Security of Patient Monitoring on a Medical IT Network

Clinical Engineering Department, Our Lady's Hospital Navan

Dara Keeley

BEAI Annual Scientific Conference 2022

Background

Physiological monitoring technology has advanced the last number of years to enable these devices to be incorporated onto healthcare provider's networks. The difficulties faced by providers in relation to cybersecurity of infrastructure and medical device systems were highlighted recently with the WannaCry ransomware attack in May 2017 and a major ransomware attack suffered by the Health Service Executive (HSE) in May 2021.

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 [1]. Aragaw et al., recommend that improving cyber resilience within a healthcare provider is a shared responsibility [2].

Objectives

A research study to determine knowledge, familiarity and awareness within Irish healthcare of:

- IEC 80001-1 standard.
- The restrictions present that prohibit the adoption of IEC 80001-1 standard and 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.

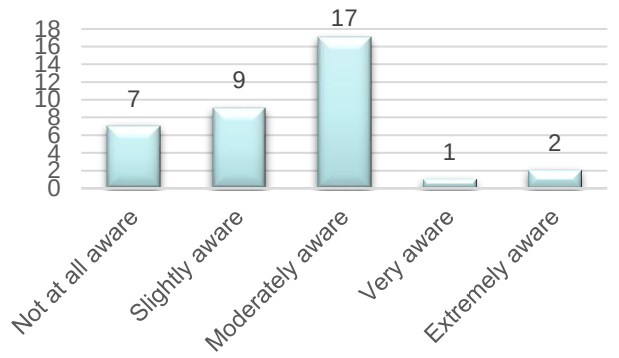
Method

An online anonymous questionnaire using the Likert scale was developed to survey Clinical Engineering members of the Biomedical and Clinical Engineering Association of Ireland.

This group was selected to participate due to the extensive level of knowledge and experience of integrating medical devices onto medical IT networks and the support of these systems.

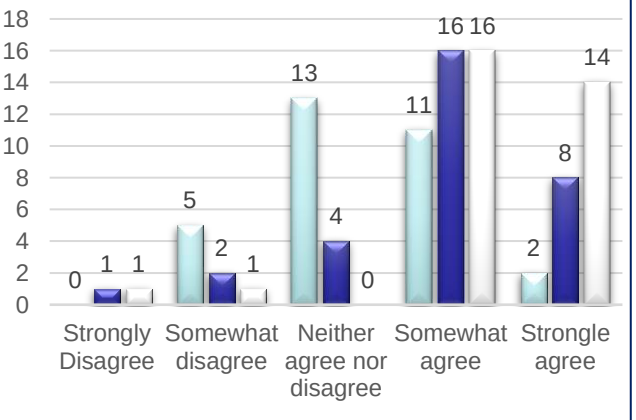
Results

1. IEC 80001-1 Standard



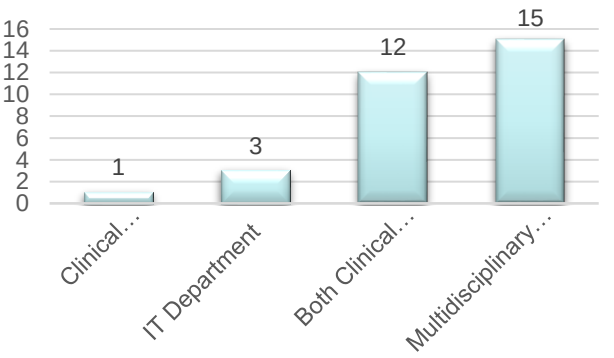
- Thirty-six respondents indicated that 19% were not at all aware, 25% were slightly aware, 47% were moderately aware, 3% were very aware and 6% extremely aware of this standard.

2. Restrictions that prohibit adoption



- Thirty-one responded for the standard being complicated to understand with 0% strongly disagreeing, 16% somewhat disagreeing, 42% neither agreeing or disagreeing, 35% somewhat agreeing and 6% strongly agreeing.
- With the lack of management support providing resources to implement the standard, 3% strongly disagreeing, 6% somewhat disagreeing, 13% neither agreeing or disagreeing, 52% somewhat agreeing and 26% strongly agreeing.
- Clinical Engineering and IT Department not being aligned with 3% strongly disagreeing, 3% somewhat disagreeing, 0% neither agreeing or disagreeing, 50% somewhat agreeing and 44% strongly agreeing.

3. Responsibility for implementing



- Thirty-one responses showed 3% believed Clinical Engineering was responsible, 10% believed the IT Department was responsible, 39% believed it was a shared responsibility between Clinical Engineering and IT Departments, while 48% believe a multidisciplinary team should manage this responsibility.

Conclusion

A multidisciplinary team should be tasked with implementing and managing a cybersecurity risk management program.

Changes are required to human behaviour, technology and healthcare provider processes to alleviate threats.

A suggestion to overcome restrictions would be digital hygiene education and heightened awareness with the development and implementation of education programs targeted at the appropriate stakeholders both internally and externally to healthcare providers. This would assist with the adoption and implementation of the IEC 80001-1 standard.

References

1. Subhan, A. (2016) 'ISO/IEC 80001 (Risk Management of Medical Devices on a Network)', *Journal of Clinical Engineering,* 41(3).

2. Argaw, S. T. *et al.* (2020) 'Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks', *BMC Medical Informatics and Decision Making,* 20(1), pp. 146.