 80001-1: Risk management of health information technology systems', Computer Standards & Interfaces 2018;60:67–72.
13. Alwi R, Prowse P. and Gaamangwe T. Proactive Role of Clinical Engineering in the Adoption of ISO/IEC 80001-1 within Healthcare Delivery Organization. 2020: IEEE, 5623-5626.
14. ISO IEC/TR 80001-2-7:2015, Application of risk management for IT-networks incorporating medical devices — Part 2-7: Application guidance — Guidance for Healthcare Delivery Organisations (HDOs) on how to self-assess their conformance with IEC 8001-1. ISO's Official Website; 2015. Available at: https://www.iso.org/obp/ui/fr/#iso:std:63509:en.
15. ISO. IEC/TR 80001-2-8:2016, Application of risk management for IT-networks incorporating medical devices — Part 2-8: Application guidance — Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2. ISO's Official Website; 2016. Available at: https://www.iso.org/standard/64635.html.
16. Calder A. NIST Cybersecurity Framework: A Pocket Guide. Ely, UNITED KINGDOM: IT Governance Ltd; 2018.
17. Symantec. Adopting the NIST Cybersecurity Framework in Healthcare. Broadcom Corporation's Official Website; 2018. Available at: https://docs.broadcom.com/doc/adoping-the-nist-cybersecurity-framework-in-healthcare-en.
18. Yuan S, Fernando A. and Klonoff DC. 'Standards for Medical Device Cybersecurity in 2018. J Diabet Sci Technol 2018;12(4):743–746.
19. ENISA. NIS Directive. European Network and Information Security Agency's Official Website; 2022. Available at: https://www.enisa.europa.eu/topics/nis-directive.
20. AAMI.org. What You Need to Know About the New MDS2. Association for the Advancement of Medical Instrumentation Official Website; 2020; Available at: https://array.aami.org/content/news/you-need-know-new-mds2
21. CertificationEurope.com. ISO 27001. Certification Europe's Official Website; 2024. Available at: https://www.certificationeurope.com/iso-certification/iso-27001/
22. EU. MDCG 2019-16 Guidance on Cybersecurity for medical devices. European Commission's Official Website; 2020. Available at: https://health.ec.europa.eu/medical-devices-sector/new-regulations/guidance-mdcg-endorsed-documents-and-other-guidance_en
23. Argaw ST, et al. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Informat Dec Mak 2020;20(1):146.