

Midocean University

Management

Risk Management

Controlling the cybersecurity Risk of the Medical Devices in Healthcare

NAHID ELTAYEIB HASSABELGOWI YOUSIF

221001105

Main Supervisor :AlFaisal Abdelhameed

Second Supervisor: Faiz Grad

Year: 2024

Introduction:

Introduction to Cybersecurity in Healthcare Clinical machinery such as patient monitors, infusion pumps, and diagnostic imaging can be manipulated and abused as they interact with patients, with the expectation of causing danger. Cybersecurity flaws are equally distributed in pacemakers, defibrillators, and numerous systems utilized in hospital settings, notably in older devices. Although Electronic Medical Records (EMR) have different data confidentiality and integrity concerns, the multi-purpose and/or computationally oriented characteristics are more promotional in comparison to clinical tools. In contrast, the utilization of these data collection applications and storage functions allows them to be used in different purposes such as ransomware attacks. Some of the EMR devices are included in the provision of productive tools for managing healthcare data and not just the previous administration or storage of a single processing activity that repeatedly happens at scheduled times. The need for resources has proven their thorough potential effectiveness to other hackers. Cybersecurity is becoming a critical part of healthcare due to the increasing reliance on large-scale, complex networks linked to electronic medical records and healthcare information systems with transferable patient data. Healthcare facilities have clinical machinery that is wide-ranging and extensive in scale. These systems consist of various vulnerable portals, which, combined, define the healthcare infrastructure's intrinsic vulnerability as a whole.

Medical devices, patient information, and other elements are valuable targets for ransomware and other malicious cyber-physical-element disruptions. Protecting the devices is critical to ensuring that the essential healthcare services they administer continue to function correctly and securely in order to protect or enhance patient safety.

1.1. Importance of Cybersecurity in Medical Devices

Comprehensive end-to-end risk management, alignment, and oversight are important for controlling cybersecurity risks in medical devices in order for general provision and therapy care to function in the healthcare delivery facility without interruption or disruption. Control of cyber risks for devices is also necessary to secure sensitive personal data that is passed through and stored on a device to ensure that it is not exposed to people not authorized to access it. The goal of a risk management plan for medical devices is to recognize, estimate, review, and manage risk levels in each use set so that the consumer and long-term healthcare technology objectives are consistent. Cybersecurity in medical devices can allow unauthorized access to secure patient identity data, confidential personal data, and affect a patient's diagnosis and procedure or time-sensitive health supplies, placing a patient at unacceptable risk of harm if false data are caused by device error triggered.

The Study of the Problem:

Despite the critical role of medical devices in patient care, many healthcare institutions lack comprehensive strategies to address the cybersecurity risks associated with these devices.

Vulnerabilities in medical devices can lead to unauthorized access, data breaches, and operational disruptions, posing severe risks to patient safety and the overall healthcare system.

The problem is exacerbated by the following factors:

1. **Outdated Software:** Many medical devices run on outdated software, making them susceptible to known vulnerabilities.
2. **Lack of Standardization:** There is a lack of standardized cybersecurity practices across different healthcare institutions and medical device manufacturers.
3. **Complex Regulatory Environment:** Navigating the complex regulatory requirements for medical device security can be challenging for healthcare providers.
4. **Limited Awareness and Training:** Healthcare professionals often lack adequate training on cybersecurity risks and best practices for mitigating these risks.

The importance of studying:

1. Patient Safety

Medical devices play a critical role in patient care, often supporting vital functions and administering essential treatments. Cybersecurity breaches can compromise device functionality, leading to:

- 1.1. Malfunctioning Devices:** Hacked devices can malfunction, delivering incorrect dosages or failing to monitor vital signs accurately, posing direct threats to patient safety.
- 1.2. Delayed Treatments:** Cyberattacks that disable medical devices can result in delays in critical treatments, jeopardizing patient outcomes.

2. Data Integrity and Privacy

Medical devices often collect and transmit sensitive patient data, which must be protected to maintain:

- 2.1. Confidentiality:** Unauthorized access to patient data can lead to breaches of patient confidentiality, eroding trust between patients and healthcare providers.
- 2.2. Integrity:** Cyberattacks can alter or corrupt patient data, leading to incorrect diagnoses and inappropriate treatments.

- 2.3. Compliance:** Ensuring data protection is crucial for compliance with regulations like HIPAA (Health Insurance Portability and Accountability Act), which mandates the protection of patient information.

3. Operational Continuity

Healthcare facilities rely on the continuous operation of medical devices to provide uninterrupted patient care. Cybersecurity incidents can disrupt these operations by:

- 3.1. Device Downtime:** Attacks that disable devices can lead to downtime, affecting the facility's ability to deliver timely care.
- 3.2. Resource Strain:** Responding to cybersecurity incidents diverts resources away from patient care to address the breach, increasing operational strain.

4. Economic Impact

Cybersecurity breaches can have significant financial repercussions for healthcare providers, including:

- 4.1. Recovery Costs:** Costs associated with mitigating breaches, including device repairs, data recovery, and system upgrades.
- 4.2. Legal Liabilities:** Potential legal fees and settlements resulting from breaches of patient data or compromised care.

- 4.3. Reputation Damage:** Loss of trust can lead to a decline in patient numbers, impacting revenue and the facility's standing in the healthcare community.

5. Regulatory Compliance

With increasing regulations governing the cybersecurity of medical devices, healthcare providers must:

- 5.1. Adhere to Standards:** Comply with standards set by regulatory bodies, such as the FDA's guidelines on medical device cybersecurity.
- 5.2. Prepare for Audits:** Ensure readiness for audits and inspections by maintaining robust cybersecurity measures.

6. Technological Advancement

Studying cybersecurity risks promotes innovation by:

- 6.1. Developing Secure Devices:** Encouraging manufacturers to integrate advanced security features into new devices.
- 6.2. Enhancing Existing Infrastructure:** Motivating healthcare providers to upgrade and secure their current technology infrastructure.

7. Broader Implications for Public Health

Cybersecurity threats to medical devices have far-reaching implications, including:

7.1. Pandemic Response: Secure medical devices are crucial for effective monitoring and treatment during public health crises, such as pandemics.

7.2. National Security: Protecting healthcare infrastructure is a component of national security, as large-scale cyberattacks could destabilize public health systems.

8. Contribution to Knowledge and Best Practices

Conducting research in this field contributes to the broader body of knowledge by:

8.1. Identifying Vulnerabilities: Highlighting common security gaps and vulnerabilities in medical devices.

8.2. Sharing Best Practices: Disseminating best practices and effective strategies for mitigating cybersecurity risks.

8.3. Informing Policy: Providing data and insights that can inform policy decisions and regulatory frameworks.

The study of cybersecurity risks associated with medical devices is of paramount importance to ensure patient safety, protect data integrity, maintain operational continuity, comply with regulations, manage economic impacts, foster technological advancement, and contribute to public health and national security. This research will not only help healthcare providers and device manufacturers mitigate current risks but also prepare for future challenges in an increasingly connected healthcare environment.

Objectives of the study:

1. Identify Common Cybersecurity Vulnerabilities in Medical Devices

- 1.1. Detailed Analysis:** Conduct a systematic analysis to identify and categorize the most prevalent cybersecurity vulnerabilities in medical devices.
- 1.2 Device Classification:** Examine different types of medical devices (e.g., diagnostic, therapeutic, monitoring) to understand specific vulnerabilities associated with each category.

2. Evaluate Current Cybersecurity Practices in Healthcare Settings

- 2.1. Survey and Interviews:** Conduct surveys and interviews with healthcare professionals and IT security experts to assess the effectiveness of current cybersecurity measures.
- 2.2. Case Studies:** Analyze case studies of healthcare institutions that have experienced cybersecurity incidents to understand how these were managed and resolved.

3. Assess the Gaps in Existing Cybersecurity Measures

- 3.1. Comparative Analysis:** Compare current practices against established cybersecurity frameworks and standards to identify gaps and weaknesses.

- 3.2. Regulatory Compliance:** Evaluate the level of compliance with existing regulations and standards, such as those from the FDA, HIPAA, and international guidelines.

4. Develop a Comprehensive Cybersecurity Risk Control Framework for Medical Devices

- 4.1. Framework Design:** Propose a structured framework that integrates best practices, standards, and innovative approaches to mitigate cybersecurity risks.
- 4.2. Implementation Guidelines:** Provide clear guidelines and protocols for healthcare providers to implement the proposed framework effectively.

5. Provide Actionable Recommendations for Healthcare Stakeholders

- 5.1. Healthcare Providers:** Offer specific recommendations to healthcare providers on how to enhance their cybersecurity posture, including staff training, device management, and incident response.
- 5.2. Device Manufacturers:** Suggest improvements in the design and development of medical devices to embed robust security features.
- 5.3. Policy Makers:** Advise policymakers on necessary updates to regulations and standards to address emerging cybersecurity threats.

6. Raise Awareness and Promote Best Practices in Medical Device Cybersecurity

- 6.1. Educational Materials:** Develop educational materials and resources to raise awareness among healthcare professionals about the importance of cybersecurity in medical devices.
- 6.2. Workshops and Seminars:** Organize workshops and seminars to disseminate findings and promote best practices in medical device cybersecurity.

7. Contribute to the Body of Knowledge in Healthcare Cybersecurity

- 7.1. Academic Publications:** Publish research findings in academic journals and present them at relevant conferences to contribute to the academic and professional discourse on medical device cybersecurity.
- 7.2. Continuous Improvement:** Encourage ongoing research and development in the field by identifying areas needing further investigation and innovation.

8. Enhance Patient Safety and Trust in Healthcare Systems

- 8.1. Risk Mitigation:** By addressing cybersecurity risks, improve the safety and reliability of medical devices, thereby enhancing overall patient safety.

8.2. Building Trust: Strengthen trust between patients and healthcare providers by demonstrating a commitment to protecting patient data and ensuring the safe operation of medical devices.

By achieving these objectives, the study aims to provide a comprehensive understanding of the cybersecurity challenges faced by medical devices in healthcare and to propose practical solutions to mitigate these risks, ultimately leading to safer and more secure healthcare environments.

Study questions:

- 1. What are the most common cybersecurity vulnerabilities found in medical devices?**
 - 1.2. How do these vulnerabilities vary across different types of medical devices?
 - 1.3. What are the underlying causes of these vulnerabilities (e.g., outdated software, lack of encryption)?
- 2. How effective are current cybersecurity practices in healthcare settings at mitigating risks associated with medical devices?**
 - 2.1. What measures are currently in place to protect medical devices from cyber threats?
 - 2.2. How do healthcare institutions train their staff to handle cybersecurity threats related to medical devices?
- 3. What are the main gaps and weaknesses in existing cybersecurity measures for medical devices?**
 - 3.1. How do current practices compare with established cybersecurity frameworks and standards?
 - 3.2. What challenges do healthcare providers face in implementing effective cybersecurity measures?
- 4. How do regulatory requirements impact the cybersecurity of medical devices in healthcare?**
 - 4.1. What are the key regulations and standards governing medical device cybersecurity?
 - 4.2. How do healthcare institutions ensure compliance with these regulations?
- 5. What strategies can be implemented to control and mitigate cybersecurity risks in medical devices effectively?**
 - 5.1. What best practices and frameworks can be adopted to enhance the cybersecurity of medical devices?

- 5.2. How can healthcare institutions and device manufacturers collaborate to improve medical device security?
- 6. **How do cybersecurity incidents involving medical devices affect patient safety and healthcare operations?**
 - 6.1. What are the potential consequences of cybersecurity breaches in medical devices on patient care?
 - 6.2. How do healthcare institutions respond to and recover from such incidents?
- 7. **What role do medical device manufacturers play in ensuring the cybersecurity of their products?**
 - 7.1. How can manufacturers integrate robust security features into the design and development of medical devices?
 - 7.2. What responsibilities do manufacturers have in updating and maintaining the security of their devices post-market?
- 8. **What are the perceptions and attitudes of healthcare professionals towards cybersecurity risks in medical devices?**
 - 8.1. How aware are healthcare professionals of the cybersecurity risks associated with medical devices?
 - 8.2. What is the level of training and education provided to healthcare professionals on medical device cybersecurity?
- 9. **What are the cost implications of implementing comprehensive cybersecurity measures for medical devices?**
 - 9.1. How do the costs of cybersecurity measures compare to the potential costs of cybersecurity incidents?
 - 9.2. What financial support and incentives are available for healthcare institutions to invest in cybersecurity?
- 10. **How can ongoing research and development contribute to improving the cybersecurity of medical devices?**
 - 10.1. What are the emerging technologies and innovations in the field of medical device cybersecurity?

10.2. How can academic and industry partnerships foster advancements in medical device security?

These questions aim to provide a comprehensive understanding of the cybersecurity challenges and solutions related to medical devices in healthcare, helping to guide the study towards actionable insights and practical recommendations.

Study hypotheses:

1. Medical devices in healthcare exhibit vulnerabilities primarily due to outdated software and inadequate encryption measures.
2. Current cybersecurity practices in healthcare settings are insufficient to effectively mitigate the risks associated with medical devices.
3. There exists a significant gap between regulatory requirements and the actual implementation of cybersecurity measures in medical device management.
4. Healthcare professionals' awareness and training regarding cybersecurity risks directly correlate with the effectiveness of cybersecurity measures in medical device usage.
5. Implementing a comprehensive cybersecurity framework, integrating security-by-design principles, will significantly enhance the protection of medical devices against cyber threats.
6. The cost implications of implementing robust cybersecurity measures are justified by the potential cost savings from preventing cybersecurity incidents in medical devices

Previous Studies:

1. Medical Device Security: An Industry Under Attack and Unprepared to Defend

Ponemon Institute. (2019). *Medical device security: An industry under attack and unprepared to defend*. Retrieved from <https://www.ponemon.org/research/ponemon-library/security/medical-device-security.html>

2. Cybersecurity for Medical Devices: Mitigating the Risks

Deloitte. (2018). *Cybersecurity for medical devices: Mitigating the risks*. Retrieved from <https://www2.deloitte.com/us/en/insights/industry/life-sciences/medical-device-cybersecurity.html>

3. Healthcare Cybersecurity: Threats and Solutions

Ragan, S., & McKeown, K. (2020). *Healthcare cybersecurity: Threats and solutions*. Springer. ISBN: 978-3-030-36142-4.

4. The State of Medical Device Cybersecurity

Smith, T. R. (2019). The state of medical device cybersecurity. *Journal of Healthcare Protection Management*, 35(1), 12-19.

5. Medical Device Cybersecurity: A Guide for HTM Professionals

Association for the Advancement of Medical Instrumentation (AAMI). (2020). *Medical device*

cybersecurity: A guide for HTM professionals. Retrieved from <https://www.aami.org/healthcare-technology/medical-device-cybersecurity-guide>

6. Healthcare Under Cyber Siege: Addressing the Threats

Nakashima, E. (2020, September 24). Healthcare under cyber siege: Addressing the threats. *The Washington Post*. Retrieved from <https://www.washingtonpost.com/technology/2020/09/24/healthcare-cybersecurity/>

7. Securing IoT Devices: Building Security into the Internet of Things

Mansfield-Devine, S. (2016). Securing IoT devices: Building security into the Internet of Things. *Computer Fraud & Security*, 2016(8), 11-14.

8. Good Practices for Cybersecurity in the Healthcare Sector

European Union Agency for Cybersecurity (ENISA). (2022). *Good practices for cybersecurity in the healthcare sector*. Retrieved from <https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services>

9. Cybersecurity in Medical Devices: Addressing the Challenges

Institute of Electrical and Electronics Engineers (IEEE). (2020). *Cybersecurity in medical devices: Addressing the*

challenges. *IEEE Transactions on Medical Devices*, 67(3), 205-215.

10. Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients

Healthcare Sector Coordinating Council (HSCC). (2019). *Health industry cybersecurity practices (HICP): Managing threats and protecting patients*. Retrieved from <https://healthsectorcouncil.org/the-hicp/>

The theoretical principles of the study:

1. Cybersecurity Frameworks and Standards

Provide structured methodologies for evaluating and improving cybersecurity measures, ensuring alignment with industry best practices and regulatory requirements.

2. Security-by-Design Principle

Emphasizes proactive integration of security measures during the design phase of medical devices, aiming to prevent vulnerabilities rather than reacting to them post-implementation.

3. Risk Management Theory

Guides the identification, assessment, and mitigation of cybersecurity risks, fostering a systematic approach to risk reduction and management.

4. Regulatory Compliance and Governance

Ensures that cybersecurity practices align with legal requirements and industry regulations, promoting accountability and adherence to established standards.

5. Human Factors and Organizational Behavior

Acknowledges the influence of human behaviors and organizational culture on cybersecurity practices, emphasizing training, awareness, and user-centric design.

Methodology and research methods:

The methodology of this study will employ a mixed-methods approach, combining qualitative and quantitative methods to comprehensively explore and analyze cybersecurity risks associated with medical devices in healthcare settings. This approach allows for a nuanced understanding of both the subjective experiences and objective realities of cybersecurity challenges. The complete details Will be mention later when start the collecting the data and start the analysis of cybersecurity challenges and solutions in the context of medical devices within healthcare. Plan to select two to three healthcare facilities, inside KSA and outside KSA later will be mention after starting the study.

Study tools:

1. Statistical Analysis Software
2. Case Study Analysis Tools
3. Project Management and Collaboration Tools

The limits of the study:

1. Sample Size and Generalizability:

The study's will limit the stakeholder to be healthcare professionals, IT specialists, and Biomedical Engineer/Technicians for the to be surveyed or interviewed, to findings the specific sample demographics.

2. Access to Data and Information:

Access to patient data or sensitive information related to cybersecurity incidents in medical devices may be restricted within some healthcare settings. Therefore, publicly available data will be used, sensitive information will be anonymized, and ethical guidelines will be adhered to in data collection and analysis.

3. Time Constraints:

Conducting a thorough study within a limited timeframe 3 months (during the term duration) may restrict the depth and breadth of data collection and analysis, but will going to Prioritize key research objectives, use efficient data collection methods, and focus on obtaining actionable insights within the given timeframe.

4. Scope of Research Questions:

The study's scope may not encompass all aspects of medical device cybersecurity, such as specific technical vulnerabilities or emerging threats. Therefore, clearly will define the research questions and objectives, focusing on areas where the study can provide meaningful contributions and insights.

5. Research Design Limitations:

Methodological constraints, such as limitations in survey design, interview techniques, or case study selection, may impact the comprehensiveness of the study, therefore will Validate research methods against establishing frameworks standards, and acknowledge any methodological limitations, and take the findings from multiple sources.

6. External Factors and Contextual Constraints:

such as changes in regulatory requirements or developments in cybersecurity technology, may affect the relevance and applicability of the study over time, so we will keep this in mind and any circumstances that arise will be mentioned and acknowledged to explain any change in results.

Conclusion

In conclusion, this study underscores the critical importance of addressing cybersecurity risks associated with medical devices in healthcare through comprehensive measures encompassing technological innovation, regulatory compliance, and stakeholder collaboration. By implementing the recommended strategies and continuing to advance research and practices in this field, healthcare organizations can safeguard patient safety, protect sensitive data, and maintain operational integrity in an increasingly interconnected digital landscape.

Resources and reference:

1. **FDA (U.S. Food and Drug Administration).** (2021). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. Retrieved from FDA Website
2. **HIPAA Journal.** (2022). *The Importance of Cybersecurity in Medical Devices*. Retrieved from HIPAA Journal
3. **Deloitte.** (2018). *Cybersecurity for Medical Devices: Mitigating the Risks*. Retrieved from Deloitte Insights
4. **Ragan, S., & McKeown, K.** (2020). *Healthcare Cybersecurity: Threats and Solutions*. Springer Publishing. ISBN: 978-3-030-36142-4.
5. **Ponemon Institute.** (2019). *Medical Device Security: An Industry Under Attack and Unprepared to Defend*. Retrieved from Ponemon Institute
6. **Morgan, S.** (2020). *Healthcare Cybersecurity Report*. Cybersecurity Ventures. Retrieved from Cybersecurity Ventures
7. **Baker, M. A., & Jackson, P. J.** (2017). *Cybersecurity and Medical Devices: An Imperative for Safety*. *Biomedical Instrumentation & Technology*, 51(2), 143-150.
8. **Mansfield-Devine, S.** (2016). *Securing IoT Devices: Building Security into the Internet of Things*. *Computer Fraud & Security*, 2016(8), 11-14.
9. **Cybersecurity & Infrastructure Security Agency (CISA).** (2021). *Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide*. Retrieved from CISA Website
10. **McKinsey & Company.** (2019). *Cybersecurity in Medical Devices: Considerations for Stakeholders*. Retrieved from McKinsey Insights
11. **Institute of Electrical and Electronics Engineers (IEEE).** (2020). *Cybersecurity in Medical Devices: Addressing the Challenges*. *IEEE Transactions on Medical Devices*, 67(3), 205-215.

12. **ENISA (European Union Agency for Cybersecurity).** (2022). *Good Practices for Cybersecurity in the Healthcare Sector*. Retrieved from [ENISA Website](#)
13. **World Health Organization (WHO).** (2020). *Global Strategy on Digital Health 2020-2025*. Retrieved from [WHO Website](#)
14. **NIST (National Institute of Standards and Technology).** (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from [NIST Website](#)
15. **Healthcare Information and Management Systems Society (HIMSS).** (2020). *2020 HIMSS Cybersecurity Survey*. Retrieved from HIMSS Website
16. **Nakashima, E.** (2020). *Healthcare Under Cyber Siege: Addressing the Threats*. The Washington Post. Retrieved from The Washington Post
17. **Smith, T. R.** (2019). *The State of Medical Device Cybersecurity*. Journal of Healthcare Protection Management, 35(1), 12-19.
18. **Healthcare Sector Coordinating Council (HSCC).** (2019). *Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients*. Retrieved from HSCC
19. **AAMI (Association for the Advancement of Medical Instrumentation).** (2020). *Medical Device Cybersecurity: A Guide for HTM Professionals*. Retrieved from AAMI
20. **European Commission.** (2021). *Medical Device Regulation (MDR) and In Vitro Diagnostic Regulation (IVDR)*. Retrieved from [European Commission](#)

المقدمة:

يصبح الأمن السيبراني جزءًا حيويًا من الرعاية الصحية بسبب الاعتماد المتزايد على الشبكات واسعة النطاق والمعقدة المرتبطة بالسجلات الطبية الإلكترونية وأنظمة الرعاية الصحية التي تحتوي على بيانات المرضى القابلة للنقل. تمتلك مرافق الرعاية الصحية أجهزة سريرية واسعة النطاق وشاملة. تتكون هذه الأنظمة من منافذ ضعيفة متنوعة، مما يحدد معًا الضعف الأساسي للبنية التحتية للرعاية الصحية ككل. تعتبر الأجهزة الطبية ومعلومات المرضى وعناصر أخرى أهدافًا قيمة لهجمات الفدية والاضطرابات السيبرانية الفيزيائية الضارة الأخرى. يعد حماية الأجهزة أمرًا حيويًا لضمان استمرار الخدمات الصحية الأساسية التي تقدمها في العمل بشكل صحيح وأمن لحماية أو تعزيز سلامة المرضى.

أهمية الأمن السيبراني في الأجهزة الطبية وإدارة المخاطر الشاملة، والتوافق والإشراف ضروري للتحكم في مخاطر الأمن السيبراني في الأجهزة الطبية لضمان عمل الرعاية الطبية العامة والعلاجية في مرافق تقديم الرعاية الصحية دون انقطاع أو تعطيل. يعد التحكم في المخاطر السيبرانية للأجهزة أيضًا ضروريًا لتأمين البيانات الشخصية الحساسة التي تمر عبر الجهاز أو تُخزن عليه لضمان عدم تعرضها للأشخاص غير المصرح لهم بالوصول إليها. الهدف من خطة إدارة المخاطر للأجهزة الطبية هو التعرف على مستويات المخاطر وتقييمها ومراجعتها وإدارتها في كل مجموعة استخدام بحيث تتماشى مع أهداف تكنولوجيا الرعاية الصحية للمستهلك والأهداف طويلة الأجل. يمكن أن يسمح الأمن السيبراني في الأجهزة الطبية بالوصول غير المصرح به إلى بيانات هوية المرضى المحمية والبيانات الشخصية السرية، ويؤثر على تشخيص المرضى وإجراءاتهم أو الإمدادات الصحية الحساسة، مما يعرض المريض لمخاطر غير مقبولة من الأذى إذا تسببت البيانات الخاطئة في خطأ في الجهاز.

التحكم بمخاطر الأمن السيبراني للأجهزة الطبية في الرعاية الصحية

إعداد الطالب/ ناهد الطيب حسب القوي يوسف

221001105

المشرف الثاني د. فائز قراد

المشرف الرئيسي د. الفيصل عبد الحميد

العام الدراسي:

2024