



GRIFFITH COLLEGE DUBLIN

Evaluating the roles of interoperability and
cybersecurity in remote patient monitoring medical
devices of chronic disease management

A dissertation submitted in partial fulfilment of the requirements of
the
MASTERS in MEDICAL DEVICE TECHNOLOGY & BUSINESS
2025

Presented in May 2025 by:

Chaitanya Potharaju

Supervisor: Brian Kearney

Candidate Declaration

Candidate Name: Chaitanya Potharaju

I certify that the dissertation entitled 'Evaluating the roles of interoperability and cybersecurity in remote patient monitoring medical devices of chronic disease management' submitted in partial fulfilment of the requirements for the Master's in Medical Device Technology & Business is the result of my own work and that where reference is made to work of others, due acknowledgement is given.

Candidate Signature:

A handwritten signature in black ink, appearing to read 'P. Chaitanya', written in a cursive style.

Date: 19 May 2025

Supervisor Name: Brian Kearney

Supervisor Signature:

Date:

Acknowledgements

I would like to sincerely thank my thesis supervisor, Brian Kearney, for his invaluable guidance and support. His expertise and advice have been extremely helpful in carrying out this research.

I would like to thank the participants for their time to participate in interviews and share their experiences and insights, which contributed greatly accomplishing the research.

Personally, I would like to thank my wife, my daughter, friends and family members for their support during my journey to complete work.

Table of Contents

List of Tables	1
List of Figures	2
List of Abbreviations	3
Abstract.....	5
Chapter 1. Introduction.....	6
1.1 Research introduction and significance	6
1.2 Purpose of the research	7
1.3 Research Objectives	8
1.4 Research Questions.....	8
1.5 Scope and limitations of the research.....	9
1.6 Structure of the Dissertation	9
Chapter 2. Literature Review.....	12
2.1 Introduction	12
2.2 Medical Device.....	12
2.3 Classification of Medical Devices	13
2.4 Software Intense Medical Devices	14
2.5 Remote Patient Monitoring Medical Devices	15
2.6 RPMDs Interoperability and Cybersecurity – Standards.....	17
2.7 Remote Patient Monitoring Medical Devices – Interoperability	18
2.8 Remote Patient Monitoring Medical Devices – Cybersecurity.....	21
2.9 RPMDs Interoperability and Cybersecurity – Current Frameworks.....	23
2.10 RPMDs Interoperability and Cybersecurity – Potential Improvements	24
Chapter 3. Research Methodology.....	27
3.1 Introduction	27
3.2 Research design	27
3.3 Research strategy	28
3.3.1 Philosophical approach – Interpretivism	29
3.3.2 Inductive approach	29
3.3.3 Data Collection Methods.....	29
3.3.4 Cross sectional time period	30
3.3.5 Data collection.....	31
3.4 Data analysis – Thematic analysis	32
3.5 Ethical considerations	33
3.5.1 Ethics approval.....	33
3.5.2 Informed consent & confidentiality	34
3.5.3 Confidentiality and anonymity.....	34

3.5.4 Data storage and security.....	35
Chapter 4. Analysis and Findings.....	37
4.1 Introduction	37
4.2 Interview setting and Participant profile	37
4.3 Analysis and Findings	40
4.3.1 Preliminary Analysis: Key Words	40
4.3.2 Analysis – Cybersecurity Threats & Vulnerabilities	42
4.3.3 Analysis — Interoperability Challenges.....	43
4.3.4 Analysis — Regulations and Standards.....	44
4.3.5 Analysis — Patient Benefits and Outcomes.....	46
4.3.6 Analysis — Cybersecurity and Interoperability Current State.....	47
4.3.7 Analysis — Cybesecurity and Interoperability Considerations	49
4.3.8 Analysis — Additional Insights by Participants.....	51
4.3.9 Analysis — Common Considerations and Challenges	52
4.3.10 Analysis — Contradicting Considerations and Challenges.....	52
4.3.11 Findings: RPMDs Interoperability and Cybersecurity – Standards	53
4.3.12 Findings: Interoperability — Enablers, Drivers and Barriers	53
4.3.13 Findings: Cybersecurity — Enablers, Drivers and Barriers	56
4.3.14 RPMDs Interoperability and Cybersecurity – Current Frameworks	59
4.3.15 RPMDs Interoperability and Cybersecurity – Potential Improvements	59
Chapter 5. Discussion and recommendations	61
5.1 Research aim and objectives	61
5.2 Overview of key findings	61
5.3 Comparisons with existing literature	62
5.3.1 Alignment with existing studies.....	62
5.3.2 New insights gained from this research	63
5.4 Recommendations to improve interoperability and cybersecurity in RPMDs	63
5.5 Limitations of the study	64
5.5.1 Methodological limitations.....	64
5.5.2 Impact of limitations on findings.....	65
5.5.3 Suggestions for future research.....	65
5.6 Conclusion	66
Chapter 6. References	68
Appendix A: Interview Questions.....	71
Appendix B: Participant Information Letter	73
Appendix C: Informed Consent Form	76
Appendix D: Ethics Application	78

List of Tables

Table 1: Participant interview topics	32
Table 2: Participant coding by role	35
Table 3: Participants associated with medical device life cycle phases	40

List of Figures

Figure 1: Typical Digital Healthcare Ecosystem, created by author	15
Figure 2: Basic Architecture of a RPM system, created by author (Khater et al., 2024).....	16
Figure 3: The 'research onion' (Saunders et al., 2023).....	27
Figure 4: Saunders research onion (Saunders et al., 2023)	28
Figure 5: Keyword identified from the interview transcript	41
Figure 6: Cybersecurity Threats & Vulnerabilities — Codes, patterns and themes	42
Figure 7: Interoperability Challenges — Codes, patterns and themes	43
Figure 8: Regulations and Standards — Codes, patterns and themes	45
Figure 9: Patient Benefits and Outcomes — Codes, patterns and themes	46
Figure 10: Cybersecurity and Interoperability Current State — Codes, patterns and themes	48
Figure 11: Cybersecurity and Interoperability Considerations — Codes, patterns and themes	50

List of Abbreviations

APIs – Application Programming Interfaces

CISA – Cybersecurity and Infrastructure Security Agency

CMD – Connected Medical Device

DHS – Digital Healthcare System

EHR – Electronic Health Record

EHRs – Electronic Health Records

EU – European Union

EU MDR – European union medical device regulation 2017/745

FDA – Federal Drug Authorities

FHIR – Fast Healthcare Interoperability Resources

GDPR – General Data Protection Regulation

HCP – Healthcare Professional

HIPAA – Health Insurance Portability and Accountability Act

HL – Health Level

HRMS - Health Remote Monitoring Systems

IEC – International Electrotechnical Commission

IEEE – Institute of Electrical and Electronics Engineers

IMDRF – International Medical Device Regulators Forum

IoT – Internet of Things

ISO – International Standards Organisation

MDSW – Medical Device Software

MDSW – Medical Device Software

MHLW – Ministry of Health, Labour and Welfare

MMA – Mobile Medical Apps

NIST – National Institute of Standards and Technology

PIL – Participant Information Letter

PMA – Premarket Approval

PMDA – Pharmaceuticals and Medical Device Agency

RPM – Remote Patient Monitoring

RPMDs – Remote Patient Monitoring Medical Devices

SaMD – Software as a Medical Device

SiMD – Software in a Medical Device

US – United States

Abstract

Evaluating the roles of interoperability and cybersecurity in remote patient monitoring medical devices of chronic disease management

Objective:

The modern-age digital healthcare system empowers the healthcare professionals and patients to effectively monitor and manage chronic disease conditions remotely and offers significant benefits such as improved patient outcomes, clinical decision support, and reduced HCP's workload. The digital healthcare system includes connected medical devices, organisation infrastructure, hospital networks, mobile apps, and multiple stakeholders such as device manufacturers, HCPs and patients. The key elements of a digital healthcare system include interoperability and cybersecurity. The interoperability ensures integration of medical devices, electronic health records (EHRs) and other systems for seamless data exchange. Whereas the cybersecurity ensures systems are resilient to minimise the threats and vulnerabilities for patient data security and privacy. The objective of this research is to evaluate the roles of interoperability and cybersecurity through the assessment of enablers, drivers, and barriers, respectively, in remote patient monitoring medical devices of chronic disease management by exploring the knowledge of different stakeholders involved in the development and application of similar systems.

Methods:

A qualitative exploration of information gathered through interviewing experienced stakeholders such as healthcare professionals, research and development engineers, regulatory affairs specialists, medical affairs professionals, marketing professionals and cybersecurity professionals involved in the development, and application of remote patient monitoring medical devices of chronic disease management. The interviews were focused on gathering experience and insights on interoperability and cybersecurity.

Results:

Consensus across participants on benefits such as improved patient outcomes and clinical decision support. The current state of interoperability framework and features facilitate data exchange leveraging existing standards. However, significant efforts were required to develop standardised communication protocols and open architecture for integration of entire digital healthcare system. The current state of cybersecurity framework and regulations such as GDPR and HIPAA ensure data protection. However, more efforts are required to improve the system resilience and data security, by following approaches such as "security by design", role-based access and enhanced authentications.

Conclusion:

The insights shared by the participants resemble with the literature review findings. The RPMDs offer significant benefits if implemented effectively to improve patient outcomes and support clinical decisions. The development and implementation of efficient RPMDs require standardised communication protocols, scalable framework, open architectures and specific standards to integrate devices in a network securely and exchange data seamlessly for effective interoperability, and with enhanced cybersecurity measures to protect patient data.

Chapter 1. Introduction

1.1 Research introduction and significance

The objective of this research is to gain deeper insights on interoperability and cybersecurity from the healthcare professionals and different stakeholders involved in the development, usage and maintenance of digital healthcare system facilitating in remote monitoring and managing patients with chronic disease conditions. The study focuses on assessing the drivers, enablers, and barriers related to interoperability and cybersecurity in remote patient monitoring medical devices of chronic disease management.

Connected Medical Device (CMD): A connected medical device is that interfaces with the internet or network facilitating in transmitting and receiving data (Machal, 2023). These devices facilitate in uploading data to a patient's record that can be accessed by the HCPs and can be utilised in monitoring chronic disease condition (Leo *et al.*, 2022) and assists in making effective clinical decisions to improve patient outcomes.

Remote Patient Monitoring (RPM): The remote patient monitoring utilises connected medical devices including sensors and wearables to gather biometric and physiological data (Peyroteo *et al.*, 2021). One of the key applications of RPM is to monitor patients with chronic health conditions and managing the data (Leo *et al.*, 2022). RPM's ability to detect chronic disease deterioration assists in early intervention of HCPs to prevent escalation to acute care (De Guzman *et al.*, 2022). Also, RPM can assure a sense of safety to patients living alone (Walker *et al.*, 2019).

Digital Healthcare System (DHS):

A digital healthcare system is the integration of connected medical devices, remote patient monitoring services, and key stakeholders involved in healthcare to improve efficacy and patient outcomes (U.S. Food & Drug Administration (FDA) [Online], 2020; Peyroteo *et al.*, 2021; Baltaxe *et al.*, 2023; Ramirez, 2024). Digital healthcare systems assist in monitoring, diagnosis, and treatment by using patient data gathered from different systems operating within the network (Lehne *et al.*, 2019; Peyroteo *et al.*, 2021; Ramirez, 2024). One of the DHS's primary objectives is to empower healthcare professionals to provide effective, patient-centred care through resource allocation optimization and support for healthcare practice advancements (Fernandez and Pallis, 2014; Ramirez, 2024).

The integration of different components of a digital healthcare system facilitates improved patient outcomes and efficacy. However, the key elements of an effective integrated digital

healthcare system depend on the efficiency of interoperability features and robust data security measures.

Interoperability is a critical element of the digital healthcare system, it is the ability of different systems to work together, and it enables data exchange across different DHS components such as connected medical devices, electronic health records, and HCPs for effective remote patient monitoring and improved patient outcomes through early interventions (Lehne *et al.*, 2019).

Cybersecurity is critical in digital healthcare system, facilitating remote patient monitoring to protect patient data and system integrity (Machal, 2023). Robust cybersecurity measures, including data encryption and access controls, are essential to prevent unauthorized access, data breaches, and cyberattacks (Machal, 2023; Khater *et al.*, 2024). Prioritizing cybersecurity is essential for patients and healthcare experts to use these devices safely and effectively (Machal, 2023).

Remote Patient Monitoring Medical Devices are incorporated with advanced technological features that facilitate remote patient data collection, continuous monitoring, early interventions, and improved management of chronic conditions. However, they present challenges such as user acceptance, minimal personal interaction with healthcare professionals, the requirement for devices or systems to work together (interoperability) and securing the devices and data from cyber threats (cybersecurity).

1.2 Purpose of the research

This research aims to explore the critical considerations of interoperability and cybersecurity incorporated in digital healthcare systems facilitating remote patient monitoring for chronic disease management. The primary objective is to gather in-depth insights from healthcare professionals and various stakeholders involved in the development, utilisation, and maintenance of digital healthcare systems. Further steps include analyses and assessment of the drivers, enablers, and barriers relevant to interoperability and cybersecurity meeting patients and users expectations including patient safety, self-management, improved healthcare services access and efficient data exchange (Walker *et al.*, 2019; Lehne *et al.*, 2019; U.S. Food & Drug Administration (FDA) [Online], 2020; Margam, 2023; Machal, 2023; Center for Devices and Radiological FDA [Online], 2024). The key emphasis is to understand the effective interoperability considerations to achieve successful data exchange across the devices within the digital healthcare system. Similarly, to understand cybersecurity measures for protecting patient data and integrity.

The research summarises the factors influencing interoperability and cybersecurity on digital healthcare systems for chronic disease management. Furthermore, this study will identify potential considerations that could improve integration and data security of the different digital healthcare components, fostering healthcare practices, patient care and outcomes in chronic disease management.

The market for remote patient monitoring devices is increasing because of several factors including the ability to customize the healthcare services based on patient needs that can be performed remotely. Remote monitoring also facilitates healthcare professionals for early intervention and supports clinical decisions as required. Also, it empowers patients to monitor and manage their own health (Walker *et al.*, 2019; Amaral *et al.*, 2024; Ramirez, 2024).

However, the potential challenges in using RPMDs include patient's ability to learning and adopting new technology, minimal personal interaction with healthcare professionals. The other important aspects are uninterrupted communication, data integrity and security (Walker *et al.*, 2019; Jaatun *et al.*, 2024).

1.3 Research Objectives

Objective #1: Identify the current standards available for interoperability and cybersecurity in remote patient monitoring medical devices.

Objective #2: Assess drivers, enablers, and barriers relevant to interoperability in remote patient monitoring medical devices.

Objective #3: Assess drivers, enablers, and barriers relevant to cybersecurity in remote patient monitoring medical devices.

Objective #4: Assess the current state of interoperability and cybersecurity frameworks in remote patient monitoring medical devices.

Objective #5: Identify the potential considerations that could improve integration and data security of the different digital healthcare components.

1.4 Research Questions

Question #1: What are the roles of interoperability and cybersecurity in remote patient monitoring for chronic disease management?

Question #2: What are the factors influencing the interoperability of remote patient monitoring for chronic disease management, or do they require improvement?

Question #3: What are the factors influencing the cybersecurity of remote patient monitoring for chronic disease management, or do they require improvement?

1.5 Scope and limitations of the research

Scope: The scope of this research is a comprehensive evaluation of cybersecurity and interoperability in remote patient monitoring medical devices used for the monitoring and management of patients with chronic disease conditions. The study aims to gather insights from healthcare professionals and stakeholders with knowledge in the development, application, and maintenance of digital healthcare systems. The study assesses the drivers, enablers, and barriers associated with interoperability and cybersecurity that influence patient outcomes and efficacy.

Limitations: The study limitations include a limited cohort gaining insights and perspectives through interviews and do not include other aspects such as user experiences or technical evaluations. A lack of global coverage to assess the interoperability and cybersecurity standards and frameworks due to the time constraints with the course. Also, detailed data analysis is not within the scope due to different constraints associated with cybersecurity and interoperability, and the use of different assessment criteria in various studies.

1.6 Structure of the Dissertation

The dissertation will be organised into five chapters.

Chapter #1 – Provides an overview of the research study. This includes the purpose of the research and study background, research objectives and research questions. Furthermore, it describes the scope and limitations of the study, significance of the study and overall structure of the Dissertation.

Chapter #2 – Literature review which introduces connected medical devices, interoperability, cybersecurity, factors influencing interoperability and cybersecurity, and critically analyses research that has been done to date on the topic.

Chapter #3 – The research methodology approach taken in this research

Chapter #4 – Data presentation and analysis of interview responses

Chapter #5 – Discussion and recommendations.

Appendix: Interview questions, Participant information letter (PIL), Informed Consent form and Ethics application form.

In the literature review research articles and journal research were undertaken to determine the information available on the considerations and challenges related to interoperability and cybersecurity in remote patient monitoring medical devices in chronic disease management. Searches were conducted using Sage, Google Scholar, PubMed and Science Direct. The search words used were Digital healthcare technologies: medical device, classification, connected medical device; connected medical devices - interoperability; connected medical devices - cybersecurity; risk management; integration; standards; regulations; challenges and opportunities; and chronic diseases - remote monitoring.

Chapter 2. Literature Review

2.1 Introduction

Remote patient monitoring with the use of medical devices was developed as an advanced method in healthcare, especially for the management of chronic diseases. Considering the increasing use of technological advances in digital healthcare systems, the importance of interoperability and cybersecurity has become essential to providing effective and safe patient care. The purpose of this literature review is to evaluate the importance of interoperability and cybersecurity in remote patient monitoring medical devices used for chronic disease management. The key considerations in assessing the interoperability include data exchange ability, electronic health records, and integration of different healthcare platforms, facilitating patient-focused care and informed decision-making. The key considerations in assessing the cybersecurity include current security measures to protect patient data from unauthorised access and vulnerabilities. The integrated healthcare solution could improve patient outcomes, reduce hospital admissions, and enhance the overall quality of care, but it could present challenges such as data security, standardisation, and patient engagement. However, when properly implemented, RPM can significantly improve patient outcomes, reduce hospital admissions, and enhance the overall quality of care. This review will explore recent research findings in interoperability and cybersecurity within the context of RPM, focusing on their impact on chronic disease management and the broader healthcare ecosystem.

2.2 Medical Device

A medical device is any instrument, apparatus, machine, or software intended for use in the diagnosis, prevention, monitoring, treatment, or alleviation of disease or other medical conditions (Tetty-Engmann. Ph.D. and Parupelli, 2023; Amaral *et al.*, 2024).

The World Health Organisation (WHO) defines a medical device as "any 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" (Tetty-Engmann. Ph.D. and Parupelli, 2023; Amaral *et al.*, 2024).

2.3 Classification of Medical Devices

The classification of medical devices is a process that considers the intended use and the associated risks during use to categorize a product (Tetty-Engmann. Ph.D. and Parupelli, 2023; Amaral *et al.*, 2024). The purpose of classification is to make sure that medical devices launched on the market are clearly identified and meet the necessary quality and safety standards specific to geographical locations (Amaral *et al.*, 2024). The classification of medical devices depends on the target country, and the regulatory control requirements for market authorization and post-market surveillance depend on the class of medical devices (Amaral *et al.*, 2024).

United States (US): The FDA classifies medical devices into three classes:

- Class I: A medical device with “low risk” subjected to general controls (Tetty-Engmann. Ph.D. and Parupelli, 2023; U.S. Food & Drug Administration (FDA) [Online], 2023a; Amaral *et al.*, 2024).
- Class II: A medical device with “moderate risk” requiring special controls and Premarket Notification 510(k) (Tetty-Engmann. Ph.D. and Parupelli, 2023; U.S. Food & Drug Administration (FDA) [Online], 2023a; Amaral *et al.*, 2024).
- Class III: A medical device with “high risk” requiring Premarket Approval (PMA) (Tetty-Engmann. Ph.D. and Parupelli, 2023; U.S. Food & Drug Administration (FDA) [Online], 2023a; Amaral *et al.*, 2024).

European Union (EU):

- Class I: A medical device with “low risk” includes non-invasive devices (EUR-Lex [Online], 2017; Tetty-Engmann. Ph.D. and Parupelli, 2023; Amaral *et al.*, 2024).
- Class IIa: A medical device with “low to medium risk” intended to use within the body for a short term (EUR-Lex [Online], 2017; Tetty-Engmann. Ph.D. and Parupelli, 2023; Amaral *et al.*, 2024).
- Class IIb: A medical device with “medium to high risk” intended to use within the body for a long term (EUR-Lex [Online], 2017; Tetty-Engmann. Ph.D. and Parupelli, 2023; Amaral *et al.*, 2024).
- Class III: A medical device with “high risk” subjected to stringent approval process (EUR-Lex [Online], 2017; Tetty-Engmann. Ph.D. and Parupelli, 2023; Amaral *et al.*, 2024).

2.4 Software Intense Medical Devices

Software Intense Medical Devices: These types of medical device functions depend on software to achieve their intended use. The software can be developed to function as an independent application or embedded into device hardware (Pashkov *et al.*, 2016).

Medical Device Software (MDSW): It can be described as software developed by the manufacturer intended for medical applications like diagnosis, prevention, investigation, monitoring, prediction, treatment, alleviation, prognosis, and prediction (Baltaxe *et al.*, 2023).

The medical device software can be typically classified as:

- **Software as a Medical Device (SaMD):** A software developed by the manufacturer to function as an independent application to achieve its intended use by utilising commercially available devices such as computers, laptops, tablets and smartphones (Hassanally and Dufour, 2021; U.S. Food & Drug Administration (FDA) [Online], 2022; Tettey-Engmann. Ph.D. and Parupelli, 2023).
- **Software in a Medical Device (SiMD):** A software developed by the manufacturer that is embedded into the hardware to function as a medical device to achieve its intended use (Carroll and Richardson, 2016; Hassanally and Dufour, 2021; U.S. Food & Drug Administration (FDA) [Online], 2022; Tettey-Engmann. Ph.D. and Parupelli, 2023).

The medical device software is classified based on its intended use and patient risk level by the regulatory bodies such as the EU and the FDA.

The latest EU regulations classify SaMD as an active medical device and classes range from class I to class IIb (Jaatun *et al.*, 2024).

The FDA software classification is based on its intended use, whether the software is developed to diagnose or treat a disease or affect the structure or function of the human body. The FDA classifies software into class I, II or III depending on the risk level associated with its application (Tettey-Engmann. Ph.D. and Parupelli, 2023).

The increase in integrating software into medical devices presents potential challenges to users if not properly managed. Hence, the definition and classification of software are critical for ensuring patient safety and the efficacy of remote patient monitoring medical devices used for chronic disease management (Pashkov *et al.*, 2016). Interoperability and cybersecurity are key factors in SIMDs used in remote patient monitoring to achieve intended use and reduce potential risks (Jaatun *et al.*, 2024; Singh, 2024).

2.5 Remote Patient Monitoring Medical Devices

Remote Patient Monitoring Medical Devices (RPMDs) incorporate technology that facilitates monitoring of patient health remotely by gathering the data using sensors and minimising the need for patient visits and admissions to hospitals or clinics, Figure 1: Typical Digital Healthcare Ecosystem, created by author illustrates a typical layout of RPMD ecosystem. RPMDs play a vital role in managing patients with chronic disease conditions and monitoring patients recovering in home care settings. Wearable devices and Health Remote Monitoring Systems (HRMS) are common types of devices that can be utilised for remote patient monitoring (Walker *et al.*, 2019; Peyroteo *et al.*, 2021; De Guzman *et al.*, 2022; Canali *et al.*, 2022; Leo *et al.*, 2022; Feinstein *et al.*, 2024; Tagne *et al.*, 2025).



Figure 1: Typical Digital Healthcare Ecosystem, created by author

RPMDs could assist healthcare professionals in finding early warning signs of potential patient health issues, these finding can be beneficial for managing and improving the health

of patients with chronic disease conditions. RPMDs could provide information to patients to monitor their conditions and potential ways to manage them. RPMDs that have the ability to interact with patients are specifically developed for managing chronic disease conditions (Peyroteo *et al.*, 2021; Leo *et al.*, 2022).

RPMDs gather biometric data, such as heart rate and blood pressure, and physiological data, such as oxygen levels. These devices make use of cloud platforms or similar systems for storage of collected data, to facilitate healthcare professional in accessing the data from anywhere thus supporting personalised and home-based healthcare services (Peyroteo *et al.*, 2021; Khater *et al.*, 2024; Ramirez, 2024).

The Figure 2: Basic Architecture of a RPM system, created by author (Khater *et al.*, 2024) illustrates the fundamental operational flow of data in remote patient monitoring system. A patient with a chronic disease uses a medical device incorporated with sensing mechanism to collect patient data and connectivity feature to exchange data. The data can be further transmitted through a communication network to the healthcare provider or integrated with the patient's Electronic Health Record (EHR). Also, the collected data can be analysed to generate alerts or indications for healthcare providers.

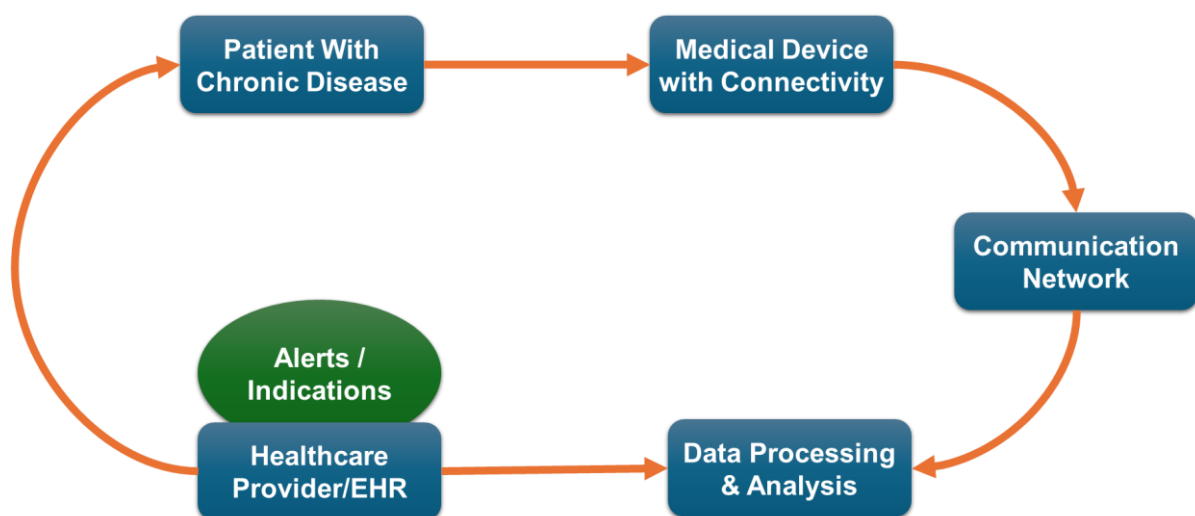


Figure 2: Basic Architecture of a RPM system, created by author (Khater *et al.*, 2024)

However, due to learning curve associated with adoption of new technology, users find potential challenges in the application of RPMDs, and in some instances the interaction with healthcare professionals is limited. Maintaining uninterrupted communication, data integrity and security are some of the other considerations (Walker *et al.*, 2019; Jaatun *et al.*, 2024).

2.6 RPMDs Interoperability and Cybersecurity – Standards

The remote patient monitoring medical devices used to manage chronic disease conditions require data collection and exchange with different systems in the network. These devices integrate with other devices to work together and to ensure data and devices are protected, and thus, the adoption of standards related to interoperability and cybersecurity is critical (Peyroteo *et al.*, 2021; Baltaxe *et al.*, 2023; Singh, 2024).

Interoperability – Standards:

The Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) standard is widely used to exchange patient data (Wang *et al.*, 2018; Lehne *et al.*, 2019; Singh, 2024). The aim of this standard is to allow different systems in the network to share patient health records such as Electronic Health Records (EHRs) and Personal Health Records (PHRs) that contains sensitive information. A two-way data exchange, allowing communication between patients and healthcare professionals, facilitates effective data (Saripalle *et al.*, 2019; Singh, 2024). Other standards include, IEEE 11073, ISO 13606, ASTM CCR, and HL7 CDA & CCD that could be used for PHRs communication and data exchange (Wang *et al.*, 2018; Saripalle *et al.*, 2019; Singh, 2024).

The Digital Imaging and Communications in Medicine (DICOM) standard is used for the management of medical imaging data (Robkin, 2015; Singh, 2024). However, DICOM's in RPM is relative less significantly used when compared to HL7.

Medical data exists in different formats, and hence, specific standards are required for effective data management. However, the integration of devices for seamless data exchange is complex by nature, so different technical standards and protocols will be implemented during their development. On the other hand, the legacy systems use proprietary formats to integrate with other systems and facilitate communication and data exchange. The varied methods of integration and communication signify the need to develop standardised communication protocols and Application Programming Interfaces (APIs) to improve device integration and data exchange for effective interoperability (Saripalle *et al.*, 2019; Singh, 2024).

Cybersecurity – Standards:

Device security and data protection are paramount in the healthcare industry. RPM that are intended to be used in global markets are required to adopt and implement region specific regulations and requirements (Vaidya, 2024; Singh, 2024; Shah, 2025).

RPMDs intended to be used in the European Union countries must comply with the EU Regulation (EU) 2017/745-MDR that outlines The European Union, Medical Device Software (MDSW). The personal data protection for individuals is defined under the General Data Protection Regulation (GDPR) (Baltaxe *et al.*, 2023).

RPMDs intended to be used in the United States must comply with the Health Insurance Portability and Accountability Act (HIPAA) outlines set of rules for protecting patient information (Baltaxe *et al.*, 2023; Vaidya, 2024; Singh, 2024). The guidance on cybersecurity for medical devices, including requirements for premarket submissions for device manufacturers, is made available by the FDA (U.S. Food & Drug Administration (FDA) [Online], 2023b; Code of Federal Regulations [Online], 2025).

The guidelines outlined by both GDPR and HIPAA focuses on protecting sensitive data and require similar kind of security measures (Baltaxe *et al.*, 2023). The essential security objectives for RPMDs include integrity, authorisation, availability, confidentiality, and secure updates (U.S. Food & Drug Administration (FDA) [Online], 2023b).

Cybersecurity risk assessment is an essential element of security management, focusing on the strengths and weakness of the system to assess scenarios that could result in exploitation of the system. Standards such as ISO 14971 can be used for safety risk assessment, IEC 62304 medical device software, and ISO 27005 can be used for cybersecurity risk assessment. Other sources such as Guidance on Cybersecurity for medical devices (MDCG 2019-160), and Cybersecurity and Infrastructure Security Agency (CISA) could facilitate device manufacturers to incorporate and integrate security in the design, that is essential for reliable performance of RPMDs (Pashkov *et al.*, 2016; U.S. Food & Drug Administration (FDA) [Online], 2023b; Jaatun *et al.*, 2024; Shah, 2025).

Currently, there are a range of standards, regulations, and guidelines available to incorporate interoperability and cybersecurity in medical devices, including those used in RPM. However, to implement and advance these standards across different technologies and healthcare settings presents constant challenges (Jaatun *et al.*, 2024; Shah, 2025).

2.7 Remote Patient Monitoring Medical Devices – Interoperability

The interoperability of a medical device signifies its ability to communicate with and work with other medical devices. Data interoperability refers to the transfer, storage, access and utilisation of data produced by different devices or systems within the network (Jendle *et al.*, 2023).

Interoperability of Remote Patient Monitoring Medical Devices (RPMDs) for chronic disease management refers to the ability of various medical devices, software applications, and healthcare systems to connect flawlessly and exchange data, thus facilitating key stakeholders to understand the data for effective utilisation. Furthermore, interoperability is an essential feature for remote patient monitoring medical devices to integrate with electronic health records (EHRs) and other healthcare IT systems and exchange data seamlessly (Wang *et al.*, 2018; U.S. Food & Drug Administration (FDA) [Online], 2023b; Jendle *et al.*, 2023; Singh, 2024; K *et al.*, 2024).

The following are key enablers, drivers and barriers influencing successful implementation of interoperability.

Enablers of Interoperability:

- **Standardized data-sharing protocols:** These are key elements to integrate and interpret different data sources. Health Level (HL7) Fast Healthcare Interoperability Resources (FHIR) is one of the available standards for device manufacturers intending to incorporate Interoperability facilitates data exchange in healthcare (Saripalle *et al.*, 2019; Jendle *et al.*, 2023; Singh, 2024).
- **Open architecture practices:** Remote Patient Monitoring Medical Devices incorporated with common technologies such as Bluetooth and network protocols could integrate with healthcare systems effectively, facilitating interoperability and resulting in seamless data exchange (Wang *et al.*, 2018; U.S. Food & Drug Administration (FDA) [Online], 2023b).
- **Cloud-based platforms:** Remote Patient Monitoring Medical Devices with the capability to connect with cloud-based systems facilitate interoperability. The cloud-based system serves as a central repository for collecting, storing, and accessing data and facilitates managing user privileges and data integration with improved data integrity and security (Fernandez and Pallis, 2014; Peyroteo *et al.*, 2021; Singh, 2024; K *et al.*, 2024).
- **Unified healthcare infrastructure:** This is a key feature that facilitates interoperability for the devices to communicate and work together when connected in a network and enables accessing patient data (K *et al.*, 2024).
- **Collaboration among stakeholders:** This is a key aspect, including end-users, experts, designers, developers and regulatory bodies for developing a successful and interoperable healthcare ecosystem (Fernandez and Pallis, 2014; Hassanaly and Dufour, 2021; Singh, 2024).

Drivers of Interoperability:

- **Need for efficient healthcare systems and minimized costs:** Devices that facilitate interoperability offers advantages to the Healthcare organisations and healthcare professionals to improve efficacy and provide cost-effective services (Fernandez and Pallis, 2014; Wang *et al.*, 2018; Jaatun *et al.*, 2024; Singh, 2024).
- **Need for engaging patients in their own healthcare:** Interoperability empowers patients and healthcare professional to share and access data seamless with healthcare systems such as electronic health records (Fernandez and Pallis, 2014; Wang *et al.*, 2018; Saripalle *et al.*, 2019; Singh, 2024).
- **Need to improve patient outcomes and the quality of decision-making:** Interoperability enables sharing and exchanging data with healthcare systems, providing healthcare professionals with complete and precise patient data to improve patient outcomes and better-informed clinical decision-making (Wang *et al.*, 2018; Singh, 2024; K *et al.*, 2024).
- **Need for personalised and home-based healthcare:** The increasing needs of chronic diseases require frequent exchanging of data between devices and healthcare professionals that can be achieved by interoperability (Peyroteo *et al.*, 2021; Baltaxe *et al.*, 2023; Sobahi and Bamabad, 2024; Ramirez, 2024).
- **Need for a learning health system:** Interoperability is critical for health system's capability to continuously learn and improve using advanced technologies such as cloud computing, the Internet of Things (IoT) and artificial intelligence (AI) (Wang *et al.*, 2018; Peyroteo *et al.*, 2021; Singh, 2024; Ramirez, 2024).

Barriers to Interoperability:

- **Lack of standardisation:** The varied technical standards, protocols, and architectures across different systems and devices could impact data exchange, and make it difficult to implement interoperability (Jendle *et al.*, 2023; Singh, 2024).
- **Integrating with legacy systems:** Requiring significant resources and investment makes it difficult to integrate with existing legacy systems (Singh, 2024).
- **Security and privacy concerns:** Due to potential threats associated with data security and privacy, it is difficult to implement data sharing and interoperability (Vaidya, 2024; Singh, 2024).
- **Organisational challenges:** The varied interests, priorities, and workflows of stakeholders make it difficult to collaborate and implement interoperability (Fernandez and Pallis, 2014; Singh, 2024).

- **Regulatory requirements and laws:** The complexity of complying with global and local regulations makes it difficult to implement interoperability (Hassanally and Dufour, 2021; Jendle *et al.*, 2023; Singh, 2024).

2.8 Remote Patient Monitoring Medical Devices – Cybersecurity

Cybersecurity in remote patient monitoring medical devices is an essential element. These devices are vulnerable to cyberattacks as they are operated in a network and could result in serious issues with patient data (Jaatun *et al.*, 2024; Sobahi and Bamabad, 2024; Vaidya, 2024; Shah, 2025). A robust cybersecurity framework could ensure authorised access and proper use of patient data and device information, thus improving the data privacy and security. The advancing digital technologies can change the requirements for cybersecurity and controls such as user authentication and data encryption (U.S. Food & Drug Administration (FDA) [Online], 2023b; Siemens-healthineers [Online], 2024; Singh, 2024).

Remote patient monitoring medical devices with secured cybersecurity controls are critical for patient safety and build trust with healthcare professionals. Device manufacturers should consider incorporating security features into the devices from the early stages of development and plan to check for threats and assess risks regularly (U.S. Food & Drug Administration (FDA) [Online], 2023b; Jaatun *et al.*, 2024; Sobahi and Bamabad, 2024; Vaidya, 2024; Shah, 2025).

The following are key enablers, drivers and barriers influencing successful implementation of cybersecurity measures.

Enablers of cybersecurity:

- **Robust Device and User Authentication:** A secure and reliable authentication process ensures only authorized users have access to data and devices could minimise the threats and vulnerabilities and increase confidence to deliver secure services (U.S. Food & Drug Administration (FDA) [Online], 2023b; Singh, 2024).
- **Data Encryption:** A system that is capable of encrypting data for communication and storage improves the data security and privacy of users. Secured encryption of data ensures that data integrity and confidentiality are maintained (U.S. Food & Drug Administration (FDA) [Online], 2023b; Siemens-healthineers [Online], 2024; Vaidya, 2024; Singh, 2024).
- **Cybersecurity by Design:** Adopting a secure development framework that includes cybersecurity requirements from early in the development process and throughout the lifecycle will result in a secure system. Also, it minimizes the security threats and

vulnerabilities by identifying the mitigation controls early in the development process (U.S. Food & Drug Administration (FDA) [Online], 2023b; Jaatun *et al.*, 2024; Sobahi and Bamabad, 2024).

- **Security Risk Management Frameworks:** The impact of security incidents can be minimized with well-defined risk management procedures. An efficient risk management process to identify and mitigate the security is critical to build a resilient system to protect against the security threats and vulnerabilities (U.S. Food & Drug Administration (FDA) [Online], 2023b; Jaatun *et al.*, 2024; Vaidya, 2024).
- **Collaborative Security Strategy:** A security strategy developed by collaborating with all stakeholders involved in the development, manufacturing, and use could result in implementing device and system lifecycle considerations with adequate security controls (Fernandez and Pallis, 2014; Hassanaly and Dufour, 2021).

Drivers of cybersecurity:

- **Need for Remote Healthcare Support:** The increasing need to monitor and manage patients remotely requires resilient systems to provide secured services with confidence and minimize the threats and vulnerabilities. Cybersecurity is an essential element in realizing the benefits of remote patient monitoring medical devices developed for use in various healthcare settings (Khater *et al.*, 2024; Jaatun *et al.*, 2024; Vaidya, 2024; Singh, 2024; Shah, 2025).
- **Need for Secured Patient Data:** Data managed by medical devices often includes sensitive information such as patient health information, and personal identity information. Data confidentiality, integrity and availability are key aspects to comply with regulations and to sustain user's trust. These elements are critical to provide safe and uninterrupted healthcare services to patients (U.S. Food & Drug Administration (FDA) [Online], 2023b; Vaidya, 2024; Singh, 2024; Shah, 2025).
- **Need for Cyber Resilient Systems (medical devices):** Devices and systems that incorporate robust security controls could be resilient to cyberattacks and facilitate providing safe and uninterrupted healthcare services (U.S. Food & Drug Administration (FDA) [Online], 2023b; Vaidya, 2024; Shah, 2025).
- **Need for Specific Data Protection Regulations:** Compliance with healthcare regulations, such as HIPAA in the United States and GDPR in the EU, ensures necessary security controls are built into the devices to minimize the cyberattacks. Also, these regulations offer guidelines for device manufacturers, healthcare professionals and users on securing sensitive information (Baltaxe *et al.*, 2023; Vaidya, 2024; Singh, 2024).

- **Need for Efficient and Improved Outcomes:** The technological advancements in medical devices, including connectivity, data collection and analysis to support informed clinical decisions, require robust cybersecurity measures to improve efficacy and patient outcomes (Walker *et al.*, 2019; Peyroteo *et al.*, 2021; Machal, 2023; Ramirez, 2024).

Barriers of cybersecurity:

- **Cybersecurity Threats:** Lack of implementation of controls on devices and inadequate security controls for integration could make the system vulnerable to cyberattacks and compromise the data, impacting data privacy and safety (Machal, 2023; Vaidya, 2024; Singh, 2024; Shah, 2025).
- **Complex and Generic Guidelines:** Lack of standards specific to medical devices that can be used in a network makes it difficult for manufacturers and organisations to implement effective security controls and make the system vulnerable to cyberattacks. The existing guidelines are complete and inadequate to build for cyber-resilient systems (Jaatun *et al.*, 2024; Shah, 2025).
- **Cost and Expertise:** Developing, implementing and maintaining devices to include robust cybersecurity measures and effective monitoring mechanisms requires financial investment and skilled professionals (Jaatun *et al.*, 2024; Shah, 2025).
- **Integration Challenges:** Integration of a broad range of devices with different intended use and functionality presents challenges in implementing effective security measures and makes the system vulnerable to cyberattacks (Wang *et al.*, 2018; Jaatun *et al.*, 2024; Singh, 2024).
- **Usability and Technical Difficulties:** Lack of effective training and implementation of rigorous security controls could impact usability from achieving its intended use. Furthermore, it could present technical challenges to users and affect the efficiency of workflow and patient outcomes (Baltaxe *et al.*, 2023; Jaatun *et al.*, 2024; Sobahi and Bamabad, 2024; Vaidya, 2024).

2.9 RPMDs Interoperability and Cybersecurity – Current Frameworks

The regulatory frameworks are key for RPMDS to integrate within a network, exchange data, and minimise cyberattacks (Baltaxe *et al.*, 2023). They provide guidance to the device manufacturers on developing, implementing, and managing the devices and systems through the product lifecycle phases. The current frameworks are a mix of existing standards, guidelines, and ongoing development efforts.

Interoperability – Current Frameworks

The objective of interoperability in healthcare is to allow seamless data transfers between different devices, systems, personnel, and organisations (Wang *et al.*, 2018). In the context of RPM devices, the ability to gather data from the device and make it available to healthcare providers by means of patient records. The standards such as HL7 FHIR and DICOM facilitate the bi-directional exchange of data across systems, focusing on the data format (Wang *et al.*, 2018). However, the technical frameworks for data handling and system architecture to integrate medical devices to achieve interoperability facilitating communication are still evolving (K *et al.*, 2024).

Cybersecurity – Current Frameworks

The objective of interoperability in healthcare is to protect data and minimise vulnerabilities, focusing on system resilience (Jaatun *et al.*, 2024; Shah, 2025). The FDA provides guidance on security objectives, including authenticity, authorisation, availability, confidentiality, and timely updates (U.S. Food & Drug Administration (FDA) [Online], 2023b).

Currently, there are various types of guidance, standards, and regulatory requirements that address cybersecurity needs. HIPAA in the US and GDPR in the EU are examples of regulations. Examples of these standards include ISO 14971 for safety risk management and ISO 27001/27005 for cybersecurity risk management. Other resources include the MDCG 2019-160 Guidance on Cybersecurity for Medical Devices and the Cybersecurity and Infrastructure Security Agency (CISA) (U.S. Food & Drug Administration (FDA) [Online], 2023b; Jaatun *et al.*, 2024; Shah, 2025). The current state standards and guidance on cybersecurity for medical devices are sometimes complex, generic and incomplete (Jaatun *et al.*, 2024).

2.10 RPMDs Interoperability and Cybersecurity – Potential Improvements

The considerations for seamless data transfers through the integration of devices and systems, as well as secured devices and data, are critical for the RPMDs. The future enhancements should consider the following:

- Standardised approaches, such as protocols and APIs, should be implemented to integrate various devices and systems, thereby facilitating smooth data transfers (Singh, 2024).

- Improved data security measures, including robust encryption and authentication protocols to prevent unauthorised access and improve data security (Vaidya, 2024; Singh, 2024).
- Role-based or rule-based data access control is important to ensure only authorised individuals can access relevant information (Vaidya, 2024).
- Cybersecurity by design is a key consideration to build and implement adequate security measures in medical devices early in the development and throughout the life cycle that are intended to be used for RPM (Jaatun *et al.*, 2024; Shah, 2025).
- Identifying an appropriate pathway to implement security features with a focus on balancing security measures with patient benefits and ethical considerations is key (Jaatun *et al.*, 2024; Vaidya, 2024).

In summary, the literature review highlighted the purpose of the remote monitoring medical devices in the digital healthcare ecosystem with a focus on the key elements, such as interoperability to facilitate seamless data exchange across different systems and stakeholders involved in the healthcare system and cybersecurity to protect patient data and integrity. These elements are essential to support clinical decision-making and improve patient outcomes.

Furthermore, the applicable standards and regulations that could require compliance to develop effective interoperability features and robust cybersecurity controls required to design an efficient healthcare system were highlighted. The key enablers, drivers and barriers in relation to interoperability and cybersecurity in remote patient medical devices for monitoring and managing patients with chronic disease conditions were highlighted. The current state and potential considerations of interoperability and cybersecurity in remote patient medical devices were highlighted to foster and meet the increasing demands for the remote patient monitoring of chronic diseases in various healthcare and use settings.

Chapter 3. Research Methodology

3.1 Introduction

The research methodology was developed based on the research onion framework that was introduced by Saunders et al. (Saunders et al., 2023). The research onion illustrated in Figure 3: The 'research onion' (Saunders et al., 2023) includes different layers that provide guidance to choose necessary elements for research at various stages to converge the research objective and focus on the specific elements that are necessary for the study. In general, these layers of research starting from the outside describe research philosophy, research assumptions, research approaches, research strategy, time horizon and procedures and techniques to collect and analyze data. This framework signifies that all layers are connected to each other and provides a pathway for the researchers to make necessary decisions along with rationale. The research methodology using a research onion framework assists the researchers to effectively plan, execute, analyze and report the research (Saunders et al., 2023).

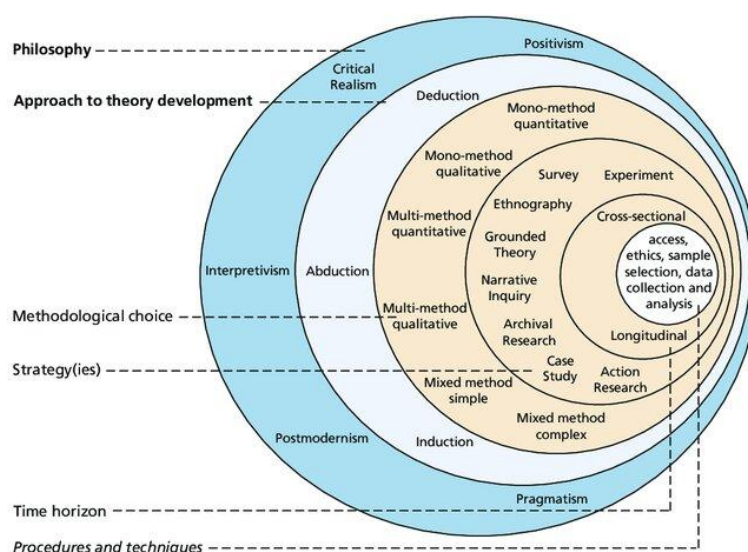


Figure 3: The 'research onion' (Saunders et al., 2023)

3.2 Research design

The research followed the approach of collecting qualitative data through one-to-one interview discussions that were recorded and transcribed by the researcher to fulfil the objectives of the study. The interviews aimed to gather knowledge and experience from experts and individuals with experience in the development, manufacturing, and application

of remote patient monitoring medical devices consisting of features such as interoperability and cybersecurity to monitor and manage patients with chronic disease conditions.

The interview format consists of open-ended questions relevant to medical devices, interoperability, and cybersecurity. The purpose of this interview format is to gain meaningful perspectives and insights on the topics to allow data collection for the next steps. Thematic analysis was carried out to identify the topics and patterns of relevant factors that influence the interoperability and cybersecurity of remote patient monitoring medical devices used for chronic disease management. Furthermore, this study will identify potential considerations that could improve integration and data security among the different digital healthcare components while fostering healthcare practices, patient care, and outcomes in chronic disease management.

3.3 Research strategy

The research methodology followed in this thesis is represented graphically by applying the research onion that was introduced by Saunders et al. (Saunders *et al.*, 2023). Figure 4: Saunders research onion (Saunders *et al.*, 2023) illustrates the chosen method for the research, and the following sections describe the different layers of research onion that relate to this thesis.

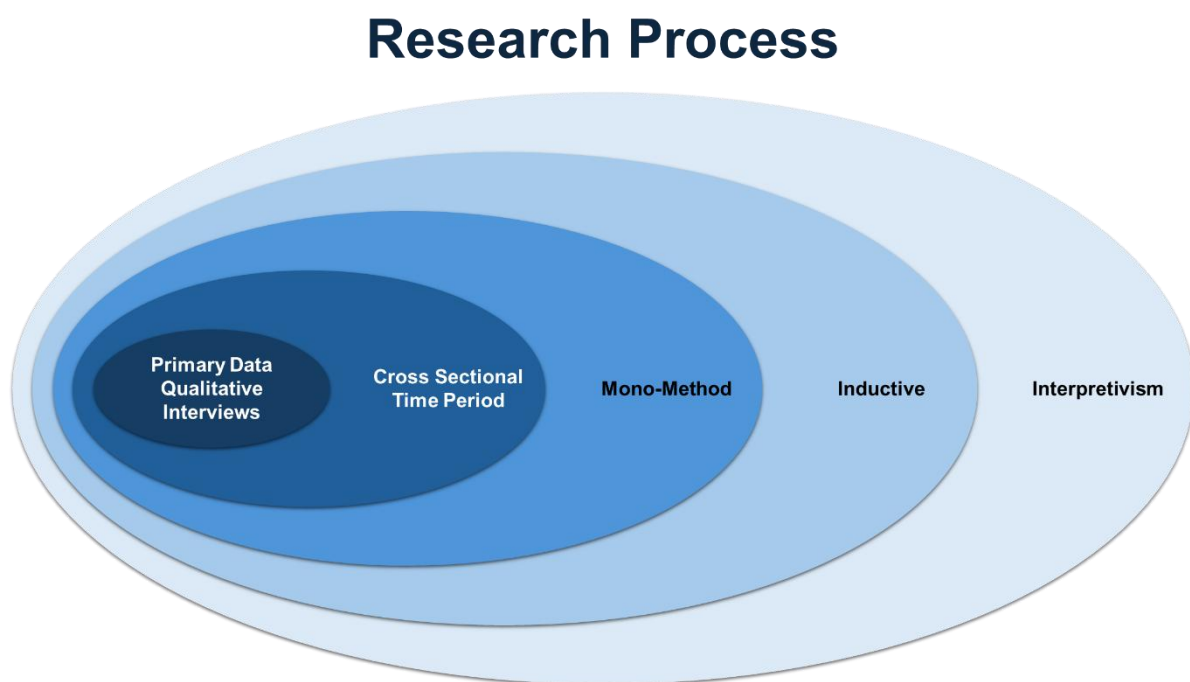


Figure 4: Saunders research onion (Saunders *et al.*, 2023)

3.3.1 Philosophical approach – Interpretivism

Interpretivism was considered as the approach for this study, as it describes the concept that reality is not objective but is based on an individual's experience and interpretation.

Interpretivism is relevant for this study because understanding unique experiences and perspectives on interoperability and cybersecurity challenges in remote patient monitoring medical devices from experts in development, manufacturing, application and maintenance is vital. The data gathered assists in gaining deeper insights in developing resilient and interoperable remote patient monitoring medical devices for chronic disease management. Therefore, this approach assists in understanding various perspectives for gathering valuable, qualitative data through interviews.

3.3.2 Inductive approach

The inductive approach was considered for this study, as it is useful in observing data, identifying patterns, and proceeding with conclusions. This approach allows for flexibility and could help identify unexpected findings from the data.

An inductive approach is relevant for analysing the data gathered through interviews from experts in the healthcare industry. Also, this approach assists in identifying repeating themes, common challenges, and frequently mentioned solutions, and in finding patterns and developing broader understanding.

The inductive approach allows the development of a theoretical framework based on the insights and experiences gathered through interviews, improving understanding of interoperability and cybersecurity in remote patient monitoring medical devices. This approach assists in deriving conclusions that are specific and relevant for this study.

3.3.3 Data Collection Methods

Monomethod implies the use of only one method for data collection in a study. The primary data for this research was gathered through interviews with experts in the healthcare industry, and it is a mono-method approach. Interviews provide qualitative data that includes expert opinions, experiences, and insights, a valuable source for exploring the evaluating roles of interoperability and cybersecurity in remote patient monitoring devices. The responses obtained through detailed questions from experts can help in understanding the challenges and solutions related to your research questions.

As part of primary data collection, participants were asked questions on the topics listed in Table 1: Participant interview topic; each topic consists of a set of questions detailed in Appendix A. These questions were thoughtfully framed to encourage participants to elaborate on their experiences, avoiding short responses. The open-ended characteristics of the questions allowed for meaningful discussions and the gathering of valuable data. Where necessary, follow-up questions were used to expand and gain more detailed insights during the interviews. A similar set of questions was used to interview all the participants to ensure a consistent approach throughout the research process. This approach facilitates minimising the variability in responses and comparison. The key emphasis was on understanding participants' perceptions and their unique experiences to address the research objectives. The data collected from these interviews was analysed using thematic analysis. This method involved identifying recurring themes or patterns within the responses through keyword analysis. The themes were compared across the participants to identify common experiences or contrasting opinions. Furthermore, this approach allowed evaluation of whether the findings are aligned or diverged from current research on the topic. This discursive method provided subjective and specific insights, unlike responses through structured survey questionnaires. The interview approach gathered individuals' experiences in depth, perspectives and understandings relevant to the topic.

Participants were identified and contacted through GCD and researchers' professional network to nominate either themselves or someone in their professional network or contacts for the interview.

Participants who are qualified experts from the healthcare industry aged between 25 and 64 years were requested from different disciplines, including healthcare roles such as research and development, regulatory affairs, medical affairs, manufacturing, and academia professionals involved in remote patient monitoring medical devices use, manufacturing and development, and to provide a good sample spread. All participants have had a full-time experience in their expertise areas for a minimum of five years within the last ten years, with an aim to interview seven participants.

3.3.4 Cross sectional time period

The objective of this research was to understand knowledge and perceptions at a particular point in time, so the requirement for data collection is only once and doesn't require repetition of data collection. However, future follow-up could be requested based on future circumstances related to the findings of this research or other new studies, particularly related to interoperability and cybersecurity in remote patient monitoring medical devices for

chronic disease management. Hence, the study used a cross-sectional time horizon rather than a longitudinal one. This research collected data through interviews between April and May 2025.

3.3.5 Data collection

The research study utilises both primary and secondary data collection methods. Primary data collection involves gathering data through interviews, surveys, and observations (Blessing *et al.*, 2024). One of the key primary data collection methods is interviewing experts to gather information and gain their insights. Secondary data collection involves utilising existing information through literature reviews of academic papers, reports, and other published materials (Blessing *et al.*, 2024).

Significance of data collection techniques: Primary data corresponds to the specific information gathered in relevance to research questions. Primary data collected using qualitative approaches help in understanding individual's experiences, opinions, and challenges (Blessing *et al.*, 2024). Interviews can provide in-depth understanding of topics like interoperability and cybersecurity challenges in remote patient monitoring medical devices from the perspective of those who develop and use them.

Secondary data collected through a thorough literature review assists in understanding existing knowledge and identifying gaps. A literature review helps understand the current state of research on interoperability and cybersecurity in remote patient monitoring medical devices. Also, it allows setting the content and development of interview questions (Blessing *et al.*, 2024).

Interviews assist in acquiring deeper insights and allow researchers to understand the "how" and "why" aspects from the responses. They facilitate gathering valuable data and provide opportunity to ask follow-up questions and clarifications related to practical challenges, solutions, and opinions that could result in finding out patterns, trends and perspectives. (Hurst, 2023; Blessing *et al.*, 2024).

Justification for Using Interviews in This Study: The aim of this research is to evaluate the roles of interoperability and cybersecurity, which are considered complex and evolving in the healthcare industry. Expert interviews are critical for gathering existing knowledge about the challenges and solutions related to interoperability and cybersecurity in remote patient monitoring medical devices and healthcare areas like chronic disease management and patient safety, which can influence the efficacy of procedures and patient outcomes (Wang *et al.*, 2018; Khater *et al.*, 2024; Jaatun *et al.*, 2024; Shah, 2025). The qualitative data from interviews and the secondary data from the literature review can complement each other.

The insights from expert opinions can validate, challenge, or provide new perspectives on the findings in assessing enablers, drivers, and barriers relevant to interoperability and cybersecurity in remote patient monitoring medical devices for chronic disease management.

The interview topics were divided into five topics as listed below in Table 1: Participant interview topic and each topic includes a set of questions as listed in Appendix A.

Sl. No.	Topics
1	Remote patient monitoring (RPM) medical devices
2	Cybersecurity — Data Privacy and Security
3	Interoperability — Data Exchange
4	Regulations
5	Usability/Applications

Table 1: Participant interview topics

Participants interviews:

- Each participant was sent an online meeting invitation with a Zoom link.
- Each participant received a follow-up email with information on the research aim, questions, consent form, and PIL.
- By using the topics in Table 1: Participant interview topic and questions in Appendix A, interviews were conducted. All the interviews were audio recorded using the Zoom platform.
- Based on the audio recording and discussions, transcripts were prepared by the researcher.
- Data was collected from the transcripts for analysis.

3.4 Data analysis – Thematic analysis

Data analysis is a key part of research, and it includes processing of raw data into meaningful information, assisting to make informed decisions based on evidence. Data analysis assists in identifying trends, correlations, patterns, and opportunities for improvement, thus facilitating the effective addressing of customer needs. Data analysis supports developing a knowledge base and further advancements, and also, it can support hypothesis testing (Blessing *et al.*, 2024).

Thematic Analysis: it is one of the key methods that can be used for analysing qualitative data. It focuses on the identification, analysis, and representation of themes in a given set of

data. This process includes data coding followed by categorization into themes and identification of patterns or trends (Saunders *et al.*, 2023).

Significance of thematic analysis to analyse Qualitative Data: Thematic analysis provides a structured approach to understanding qualitative data, collected through interview transcripts (Blessing *et al.*, 2024). Identifying themes assists researchers to understand the common ideas, opinions, and experiences expressed by participants. Further steps such as coding and categorising help to identify key patterns and significance that emerge from the data. It facilitates obtaining a deeper understanding of the research topic by going beyond simple summaries of the data (Walker *et al.*, 2019; Ramirez, 2024).

Relevance of Thematic Analysis for This Study: This research focuses on collecting qualitative data through expert interviews and generating qualitative data. Thematic analysis is an appropriate method for analysing the type of data gathered through interview. It facilitates to systematically analyse the experts' insights on interoperability and cybersecurity real-time challenges and solutions in remote patient monitoring medical devices. The application of thematic analysis can identify key themes related to interoperability and cybersecurity in remote monitoring medical devices (Walker *et al.*, 2019; Ramirez, 2024):

- Enablers, drivers and barriers of interoperability.
- Enablers, drivers and barriers of cybersecurity.
- Further analysis could assist in identifying the best practices, current framework, regulations, standards, and future trends.

Another source of data is the literature review, which can provide qualitative data that can be analysed using thematic analysis, a qualitative data analysis method (Tian *et al.*, 2021; Ramirez, 2024). A systematic identification and analysis could identify the common themes from both expert interviews and the literature review findings, facilitating a comprehensive evaluation of the roles of interoperability and cybersecurity in the context of remote patient monitoring for chronic disease management.

3.5 Ethical considerations

3.5.1 Ethics approval

The Griffith College Innopharma ethics committee approved and accepted the research before to the involvement of participants. The ethical application form was included in Appendix D of this report.

The dissertation supervisor approved the interview questions without the need for consulting the Griffith College Innopharma ethics committee. The interview did not have questions relating to specific events involving medical equipment, except for the role-specific questions. All responses were handled with strict confidentiality and were not disclosed to the regulator, the public, or the organisation. Participation was voluntary. No participant retracted consent before or following the interviews. Thus, it may be concluded that the data collection process presented no ethical concerns.

3.5.2 Informed consent & confidentiality

The Participant Information Letter (PIL), included in Appendix B of this report, was sent to each potential participant, detailing the topic content and objectives of the research. The brief introductory letter, along with the PIL, Participant Information Letter (PIL), included in Appendix C of this report, and interview questions as outlined in Appendix A, were sent out by email. It assists in introducing the researcher and their background, the topic of study, and the objectives of the study. The interview details specified that a series of open-ended questions will be asked.

As signed consent was obtained from each participant prior to the interviews, and anonymity was ensured in the data processing and presentation by the use of codes, as outlined in Table 2: Participant coding by role. Participants were informed that their participation might improve the understanding of the factors and considerations that influence interoperability and cybersecurity in remote patient monitoring medical devices for chronic disease management.

3.5.3 Confidentiality and anonymity

Anonymity was ensured in the data analysis by assigning individuals numerical codes ranging from 1 to 11, as indicated in Table 2: Participant coding by role. The order of the interviews was determined by the chronological date, with participant 1 being the first interviewed. A transcript was submitted for review, and upon approval, it was used for data interpretation and analysis. Participants had the right to withdraw at any point until two weeks post-interview. No participants retracted their permission for this study.

Participant	Role
Participant 1	Manufacturing/Operations Specialist
Participant 2	Cybersecurity Professional

Participant 3	Program/Project Manager
Participant 4	Regulatory Affairs Professional
Participant 5	Systems Engineering Professional
Participant 6	Software Engineering Professional
Participant 7	Medical Affairs Professional
Participant 8	Global Marketing Professional
Participant 9	Software Engineering Professional
Participant 10	Quality Systems Engineering Professional
Participant 11	Healthcare Professional

Table 2: Participant coding by role

3.5.4 Data storage and security

The audio recording and interview transcripts will be stored for a period of two years post-submission if the research remains unpublished or for four years if the research is published. The data will be stored on a password-protected laptop, with the researcher being the exclusive user. The laptop will be secured in a locked cabinet within the researchers' residence, specifically in a room designated for work and study.

Chapter 4. Analysis and Findings

4.1 Introduction

The thematic data analysis technique was used to analyse the qualitative data collected through the interviews with participants experienced in remote patient monitoring (RPM) medical devices, cybersecurity, or interoperability (Blessing *et al.*, 2024). The approach followed allows exploring the individual insights and experiences through one-to-one discussions. The data was analysed to address the research objectives.

Thematic analysis is appropriate for this study because it helps uncover common perspectives and experiences related to RPM, cybersecurity, and interoperability. Also, the thematic analysis technique facilitates identifying, analysing, and reporting themes within qualitative data. During the analysis, appropriate statements, phrases, or keywords were identified by going through the interview discussions and transcripts. The initial codes were assigned to this information. Furthermore, patterns were identified based on the grouping of codes and categories, followed by the development of themes related to research objectives (Saunders *et al.*, 2023; Blessing *et al.*, 2024).

Research Objectives:

Objective #1: Identify the current standards available for interoperability and cybersecurity in remote patient monitoring medical devices.

Objective #2: Assess drivers, enablers, and barriers relevant to interoperability in remote patient monitoring medical devices.

Objective #3: Assess drivers, enablers, and barriers relevant to cybersecurity in remote patient monitoring medical devices.

Objective #4: Assess the current state of interoperability and cybersecurity frameworks in remote patient monitoring medical devices.

Objective #5: Identify the potential considerations that could improve integration and data security of the different digital healthcare components.

4.2 Interview setting and Participant profile

Each participant was asked to provide responses to the interview questions, as per Appendix A. These questions were framed based on the research objectives to explore and

gather participants' experiences and insights on interoperability, cybersecurity, regulations and standards in remote patient monitoring medical devices for managing chronic disease management. The participants were chosen as a representation of different stakeholders involved in the medical device life cycle phases. At instances, follow-up questions were asked for deeper understanding of the considerations and challenges with relevant examples based on the participant's expertise.

During the interviews, in a few instances participants provided responses for more than one question because of the dependences based on their experience, relevance and the context of the topics. However, questions were excluded only in the instances where participants had adequate knowledge or relevant experience on the topic. The interview process ensured that participants were asked questions in all five topics designed for the interviews. The sequence questions were altered with a few participants to continue the engagement and relevance of the discussions.

The Zoom meeting platform was used to schedule and conduct interviews with all the participants. Participants were requested to join for one-to-one discussions over Zoom online meetings, and the discussion was recorded using the in-built Zoom audio recording feature. The audio recording of the interviews benefitted in numerous instances during the transcript preparation and data analysis. Each participant received interview transcript that was prepared after each meeting by the researcher using the audio recordings.

The duration of the interviews varied across participants, and in a few instances the interviews were up to 45 minutes. The interviews were scheduled and conducted based on participants' availability, as a few of the participants reside in the United States and to suit the time zones. The interviews were conducted during the weekdays and weekends, during the office hours and outside the office hours.

The interview topics were framed in such a way that the initial topic focuses on basic questions to set the context of the RPM devices for various reasons. One of the main reasons for starting the interview with basic questions was to help the participants engage and involve themselves in the conversation. As the later sections of the interview were too intense, it is to help the participants to gather focus and become involved in deeper discussions. The participants discussed a wide variety of medical devices, including simple devices like glucose monitors and wearables, as well as complex devices that integrate with MRI technology. There was a lot of emphasis on the data, cybersecurity, interoperability, regulations/ standards, challenges, trust, and cost, as illustrated in the Figure 5: Keyword identified from the interview transcript.

All participants voluntarily agreed to participate in the interviews to discuss their experiences and opinions regarding the questions that were asked. The interviews were completed with all the participants, and overall, the participation is satisfactory. All participants provided candid answers and were to elaborate on specific topics and follow-up questions. The interview process allowed the researcher to gain deeper insights on interoperability and cybersecurity in RPM for chronic disease management with their consent, along with open engagement, which facilitated primary data collection for this study with greater confidence.

The interview process involved discussion with eleven participants who belong to various stakeholder groups associated with medical device life cycle phases such as Design and Development, Manufacture/Operations, Pre-Market Assessment and Approval, and Post-Market Surveillance & Management to gather adequate and relevant information, as per the information in the Table 3: Participants associated with medical device life cycle phases. These participants belong to different functional departments such as R&D systems engineering, R&D cybersecurity, R&D software engineering, program/project management, regulatory affairs, medical affairs and healthcare professionals. The participants are working professionals with leading medical device manufacturers and healthcare facilities spread across different geographical locations. They are working or previously worked on medical devices intended for remote patient monitoring and managing chronic disease conditions.

Participant	Role	Life Cycle Phase
Participant 1	Manufacturing/Operations Specialist	Manufacture
Participant 2	Cybersecurity Professional	Design and Development
Participant 3	Program/Project Manager	Manufacture
Participant 4	Regulatory Affairs Professional	Pre-Market Assessment and Approval Post-Market Surveillance & Management
Participant 5	Systems Engineering Professional	Design and Development
Participant 6	Software Engineering Professional	Design and Development
Participant 7	Medical Affairs Professional	Design and Development Post-Market Surveillance & Management

Participant	Role	Life Cycle Phase
Participant 8	Global Marketing Professional	Design and Development Post-Market Surveillance & Management
Participant 9	Software Engineering Professional	Design and Development
Participant 10	Quality Systems Engineering Professional	Design and Development Manufacture Post-Market Surveillance & Management
Participant 11	Healthcare Professional	Post-Market Surveillance & Management

Table 3: Participants associated with medical device life cycle phases

The knowledge of these participants working in different functions, devices or systems, roles, and domains and this broad range of varied skills are essential for this study. It helps in exploring the multiple areas and dimensions in understanding the considerations and challenges associated with RPMDs. The experience level of the participants selected for this study varies between 7 years and 20 years in healthcare or medical devices or other regulated industry.

4.3 Analysis and Findings

4.3.1 Preliminary Analysis: Key Words

The interview transcripts were analysed to understand the common terminology used by the participants during the discussion. The following illustrated in the Figure 5: Keyword identified from the interview transcript are a few of the keywords that were frequently used by the participants while discussing the topics RPM, cybersecurity, interoperability, regulations and standards, application and usability:

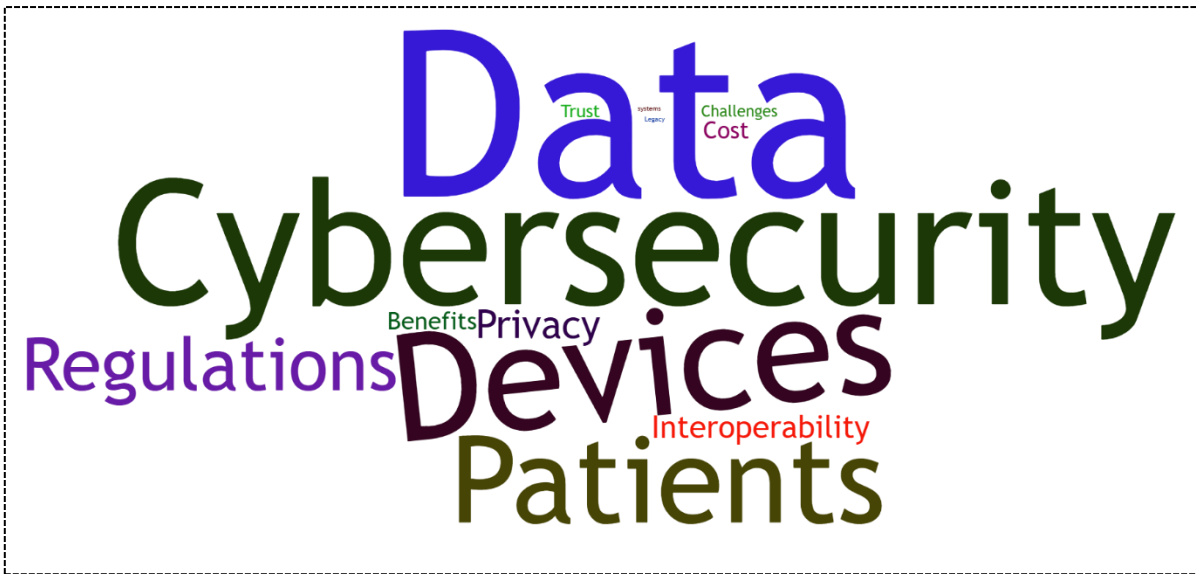


Figure 5: Keyword identified from the interview transcript

- **Data:** The term “data” was used more frequently during discussions including different variations, such as patient data, health data, sensitive data, data privacy, data security, data exchange, data integrity, data management, and data overload.
- **Cybersecurity:** The term “cybersecurity” was used more frequently during discussions, including different variations, such as cybersecurity threats, data security, security measures, network security, security by design, security updates, and cyber-attacks.
- **Devices:** The term “devices” was used more frequently during discussions, including different variations, such as RPM devices, medical devices, legacy devices, implantable devices, and connected devices.
- **Patients:** The term “patients” was used more frequently during discussions.
- **Regulations:** The term “regulations” was used moderately during discussions, including different variations, such as GDPR, HIPPA, IEC, NIST, FDA, global regulations, unified standards, data standards, regulatory bodies, and regulatory pathways.
- **Privacy:** The term “privacy” was used moderately during discussions.
- **Interoperability:** The term “interoperability” was used moderately during discussions, including different variations, such as integrating systems, data exchange, and connectivity.
- **Benefits:** The term “benefits” was used less frequently during discussions.

- **Cost:** The term “trust” was used less frequently during discussions.
- **Trust:** The term “trust” was used less frequently during discussions.
- **Challenges:** The term “challenges” was used less during discussions, including different variations, such as primary challenges, significant challenges, technical issues, and complexity.
- **Legacy systems:** The term “legacy systems” was used less frequently during discussions.

4.3.2 Analysis – Cybersecurity Threats & Vulnerabilities

The interview data was analysed to identify the different aspects including codes, patterns and theme related to cybersecurity in RPMDs are illustrated in Figure 6: Cybersecurity Threats & Vulnerabilities — Codes, patterns and themes and as follows:

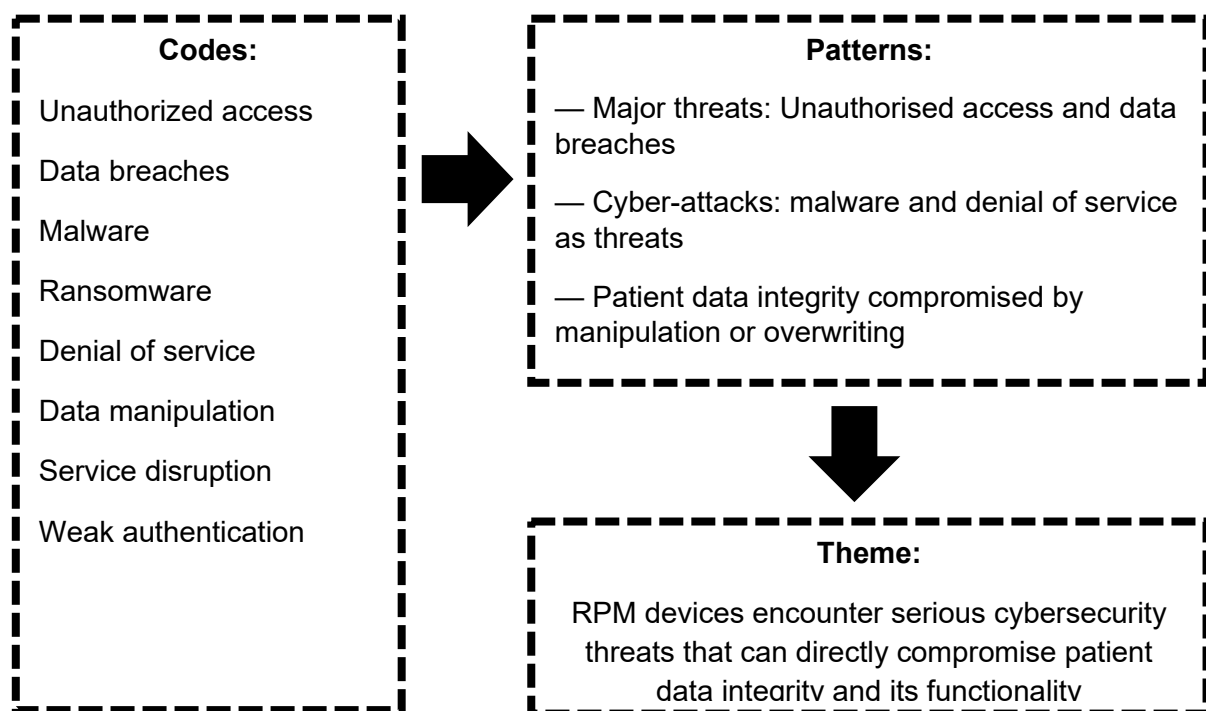


Figure 6: Cybersecurity Threats & Vulnerabilities — Codes, patterns and themes

- **Theme:** RPM devices encounter serious cybersecurity threats that can directly compromise patient data integrity and its functionality.
- **Patterns:**
 - During the discussions, unauthorised access and data breaches were highlighted as major threats to RPMS devices by the participants.

- During the discussions, cyber-attacks such as malware and denial of service were mentioned by the participants.
- During the discussions, patient data integrity compromise, either by manipulation or overwriting, was mentioned by participants.
- **Codes:** Unauthorized access, data breaches, malware, ransomware, denial of service, data manipulation, service disruption, weak authentication.

This theme emphasizes that RPMDs should include robust security measures to ensure secure device operation and data safety because of cyber-attacks. The information from the interviews suggests consensus among the participants in relation to the device operations and patient data security.

4.3.3 Analysis — Interoperability Challenges

The interview data was analysed to identify the different aspects including codes, patterns and theme related to interoperability challenges in RPMDs are illustrated in Figure 7:

Interoperability Challenges — Codes, patterns and themes and as follows:

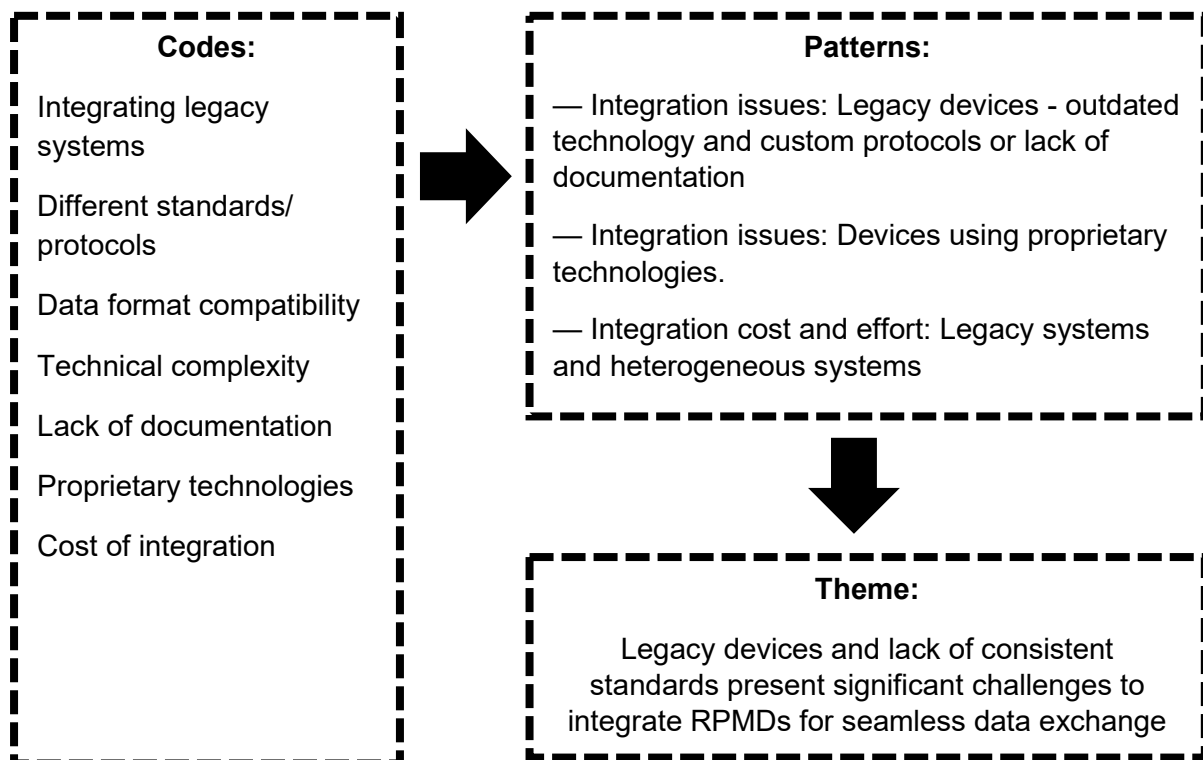


Figure 7: Interoperability Challenges — Codes, patterns and themes

- **Theme:** Legacy devices and lack of consistent standards present significant challenges to integrate RPMDs for seamless data exchange.

- **Patterns:**
 - During the discussions, integration issues due to legacy devices using outdated technology and custom protocols or lack of documentation were highlighted by the participants.
 - During the discussions, integration issues with devices using proprietary technologies were mentioned by the participants.
 - During the discussions, the cost and effort required for integration, specifically with legacy systems, were mentioned by the participants.
- **Codes:** Integrating legacy systems, different standards/protocols, data format compatibility, technical complexity, lack of documentation, proprietary technologies, cost of integration.

This theme signifies the importance of standardised protocols and communication methodologies to facilitate device integration and data exchange seamlessly. The information from the interviews suggests consensus among the participants in relation to the legacy device issues and lack of standardised communication protocols.

4.3.4 Analysis — Regulations and Standards

The interview data was analysed to identify the different aspects including codes, patterns and theme related to regulations and standards in RPMDs are illustrated in Figure 8: Regulations and Standards — Codes, patterns and themes and as follows:

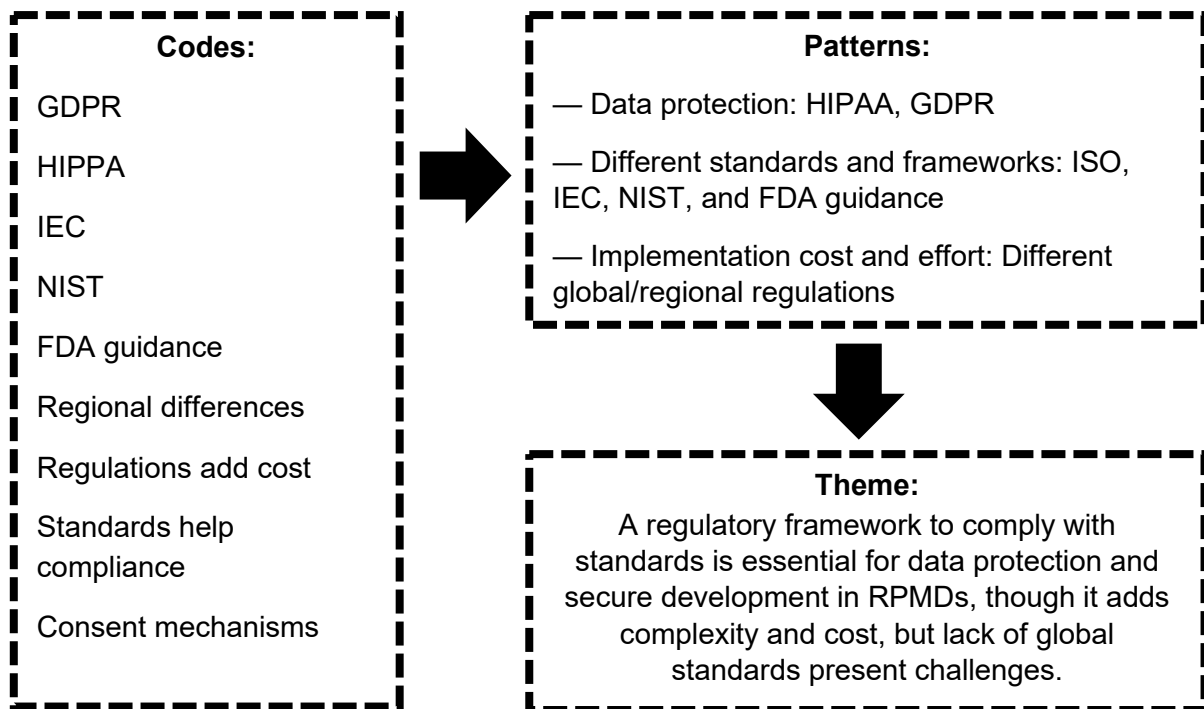


Figure 8: Regulations and Standards — Codes, patterns and themes

- **Theme:** A regulatory framework to comply with standards is essential for data protection and secure development in RPMs, though it adds complexity and cost, but lack of global standards present challenges.
- **Codes:** GDPR, HIPPA, IEC, NIST, FDA guidance, regional differences, regulations add cost, standards help compliance, consent mechanisms.
- **Patterns:**
 - During the discussions, the data protection regulations such as GDPR in the EU and HIPAA in the US were mentioned as primary drivers for data security and privacy in RPMs by participants.
 - During the discussions, different standards and frameworks (such as IEC, NIST, and FDA guidance) were mentioned as essential for ensuring compliance and incorporating security by participants.
 - During the discussions, factors that impact development and add cost to RPMs because of different global/regional regulations were mentioned by participants.

This theme highlights the data protection regulations in ensuring data security and privacy in the RPMs and the lack of global standards impacting the RMPD's development and cost. The information from the interviews suggests consensus among the participants in relation to the availability of different standards and guidance on incorporating security measures.

4.3.5 Analysis — Patient Benefits and Outcomes

The interview data was analysed to identify the different aspects including codes, patterns and theme related to patient benefits and outcomes to users by RPMDs are illustrated in Figure 9: Patient Benefits and Outcomes — Codes, patterns and themes and as follows:

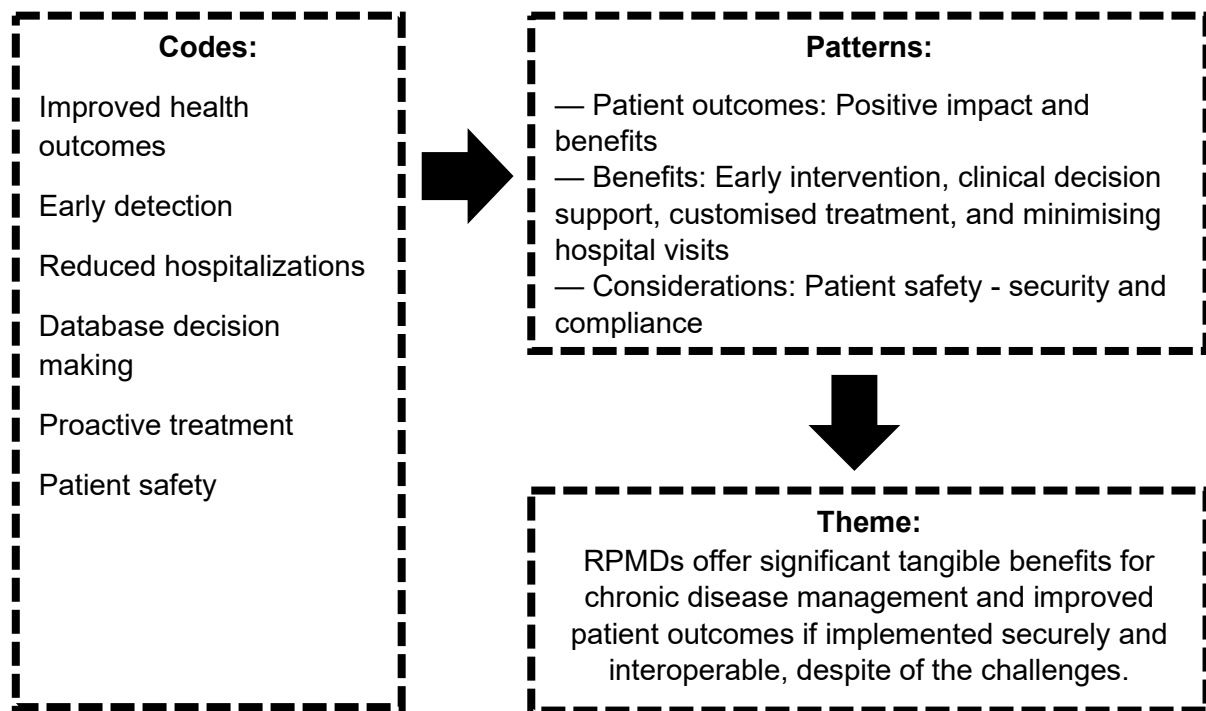


Figure 9: Patient Benefits and Outcomes — Codes, patterns and themes

- **Theme:** RPMDs offer significant tangible benefits for chronic disease management and improved patient outcomes if implemented securely and interoperable, despite of the challenges.
- **Codes:** Improved health outcomes, early detection, reduced hospitalizations, database decision making, proactive treatment, patient safety.
- **Patterns:**
 - During the discussions, the positive impact and benefits of RPMDs on patient health outcomes were discussed by participants.
 - During the discussions, benefits such as early intervention, clinical decision support, and customised treatment, and minimising hospital visits were highlighted by participants.
 - During the discussions, considerations for patient safety as a key driver for security and compliance in RPMDs were mentioned by participants.

This theme signifies that successfully implemented RPMDs will offer significant benefits to the users and help in improving the patient outcomes, with the patient as a key driver for security and compliance in RPMDs. The information from the interviews suggests consensus among the participants in relation to the improved patient outcomes and other benefits, including early intervention and clinical decision support.

4.3.6 Analysis — Cybersecurity and Interoperability Current State

The interview data was analysed to identify the different aspects including codes, patterns and theme related to the current state of cybersecurity and interoperability in RPMDs are illustrated in Figure 10: Cybersecurity and Interoperability Current State — Codes, patterns and themes and as follows:

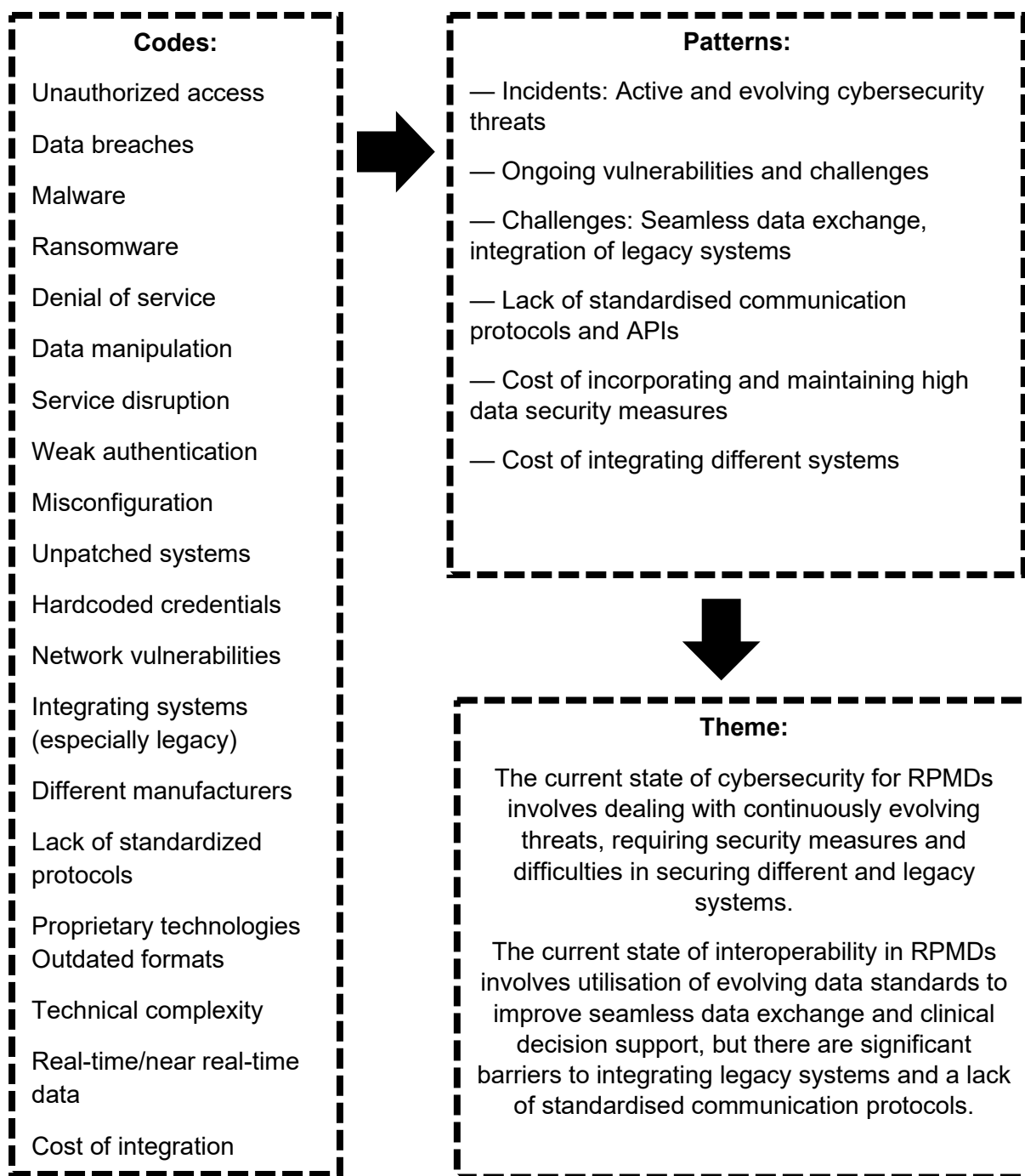


Figure 10: Cybersecurity and Interoperability Current State — Codes, patterns and themes

- **Theme:** The current state of cybersecurity for RPMDs involves dealing with continuously evolving threats, requiring security measures and difficulties in securing different and legacy systems.
The current state of interoperability in RPMDs involves utilisation of evolving data standards to improve seamless data exchange and clinical decision support, but

there are significant barriers to integrating legacy systems and a lack of standardised communication protocols.

- **Codes:** Unauthorized access, data breaches, malware, ransomware, denial of service, data manipulation, service disruption, weak authentication, misconfiguration, unpatched systems, hardcoded credentials, network vulnerabilities, Integrating systems (especially legacy), different manufacturers, lack of standardized protocols, proprietary technologies, outdated formats, technical complexity, real-time/near real-time data, cost of integration.
- **Patterns:**
 - During the discussion, incidents such as active and evolving cybersecurity threats impacting RPM devices were highlighted by participants.
 - During the discussion, ongoing vulnerabilities and challenges within the current state were highlighted by participants.
 - During the discussion, significant challenges in achieving seamless data exchange, specifically with the integration of legacy systems, were highlighted by participants.
 - During the discussion, the lack of standardised communication protocols and APIs was highlighted by participants.
 - During the discussion, the cost of incorporating and maintaining high data security measures, as well as the cost of integrating different systems, was highlighted by participants.

This theme indicates that the current state of cybersecurity provides resilience in the latest systems to mitigate threats and vulnerabilities. However, this is an issue in the legacy systems or systems that are poorly maintained. This theme indicates that the current state of interoperability has advantages to utilising evolving standards for seamless data exchange. However, there are significant challenges associated with integrating the complete healthcare ecosystem.

4.3.7 Analysis — Cybersecurity and Interoperability Considerations

The interview data was analysed to identify the different aspects including codes, patterns and theme related to the cybersecurity and interoperability considerations in RPMDs are illustrated in Figure 11: Cybersecurity and Interoperability Considerations — Codes, patterns and themes and as follows:

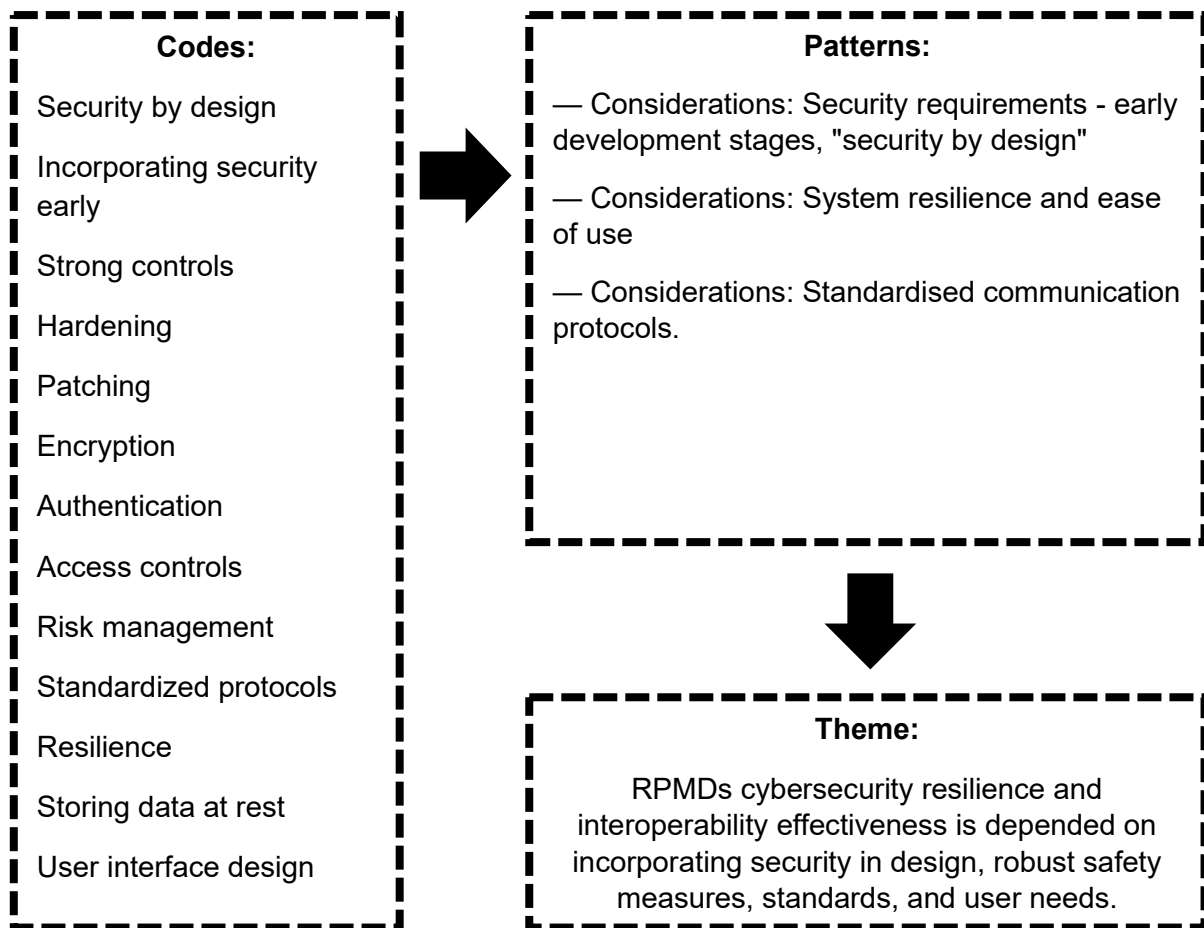


Figure 11: Cybersecurity and Interoperability Considerations — Codes, patterns and themes

- **Theme:** RPMDs cybersecurity resilience and interoperability effectiveness is depended on incorporating security in design, robust safety measures, standards, and user needs.
- **Codes:** Security by design, incorporating security early, strong controls, hardening, patching, encryption, authentication, access controls, risk management, standardized protocols, resilience, storing data at rest, user interface design.
- **Patterns:**
 - During the discussions, considerations of security requirements in the design from the early development stages, "security by design", were highlighted by participants.
 - During the discussions, considerations for system resilience and ease of use focusing on the device functionality to meet intended use during loss of connectivity were highlighted by participants.

- During the discussions, the significance of specific approaches like encryption, strong authentication and access controls, and regular patching/software updates was emphasised by participants.
- During the discussions, consideration for using standardised communication protocols (such as HL7 and DICOM) to improve interoperability was highlighted by participants.

This theme signifies the key considerations for cybersecurity and interoperability in RPMDs, such as security by design, system resilience, ease of use and standardised communication protocols focusing on interoperability. The information from the interviews suggests consensus among the participants in terms of approaches to be followed to minimise the impact on RPMD's functionality.

4.3.8 Analysis — Additional Insights by Participants

The following are the additional finding identified by analysing the interview data in relation to assessing cybersecurity and interoperability roles in remote patient monitoring medical devices of chronic disease management.

- If the devices are meant to be used in an open setting, a specific consideration on the anonymisation of patient data was highlighted.
- A consideration to include more than one connectivity option in RPMDs based on their risk class.
- A consideration to distinguish "real time" and "near real time" data reporting, which can potentially lead to ambiguity.
- Digital literacy barriers that can significantly impact patient adherence and the functionality of devices were highlighted.
- The cost and complexity associated with complying with regulation was highlighted that could potentially impact the innovators belonging to start-ups or small organisations in launching more advanced and beneficial products to market.
- Automation of workflows through user interface/experience design could potentially result in minimising the need for extensive user training.

4.3.9 Analysis — Common Considerations and Challenges

The following are common considerations and challenges identified by analysing the interview data in relation to assessing cybersecurity and interoperability roles in remote patient monitoring medical devices of chronic disease management. There were various viewpoints that were consistent across participants:

- Importance of integrating “Security by Design” early in the development process to build resilient RPDMs.
- Challenges and limitations associated to integrate RPDMs with legacy systems in relation to interoperability.
- Significance of regulations such as GDPR and HIPAA in driving data security and privacy requirements in the development of RPMDs.
- Robust security measures implementation incurs additional costs on RPMDs.
- Patient safety and improved outcomes are priorities in driving the efforts for the future state of cybersecurity and interoperability in RPDMs.
- The importance of trust and training for successful adoption and use of RPDMs.
- The priority for data privacy and security in RPDMs.

4.3.10 Analysis — Contradicting Considerations and Challenges

There were no major contradictions by analysing the interview data in relation to assessing cybersecurity and interoperability roles in remote patient monitoring medical devices of chronic disease management. However, there were differing levels of emphasis:

- A few of the participants strongly highlighted the cost as a burden for complying with regulations, while others stressed patient safety first and cost as a secondary factor. Also, security investments are tangibly related to patient benefits.
- A few of the participants, in relation to data anonymisation, took slightly different approaches, such as a few participants being inclined towards avoiding the collection of identifiable data, while the other participants had the option to anonymise data on the device display.

4.3.11 Findings: RPMDs Interoperability and Cybersecurity – Standards

Interoperability – Standards:

The interoperability standards findings from the literature review include HL7 FHIR and DICOM align with the information gathered from the industry experts through interviews. However, other standards such as IEEE 11073, ISO 13606, ASTM CCR, and HL7 CDA & CCD (Robkin, 2015; Wang *et al.*, 2018; Saripalle *et al.*, 2019; Lehne *et al.*, 2019; Singh, 2024) were not mentioned during the discussions, signifies the lack of a standardised approach in adopting interoperability standards.

Cybersecurity – Standards:

The interoperability standards findings from the literature review include GDPR in the EU and HIPAA in the US (Baltaxe *et al.*, 2023; Vaidya, 2024; Singh, 2024) align with the information gathered from the industry experts through interviews. Similarly, other standards, including ISO 14971, ISO 27005 and FDA guidance, coincide with literature review and interview data analysis findings. However, the data analysed implies the standards are general and complex to implement.

4.3.12 Findings: Interoperability — Enablers, Drivers and Barriers

The following are key findings in relation to enablers, drivers and barriers influencing successful implementation of interoperability controls through literature review and interview data.

Enablers of Interoperability:

- The utilisation of existing data standards and protocols like HL7 FHIR and DICOM could facilitate seamless data exchange across devices and systems discussed during interviews, aligns with literature review findings (Saripalle *et al.*, 2019; Jendle *et al.*, 2023; Singh, 2024), and implies device manufacturers are making efforts in leveraging the current standards to incorporate interoperability features.
- A robust network framework and infrastructure are necessary to support the increasing demands of integrating devices and managing data transfers discussed during interviews, aligns with literature findings to develop infrastructure such as cloud-based platforms for improved data integration and management (Fernandez and Pallis, 2014; Peyroteo *et al.*, 2021; Singh, 2024; K *et al.*, 2024), which implies the focus for future demand and effective data management.

- Multiple connectivity options such as Ethernet, Wi-Fi, and Bluetooth within devices enable connectivity in different healthcare and use settings discussed during interviews, aligns with literature findings to practice an open architecture model to facilitate seamless integration with different technologies such as Bluetooth and networks (Wang *et al.*, 2018; U.S. Food & Drug Administration (FDA) [Online], 2023b), which implies minimising the dependencies on custom technologies.
- Incorporating standardised data formats in devices facilitates integrating devices and seamless data exchange discussed during interviews, aligns with literature review findings (Saripalle *et al.*, 2019; Jendle *et al.*, 2023; Singh, 2024), which implies that standardised data formats are essential for the effective interoperability.
- Additionally, incorporating interoperability requirements at early stages of device development ensures robust product features for connectivity and seamless data exchange were discussed during interviews. However, additional literature review findings include unified healthcare infrastructure and collaboration among stakeholders (Fernandez and Pallis, 2014; Hassanaly and Dufour, 2021; Singh, 2024; K *et al.*, 2024), which are key for achieving effective interoperability.

Drivers of Interoperability:

- Discussions about informed clinical decision support are a significant driver facilitating bi-directional data exchange and provide healthcare professionals with necessary information for timely intervention, align with the literature review findings of the need for efficient healthcare systems and minimized costs (Fernandez and Pallis, 2014; Wang *et al.*, 2018; Jaatun *et al.*, 2024; Singh, 2024), which are key for improving efficacy and providing affordable healthcare services.
- Discussions about integration with electronic health records (EHRs) and patient data management systems are essential for patient information management and improving workflows, align with the literature review findings of the need for engaging patients in their own healthcare (Fernandez and Pallis, 2014; Wang *et al.*, 2018; Saripalle *et al.*, 2019; Singh, 2024), and signify the importance of interoperability in engaging and adopting the RPMDs.
- Discussions about features that support the integration of systems from different manufacturers for effective communication are necessary for digital healthcare systems and seamless data exchange, align with the literature review findings of the need for personalised and home-based healthcare (Peyroteo *et al.*, 2021; Baltaxe *et*

al., 2023; Sobahi and Bamabad, 2024; Ramirez, 2024), and signify the importance of interoperability for seamless data exchange in multiple use environments.

- Discussions about achieving improved patient outcomes through coordinated care enabling seamless data exchange, align with the literature review findings of the need for improving patient outcomes and the quality of decision-making (Wang *et al.*, 2018; Singh, 2024; K *et al.*, 2024), and signify the importance of interoperability in improving patient outcomes.
- Discussions about the ability to exchange data effectively to support data availability and database decision-making align with the literature review findings of the need for a learning health system (Wang *et al.*, 2018; Peyroteo *et al.*, 2021; Singh, 2024; Ramirez, 2024), which are key for improving the ability to support clinical decisions.

Barriers to Interoperability:

- A primary challenge is the integration of legacy systems using outdated technology and protocols with the latest systems highlighted in the interviews, aligning with the literature review findings of the integration of legacy systems (Singh, 2024), which could limit achieving a digital healthcare system capable of exchanging data effectively.
- The lack of standardised communication protocols for integrating different systems presents challenges for seamless data exchange highlighted in the interviews, aligning with the literature review findings of the lack of standardisation (Jendle *et al.*, 2023; Singh, 2024), which could limit device integration and seamless data exchange.
- The interview data analysis highlights the limitations associated with existing healthcare facilities' infrastructure could limit the integration of RPMs and functionality. However, the literature review findings about the organisational challenges include the varied interests, priorities, and workflows of stakeholders (Fernandez and Pallis, 2014; Singh, 2024), which implies the significance of an organisation and stakeholders impacting interoperability.
- Additional findings from interview data analysis include that the use of proprietary protocols creates closed loop challenges and restricts the integration of systems from different manufacturers. The cost associated with implementing effective infrastructure and integration solutions could limit the integration of RPMs and functionality. These signify the practical challenges impacting the interoperability in a healthcare setting.

- Additional findings from the literature review include that security and privacy concerns in the data exchange (Vaidya, 2024; Singh, 2024), and the complexity associated with complying with the regulations (Hassanally and Dufour, 2021; Jendle *et al.*, 2023; Singh, 2024), signify the dependencies associated which could impact the implementation of interoperability.

4.3.13 Findings: Cybersecurity — Enablers, Drivers and Barriers

The following are key findings in relation to enablers, drivers and barriers influencing successful implementation of cybersecurity measures through literature review and interview data.

Enablers of cybersecurity:

- Incorporating cybersecurity requirements at an early stage of the development process and throughout the lifecycle phases, meaning "security by design," strengthens the resilience of devices against threats discussed during interviews, aligns with the literature review findings on cybersecurity by design (U.S. Food & Drug Administration (FDA) [Online], 2023b; Jaatun *et al.*, 2024; Sobahi and Bamabad, 2024), and signifies the importance of a development framework that includes cybersecurity requirements.
- Adopting standardised security frameworks and standards facilitates managing risks effectively throughout the product lifecycle discussed during interviews, aligns with the literature review findings of security risk management frameworks (U.S. Food & Drug Administration (FDA) [Online], 2023b; Jaatun *et al.*, 2024; Vaidya, 2024), and highlights the importance of assessing and managing risks associated with sensitive patient data.
- Application of techniques such as data encryption, both for data stored on the device and data being transmitted, enhances data protection for sensitive information discussed during interviews, aligns with the literature review findings of data encryption (U.S. Food & Drug Administration (FDA) [Online], 2023b; Siemens-healthineers [Online], 2024; Vaidya, 2024; Singh, 2024), and highlights the significance of protecting and securing patient data.
- Updating systems regularly with software updates and patches is an essential aspect of mitigating vulnerabilities and maintaining secure devices over time discussed during interviews, aligning with the literature review findings of collaborative security strategy (Fernandez and Pallis, 2014; Hassanally and Dufour, 2021), signifying the

important elements needed to consider for securing the RPMDs from threats and vulnerabilities.

- Additionally, during the interviews, it was discussed that training and support to operate devices safely and effectively assists healthcare professionals and end-users in understanding the risks associated with security. However, the literature review highlights that a robust device and user authentication process could minimise the threats and vulnerabilities and also increase confidence to deliver secure services (U.S. Food & Drug Administration (FDA) [Online], 2023b; Singh, 2024).

Drivers of cybersecurity:

- Discussions about the security measures to protect against primary threats such as unauthorised access, data breaches, malware, and data manipulation are key drivers for improving cybersecurity and align with the literature review findings of the need for cyber resilient systems (U.S. Food & Drug Administration (FDA) [Online], 2023b; Vaidya, 2024; Shah, 2025), which could improve device security and data protection.
- Discussions about the security measures to ensure patient data privacy and integrity that are vital aspects for providing accurate diagnosis, treatment, and overall reliability of RPM systems align with the literature review findings of the need for secured patient data (U.S. Food & Drug Administration (FDA) [Online], 2023b; Vaidya, 2024; Singh, 2024; Shah, 2025), which implies effective and secure data management is key for RPMDs.
- Discussions about the security measures to protect patient safety are critical, as cybersecurity failures can potentially result in serious and even life-threatening incidents and align with the literature review findings of the need for cyber resilient systems (U.S. Food & Drug Administration (FDA) [Online], 2023b; Vaidya, 2024; Shah, 2025), which could improve device security and data protection.
- Discussions about the security measures that build and maintain trust with patients and healthcare professionals encourage the adoption and effective use of RPMDs and align with the literature review findings of the need for remote healthcare support (Khater *et al.*, 2024; Jaatun *et al.*, 2024; Vaidya, 2024; Singh, 2024; Shah, 2025), which benefits the adoption and application of RPMDs.
- Discussions about complying with regulations like HIPAA, GDPR, and FDA guidelines are mandatory driver that requires robust security measures and improves system resilience, aligns with the literature review findings of the need for specific

data protection regulations (Baltaxe *et al.*, 2023; Vaidya, 2024; Singh, 2024), and signifies the key elements of data protection and security.

Barriers of cybersecurity:

- Challenges associated with legacy systems or outdated technology could result in system exploitation and compromise security measures highlighted in the interviews, aligning with the literature review findings of cybersecurity threats (Machal, 2023; Vaidya, 2024; Singh, 2024; Shah, 2025), which could result in patient data compromise and security threats.
- The cost associated with implementing and maintaining high data security measures could be significant and might result in a limitation impacting the development cost and device price highlighted in the interviews, aligning with the literature review findings of cost and expertise (Jaatun *et al.*, 2024; Shah, 2025), which could impact the implementation of robust security measures.
- Inadequate controls to achieve a proper balance between incorporating robust security and offering clinical functionality and usability for healthcare professionals are challenges highlighted in the interviews, aligning with the literature review findings of usability and technical difficulties (Baltaxe *et al.*, 2023; Jaatun *et al.*, 2024; Sobahi and Bamabad, 2024; Vaidya, 2024), which impact the adoption and application of RPMDs in various healthcare and use settings.
- Navigating complex and sometimes differing global data protection regulations adds layers of difficulty and cost to device development and compliance highlighted in the interviews, aligning with the literature review findings of complex and generic guidelines (Jaatun *et al.*, 2024; Shah, 2025), which could impact the development of cyber resilient RPMDs.
- The nature of cyber threats that constantly evolve requires continuous monitoring and resources to minimise impact from new attacks to systems and sustain system resilience highlighted in the interviews, aligning with the literature review findings of cost and expertise (Jaatun *et al.*, 2024; Shah, 2025), which could impact monitoring of risk and implementation of robust security measures.
- Additionally, literature review findings include that challenges associated with the integration of heterogeneous systems could result in weak security controls (Wang *et al.*, 2018; Jaatun *et al.*, 2024; Singh, 2024).

4.3.14 RPMDs Interoperability and Cybersecurity – Current Frameworks

Interoperability – Current Framework: The interview discussions highlighted the current state of interoperability framework, focusing on the lack of standardised communication protocols, which is similar to the literature findings (Wang *et al.*, 2018). The evolution of the different levels of interoperability was highlighted in the interview discussion, which is similar to literature findings (K *et al.*, 2024). The other elements of the framework, such as security, privacy, device integration and bi-directional data communication, were discussed in the interviews by the participants and highlighted in the literature review (Saripalle *et al.*, 2019; Jendle *et al.*, 2023; Singh, 2024). Overall, the insights provided by the participants were similar to the literature review findings on the key components of an interoperability framework.

Cybersecurity – Current Framework: The interview discussions highlighted the current state of cybersecurity framework, focusing on the guidelines and best practices such as IEC/ISO 27001, IEC81001-5-1, the National Institute of Standards and Technology (NIST) and FDA's Secure Product Development Framework (SPDF), similar to literature review findings (Wang *et al.*, 2018; U.S. Food & Drug Administration (FDA) [Online], 2023b). Risk management ISO 14971, AAMI TIR 57, similar to literature review findings (Wang *et al.*, 2018; U.S. Food & Drug Administration (FDA) [Online], 2023b). Furthermore, similarity to adopt consistent processes to improve system resilience (Jaatun *et al.*, 2024; Shah, 2025). The significance of GDPR and HIPAA were discussed during the interviews, which was aligning with literature review findings (Baltaxe *et al.*, 2023). Regulatory compliance could be challenging due to these standards sometimes being complex, generic and incomplete (Jaatun *et al.*, 2024), as were similar findings from the interview data. Overall, the insights provided by the participants were similar to the literature review findings on the key components of a cybersecurity framework.

4.3.15 RPMDs Interoperability and Cybersecurity – Potential Improvements

The literature review and interview data analysis highlighted the following considerations as potential improvements in relation to interoperability for seamless data transfers through the integration of devices and systems and cybersecurity for device security and data protection, which are critical for the RPMDs:

- Both the literature review findings and participants emphasised the standardised approaches, such as protocols and APIs, for integration of devices and facilitating seamless data exchange (Singh, 2024).

- Both the literature review findings and participants emphasised improvement for data security, such as robust encryption and authentication protocols to prevent unauthorised access and improve data protection (Vaidya, 2024; Singh, 2024).
- Both the literature review findings and participants emphasised the importance of role-based or rule-based data access control to improve data security and accessibility (Vaidya, 2024).
- Both the literature review findings and participants emphasised that cybersecurity by design is a key consideration to improve system resilience and a means to minimise threats and vulnerabilities (Jaatun *et al.*, 2024; Shah, 2025).
- Both the literature review findings and participants emphasised that balance between implementation of security features to improve patient benefits and ethical considerations is essential (Jaatun *et al.*, 2024; Vaidya, 2024).

In summary, the data gathered from industry experts through interviews, which reflect their experience and expertise, resemble the findings of the literature review. These findings address the research objectives and help identify appropriate responses to the research questions regarding the roles of interoperability and cybersecurity in remote patient monitoring for chronic disease management.

Chapter 5. Discussion and recommendations

5.1 Research aim and objectives

The aim of this research is to assess the current standards available for interoperability and cybersecurity in remote patient monitoring medical devices. It also focusing on assessing the relevant drivers, enablers, and barriers for both interoperability and cybersecurity in these devices. Furthermore, the research will evaluate the current state of frameworks for these aspects and identify potential considerations that could lead to improved integration and data security of the different digital healthcare components.

The objective of this research is to gain deeper insights on interoperability and cybersecurity in remote patient monitoring medical devices form the healthcare professionals and different stakeholders involved in the development, usage and maintenance of digital healthcare system facilitating in remote monitoring and managing patients with chronic disease conditions.

5.2 Overview of key findings

The key findings of this research include the assessment of interoperability and cybersecurity significance in remote patient monitoring medical devices (RPMDs) used for chronic disease management. Interoperability and cybersecurity are the essential elements of a robust digital healthcare ecosystem. Effective interoperability controls are essential for the integration of different devices and systems in a network to facilitate seamless exchange of patient data, while strong cybersecurity measures protect sensitive data from threats and vulnerabilities. These both are critical for the safety and effectiveness of RPMDs, eventually resulting in improved patient outcomes and efficient healthcare delivery. The study is focused on assessing the key enablers, drivers, and barriers impacting these areas.

The literature review findings include that RPMDs are becoming increasingly important for managing patients with chronic conditions facilitating in patient data collection remotely. Another finding is the significance of existing standards for these devices. The importance of interoperability standards such as HL7 FHIR, DICOM for seamless exchange of patient health records. The importance of interoperability standards such as HIPAA in the US and GDPR in the EU mandate data protection measures. These regulations focus on similar security controls to protect sensitive data, focusing on integrity, authorization, availability, confidentiality, and secure updates. Also, noted the complexity involved in integrating legacy

systems that often use proprietary data communication protocols, impacting seamless data exchange. The literature review also indicated that different standards and guidelines exist but there are challenges associated in implementing them effectively across different technologies and healthcare settings.

The key findings from analysing the interview data from various stakeholders include that RPMDs and healthcare professionals provided practical, real-world insights into the challenges and considerations of interoperability and cybersecurity in RPMDs. Participants highlighted that RPM devices encounter serious cybersecurity threats, including unauthorised access, data breaches, malware, and data manipulation, that could result in compromising patient data integrity and device functionality. They highlighted the lack of standardised communication protocols, and the legacy systems present significant constraints in achieving seamless data exchange and interoperability. Participants agreed on the importance of regulations like GDPR and HIPAA as primary drivers for data security and privacy. Participants also consistently highlighted the significant patient benefits offered by RPMDs, such as improved patient outcomes and early detection and intervention, provided if devices are implemented securely and are interoperable. The interview data finding stressed the need for incorporating security early in the development phase, often referred to as "security by design", to build resilient systems. Another common consideration across the participants was cost, both for developing and implementing robust security measures and for the integration of complex systems.

5.3 Comparisons with existing literature

5.3.1 Alignment with existing studies

The research findings from this research study considerably align with existing literature in relation to the roles of interoperability and cybersecurity in remote patient monitoring medical devices (RPMs) for chronic disease management. The literature review indicated that standards like HL7 FHIR are crucial for seamless patient data exchange, and regulations like HIPAA and GDPR require data protection. The data collected from interviews effectively supported these points, participants frequently mentioned GDPR and HIPAA as primary drivers for data security and privacy requirements. Cybersecurity threats such as unauthorised access and data breaches were indicated as serious risks to RPMs in both the literature and interviews. Similarly, challenges associated with integrating legacy systems and the lack of standardised communication protocols were highlighted as major barriers to interoperability in both the literature and interview findings. The patient benefits,

including improved outcomes and early detection and intervention, identified in the literature review were consistently stressed by interview participants. Furthermore, the importance of "security by design" was a repeated theme in both sources. This strong alignment confirms that the key enablers, drivers and barriers identified through the qualitative interviews are consistent with the current understanding presented in research literature, validating the research's objectives.

5.3.2 New insights gained from this research

The new insights gained from this research are primarily through the qualitative interview data, which provided deeper insights and real-world perspectives. The experiences and knowledge of the participants who are experts in the medical device industry and healthcare professionals offered sophisticated viewpoints not always obvious in the literature. Participants shared practical experience on the challenges associated with integrating legacy systems, describing issues with outdated technology, custom protocols, and lack of documentation. They also explained the real-world experience of various cybersecurity threats encountered in different healthcare settings. The impact of the cost associated with implementing robust security measures and integrating complex systems is a significant insight, as is their consideration of this cost in relation to patient safety and benefits. The interview discussions also highlighted the importance of user experience, modes of training, and building trust with healthcare professionals and patients as critical factors for successful RPMDs adoption and effective use, going beyond technical considerations. Other considerations, such as anonymising patient data or providing multiple connectivity options based on device risk class, were also identified from the qualitative data, as practical considerations for device design and deployment.

5.4 Recommendations to improve interoperability and cybersecurity in RPMDs

The following are the recommendations based on the research findings that could improve interoperability and cybersecurity in Remote Patient Monitoring Medical Devices (RPMDs).

- The system resilience can be improved by considering the security requirements at the early stage of the development process, focusing on "security by design". Also, to establish an effective requirements management framework ensuring end-to-end traceability. Also, adoption of security practices throughout the device life cycle phases.

- Implementing a scalable security architecture framework that can be adopted for different devices based on their intended use and risk class. This consideration yields improved time to market and cost burden.
- The interoperability effectiveness can be improved with a collaborative working group comprising industry experts to implement standardised communication protocols across the key medical devices used in healthcare settings for seamless data exchange utilising the standards such as HL7 FHIR and DICOM and to integrate Electronic Health Records (EHRs).
- The implementation of an open and scalable interoperability architecture platform layer that could transform the data from different systems that can be utilised by systems such as the electronic health records (EHR) would result in improved interoperability controls.

These comprehensive steps can significantly enhance the effectiveness, safety, and application of RPMDs for chronic disease management.

5.5 Limitations of the study

5.5.1 Methodological limitations

This research was limited by the information available at the time of the study design based on the knowledge of industry experts working in medical device development and manufacturing and healthcare professionals working in the public healthcare system on remote patient monitoring medical devices. Therefore, the researcher chose to select participants who are working on the pre-market assessment and approval, design and development, manufacture and post-market surveillance & management product life cycle phases to gain insights and to support the design of further studies. These participants work as manufacturing/operations specialists, cybersecurity professionals, program/project managers, regulatory affairs professionals, systems engineering professionals, software engineering professionals, medical affairs professionals, global marketing professionals, software engineering professionals, quality systems engineering professionals, and healthcare professionals.

The researcher, based on the timeline available for this study, opted to interview eleven participants, resulting in a small sample size. However, the data collected provided sufficient insights to frame the design for further research on this topic.

The research was intentionally designed to recruit at least seven participants who had more than 10 years of experience in medical device design and development. The remaining three participants had less than 10 years of experience in the role and were deemed as eligible for the interviews. The participants had extensive experience in the medical device industry and other regulated industries, predominantly working on different classes of medical devices sold in the US and the EU. However, the research does not recruit participants from a bio-medical group and academic community due to the timeframe available to explore and find a suitable person with relevant experience.

The duration of the interviews in certain instances extended up to 45 minutes. That was because of the engagement of participants and their willingness to share more experience and insights in relation to the interview topics and questions. This certainly provided an opportunity to collect more practical experiences and insights that helped in primary data analysis.

5.5.2 Impact of limitations on findings

The participants were selected from different departments initially to gather comprehensive input from professionals working on medical devices in different departments, so it was difficult to formulate cohorts and derive comparisons between the cohorts. However, more participants need to be chosen for further studies from various departments due to the nature and complexity associated with remote patient monitoring medical devices.

5.5.3 Suggestions for future research

Further research can be designed by focusing on risk and intended use of the device targeting a simple class I device and up to class III devices to understand the considerations and challenges to incorporate security by design and interoperability at early stages of device development. Also, to assess the considerations and challenges to develop scalable security framework and scalable open architecture for effective interoperability of remote patient monitoring medical devices.

Further research can be designed by focusing on participants based on their roles, by recruiting participants who work in a specific department from various organisations to provide opportunities to gather deeper insights in assessing the practices followed across the different medical device manufacturers. This study also provides opportunities to assess considerations and challenges in developing unified security framework and a unified open architecture for interoperability suitable for different levels of interoperability.

5.6 Conclusion

The research is aimed to evaluate the roles of interoperability and cybersecurity in remote patient monitoring medical devices (RPMDs) used for managing chronic diseases conditions. Findings confirmed the need for effective interoperability controls are essential for seamless data exchange between medical devices, electronic health records (EHRs), and other healthcare systems. However, there are significant interoperability challenges identified including integration of legacy systems and a lack of standardised communication protocols. Similarly, cybersecurity measures are critical to protect patient data and in improving system security from threats and vulnerabilities. Regulations such as GDPR in the EU and HIPAA in the US are significant drivers for implementing data protection requirements. The research highlighted the challenges associated with implementation of standards across different technologies and systems. Overall, the study validated many points from existing literature while providing practical, real-world insights from industry experts. The insights gained highlight that successful deployment of RPMDs significantly benefits patients by enabling improved health outcomes, early detection of issues, and reduced hospitalisations. However, the realisation of these benefits is dependent on developing and implementing systems that are both highly interoperable and cyber-resilient.

Key considerations for improvement include incorporating "security by design" early in the development process and throughout the device lifecycle. Adopting standardised protocols and developing open, scalable architectures are important steps to overcome interoperability barriers with diverse systems. While there are challenges, such as the cost and complexity of implementing these measures, the primary objective is to protect patient safety and improve clinical decision-making drives the need for continuous advancements in both areas. Finally, enhancing interoperability and cybersecurity in RPMDs is fundamental to fostering advanced healthcare practices and improving patient care for chronic disease management in the modern-age digital healthcare system.

Chapter 6. References

- Amaral, C. *et al.* (2024) (20) 'Global Regulatory Challenges for Medical Devices: Impact on Innovation and Market Access'. *Applied Sciences*, 14(20), p. 9304. DOI: 10.3390/app14209304.
- Baltaxe, E. *et al.* (2023) 'The Assessment of Medical Device Software Supporting Health Care Services for Chronic Patients in a Tertiary Hospital: Overarching Study'. *Journal of Medical Internet Research*, 25(1), p. e40976. DOI: 10.2196/40976.
- Blessing, A., Henry, Z. and Micheal, D. (2024) 'Data Collection and Analysis Techniques'.
- Canali, S., Schiaffonati, V. and Aliverti, A. (2022) 'Challenges and Recommendations for Wearable Devices in Digital Health: Data Quality, Interoperability, Health Equity, Fairness'. *PLOS Digital Health*, 1(10), p. e0000104. DOI: 10.1371/journal.pdig.0000104.
- Carroll, N. and Richardson, I. (2016) 'Software-as-a-Medical Device: Demystifying Connected Health Regulations'. *Journal of Systems and Information Technology*, 18, pp. 186–215. DOI: 10.1108/JSIT-07-2015-0061.
- Center for Devices and Radiological FDA [Online]. (2024) 'Medical Device Interoperability'. FDA. Available at: <https://www.fda.gov/medical-devices/digital-health-center-excellence/medical-device-interoperability> (Accessed: 3 November 2024).
- Code of Federal Regulations [Online]. (2025) 21 CFR 820.30 -- Design Controls. Available at: <https://www.ecfr.gov/current/title-21/part-820/section-820.30> (Accessed: 13 May 2025).
- De Guzman, K.R. *et al.* (2022) 'Economic Evaluations of Remote Patient Monitoring for Chronic Disease: A Systematic Review'. *Value in Health*, 25(6), pp. 897–913. DOI: 10.1016/j.jval.2021.12.001.
- EUR-Lex [Online]. (2017) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, Amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA Relevance.). Available at: <http://data.europa.eu/eli/reg/2017/745/oj/eng> (Accessed: 24 April 2024).
- Feinstein, M. *et al.* (2024) 'REMOTE MONITORING AND ARTIFICIAL INTELLIGENCE: OUTLOOK FOR 2050'. *Anesthesia and Analgesia*, 138(2), pp. 350–357. DOI: 10.1213/ANE.0000000000006712.
- Fernandez, F. and Pallis, G. (2014) 'Opportunities and Challenges of the Internet of Things for Healthcare'. In *Proceedings of the 4th International Conference on Wireless Mobile Communication and Healthcare - 'Transforming Healthcare through Innovations in Mobile and Wireless Technologies'*. 4th International Conference on Wireless Mobile Communication and Healthcare - 'Transforming healthcare through innovations in mobile and wireless technologies'. Athens, Greece: ICST. DOI: 10.4108/icst.mobihealth.2014.257276.
- Hassanally, P. and Dufour, J.C. (2021) 'Analysis of the Regulatory, Legal, and Medical Conditions for the Prescription of Mobile Health Applications in the United States, The European Union, and France'. *Medical Devices: Evidence and Research*, 14, pp. 389–409. DOI: 10.2147/MDER.S328996.
- Hurst, A. (2023) 'Chapter 10. Introduction to Data Collection Techniques'. Available at: <https://open.oregonstate.edu/qualresearchmethods/chapter/chapter-10-introduction-to-data-collection-techniques/> (Accessed: 9 April 2025).
- Jaatun, M.G. *et al.* (2024) 'NEMECYS: Addressing Challenges to Building Security Into Connected Medical Devices'. *Procedia Computer Science*, 239, pp. 1361–1368. DOI: 10.1016/j.procs.2024.06.307.

- Jendle, J. *et al.* (2023) 'A Narrative Commentary about Interoperability in Medical Devices and Data Used in Diabetes Therapy from an Academic EU/UK/US Perspective'. *Diabetologia*, 67(2), p. 236. DOI: 10.1007/s00125-023-06049-5.
- K, M. *et al.* (2024) 'Medical Data Integration and Interoperability through Remote Monitoring of Healthcare Devices'. 15, pp. 60–72. DOI: 10.58346/JOWUA.2024.12.005.
- Khater, H.M. *et al.* (2024) 'Empowering Healthcare With Cyber-Physical System—A Systematic Literature Review'. *IEEE Access*, 12, pp. 83952–83993. DOI: 10.1109/ACCESS.2024.3407376.
- Lehne, M. *et al.* (2019) 'Why Digital Medicine Depends on Interoperability'. *Npj Digital Medicine*, 2(1), pp. 1–5. DOI: 10.1038/s41746-019-0158-1.
- Leo, D.G. *et al.* (2022) 'Interactive Remote Patient Monitoring Devices for Managing Chronic Health Conditions: Systematic Review and Meta-Analysis'. *Journal of Medical Internet Research*, 24(11), p. e35508. DOI: 10.2196/35508.
- Machal, M. (2023) 'An Overview About Connected Medical Devices and Their Risks'. *Studies in Health Technology and Informatics*, 305, pp. 119–122. DOI: 10.3233/SHTI230438.
- Margam, R. (2023) 'CONNECTING HEALTHCARE ECOSYSTEMS: THE JOURNEY OF INTEROPERABILITY'. DOI: 10.17605/OSF.IO/PG6C9.
- Pashkov, V., Gutorova, N. and Harkusha, A. (2016) 'Medical Device Software: Defining Key Terms'. *Wiadomosci Lekarskie (Warsaw, Poland : 1960)*, 69, pp. 813–817.
- Peyroteo, M. *et al.* (2021) 'Remote Monitoring Systems for Patients With Chronic Diseases in Primary Health Care: Systematic Review'. *JMIR mHealth and uHealth*, 9(12), p. e28285. DOI: 10.2196/28285.
- Ramirez, M.V.U. (2024) *Advancements in Connected Medical Devices: Assessing Innovations in Remote Monitoring and Diagnosis*. Available at: <https://primerascientific.com/journals/psmph/PSMPH-05-155> (Accessed: 26 February 2025).
- Robkin, M. (2015) 'Levels of Conceptual Interoperability Model for Healthcare: Framework for Safe Medical Device Interoperability'. *Levels of Conceptual Interoperability Model for Healthcare Framework for Safe Medical Device Interoperability*. Available at: https://www.academia.edu/37837939/Levels_of_Conceptual_Interoperability_Model_for_Healthcare_Framework_for_Safe_Medical_Device_Interoperability (Accessed: 26 February 2025).
- Saripalle, R., Runyan, C. and Russell, M. (2019) 'Using HL7 FHIR to Achieve Interoperability in Patient Health Record'. *Journal of Biomedical Informatics*, 94, p. 103188. DOI: 10.1016/j.jbi.2019.103188.
- Saunders, M.N. *et al.* (2023) *Research Methods for Business Students*. 9th Edition. PEARSON EDUCATION LIMITED Available at: https://www.researchgate.net/publication/240218229_Research_Methods_for_Business_Students (Accessed: 8 April 2025).
- Shah, N. (2025) 'Securing Life-Saving Devices Challenges and Solutions in Medical Device Cybersecurity'.
- Siemens-healthineers [Online] (2024) *Cybersecurity*. Available at: <https://www.siemens-healthineers.com/en-uk/support-documentation/cybersecurity> (Accessed: 11 August 2024).
- Singh, J. (2024) 'Challenges with Medical Devices Connected To Hospital Network'. *International Journal for Research in Applied Science and Engineering Technology*, 12, pp. 735–749. DOI: 10.22214/ijraset.2024.63187.
- Sobahi, N. and Bamabad, A. (2024) 'Cyber-Attacks Risk Analysis of a Connected Pulse Oximeter Device: A Threat Modeling Using STRIDE and DREAD Models'. *International Journal for Scientific Research*, 3, pp. 280–315. DOI: 10.59992/IJSR.2024.v3n5p10.

Tagne, J.F. *et al.* (2025) 'Challenges for Remote Patient Monitoring Programs in Rural and Regional Areas: A Qualitative Study'. *BMC Health Services Research*, 25, p. 374. DOI: 10.1186/s12913-025-12427-z.

Tetty-Engmann, Ph.D., F. and Parupelli, S.K. (2023) 'A Review of Biomedical Devices: Classification, Regulatory Guidelines, Human Factors, Software as a Medical Device, and Cybersecurity'. *Biomedical Materials & Devices*. DOI: 10.1007/s44174-023-00113-9.

Tian, J. *et al.* (2021) 'Regulatory Perspectives of Combination Products'. *Bioactive Materials*, 10, pp. 492–503. DOI: 10.1016/j.bioactmat.2021.09.002.

U.S. Food & Drug Administration (FDA) [Online]. (2023a) *Classify Your Medical Device*. FDA. Available at: <https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device> (Accessed: 18 May 2025).

U.S. Food & Drug Administration (FDA) [Online]. (2023b) 'Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions'.

U.S. Food & Drug Administration (FDA) [Online]. (2022) 'What Are Examples of Software as a Medical Device?' FDA. Available at: <https://www.fda.gov/medical-devices/software-medical-device-samd/what-are-examples-software-medical-device> (Accessed: 9 October 2024).

U.S. Food & Drug Administration (FDA) [Online]. (2020) 'What Is Digital Health?' FDA. Available at: <https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health> (Accessed: 3 November 2024).

Vaidya, S. (2024) 'Enhancing Cybersecurity in Healthcare IoT Ecosystems: A Comprehensive Framework for Securing Medical Data and Devices'. *Educational Administration Theory and Practices*, 30. DOI: 10.53555/kuey.v30i6(S).5371.

Walker, R.C. *et al.* (2019) 'Patient Expectations and Experiences of Remote Monitoring for Chronic Diseases: Systematic Review and Thematic Synthesis of Qualitative Studies'. *International Journal of Medical Informatics*, 124, pp. 78–85. DOI: 10.1016/j.ijmedinf.2019.01.013.

Wang, Y.C. *et al.* (2018) 'WHY INTEROPERABILITY IS ESSENTIAL IN HEALTH CARE'. In *Procuring Interoperability: Achieving High-Quality, Connected, and Person-Centered Care*. National Academies Press (US). Available at: <https://www.ncbi.nlm.nih.gov/books/NBK594855/> (Accessed: 26 February 2025).

Appendix A: Interview Questions

1. Remote patient monitoring (RPM) medical devices:

- 1.1. Do you work on medical devices including software?
- 1.2. Is the device used to monitor patient conditions remotely?
- 1.3. Is the device used to connect to a mobile device/computer and/or hospital network?
- 1.4. Is the device used to exchange data to/from the patient and healthcare professionals (HCPs)?

2. Cybersecurity — Data Privacy and Security:

- 2.1. What are the primary cybersecurity threats and vulnerabilities in RPM devices, and how do they potentially compromise patient data integrity?
- 2.2. How do current data standards influence the ability to make clinical decisions through data exchange (interoperability) from RPM devices for HCPs involved in chronic disease management?
- 2.3. What are the approaches that could strengthen the resilience of RPM devices against evolving cyber threats, without impacting clinical functionality?
- 2.4. How does the cost of incorporating high data security measures relate to the patient benefits? Please elaborate on patient benefits.

3. Interoperability — Data Exchange:

- 3.1. What are the primary challenges in integrating systems (including legacy) from different manufacturers with RPM devices to facilitate seamless data exchange?
- 3.2. How do interoperability standards (e.g., HL7 FHIR, DICOM) impact the ability to exchange data (accuracy & timeliness) between RPM devices and other systems such as electronic health records (EHRs) and patient data management systems (PDMS) in chronic disease management?
- 3.3. How does the real-time data availability and system resilience (cybersecurity) play in chronic disease management?
- 3.4. How does the cost of incorporating an effective infrastructure for data exchange relate to the patient benefits? Please elaborate on patient benefits.

4. Regulations and standards:

- 4.1. What are the primary challenges to ensuring RPM devices comply with data protection regulations, like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), in chronic disease management?
- 4.2. How do different global regulatory requirements affect the development and operation of RPM devices interoperability in chronic disease management?

- 4.3. What strategies can be adopted to adhere to global cybersecurity and interoperability standards?
- 4.4. How does the cost of incorporating regulations relate to the patients benefits?
Please elaborate on patient benefits.

5. Usability/Applications:

- 5.1. What are the most significant challenges in using RPM devices in chronic disease management?
- 5.2. What are the benefits HCPs realise from RPM devices in terms of monitoring, managing, making informed clinical decisions, and improving patient outcomes for chronic disease?
- 5.3. What are the considerations that could encourage and increase trust in HCPs to use RPM devices for effective data exchange and mitigate cybersecurity risks?
- 5.4. What specific training and support do HCPs need to operate RPM devices effectively with confidence?

Appendix B: Participant Information Letter



Participant Information Letter

TITLE OF THE STUDY:

Evaluating the roles of interoperability and cybersecurity in remote patient monitoring medical device of chronic disease management

I would like to invite you to take part in a research study. Before you decide you need to understand why the research is being done and what it would involve for you. Please take time to read the following information carefully. Ask questions if anything you read is not clear or if you would like more information. Take time to decide whether or not to take part.

WHO I AM AND WHAT THIS STUDY IS ABOUT

My name is Chaitanya Potharaju, I am a student at Griffith College Dublin, where I'm undertaking a master's in Medical Device Technology and Business. This research forms part of the final dissertation module which leads to a level 9 MSc qualification. The dissertation focuses on assessing the roles of the interoperability and cybersecurity in remote patient monitoring medical device influencing in making informed clinical decisions in chronic disease management. The purpose of the study is to gather deeper insights from healthcare professionals and stakeholders involved in the development, use, and maintenance of remote patient monitoring medical devices to assesses the drivers, enablers, and barriers related to interoperability and cybersecurity, and considerations influencing the patient outcomes and efficacy.

WHAT WOULD TAKING PART INVOLVE?

The participant will be requested to join in a one-on-one interview with the researcher, Chaitanya Potharaju. The interview duration will be about 30 mins but will not exceed more than 40 minutes. The type of interview can be in person, by telephone, or online using Teams or Zoom. The interview will be audio-recorded for the purpose of taking notes and for

transcription. The information gathered will be coded and used anonymously in the analysis and dissertation writing.

We will ask each participant to respond to a series of 10 to 15 questions. These questions will be independent of any specific personal or patient experience with device use. The aim of the interview is to explore the knowledge and experience of healthcare professionals and stakeholders who have experience in at least one of the areas of remote patient monitoring devices development, usage and maintenance.

WHY HAVE YOU BEEN INVITED TO TAKE PART?

As a participant, you are meeting the criteria for taking part in the research and have been invited to participate in this interview based on your knowledge and expertise in the remote patient monitoring medical device. The criteria include either you work or have worked on the remote patient monitoring medical devices for at least a minimum period of three years.

DO YOU HAVE TO TAKE PART?

Participation is voluntary. You have the right to refuse participation, and to refuse to answer any question without any consequence whatsoever. This consent may be withdrawn at any time in the process up to two weeks after the interview has been undertaken. If you need to withdraw you can contact myself at chaitanya.potharaju@student.griffith.ie or +353892000548.

WHAT ARE THE POSSIBLE RISKS AND BENEFITS OF TAKING PART?

The possible benefits of this research include understanding and assessing the factors influencing the interoperability and cybersecurity of remote patient monitoring medical devices in chronic disease management.

The information will assist in assessing the considerations for seamless data exchange between remote patient monitoring medical devices and other systems used within the network, without compromising the data integrity and privacy, and mitigating cybersecurity vulnerabilities that might improve the patient outcomes and efficacy.

There is no risk of a loss of your confidentiality and no risk of harm to the participant. The aim of the research is to gather information based on the participant's knowledge and expertise in remote patient monitoring medical devices for chronic disease management.

WILL TAKING PART BE CONFIDENTIAL?

The non-anonymised participant's data in the form of signed consent form is collected. Audio recordings are anonymised, these are collected and retained as part of the research

process. Data analysis is coded and therefore confidentiality is provided in the data analysis and discussion.

HOW WILL INFORMATION YOU PROVIDE BE STORED AND PROTECTED?

Signed consent forms and original audio recordings will be retained in a password protected laptop stored in a cabinet, whose sole use is by the researcher. It will be stored for 2 years after the dissertation is submitted, expected date of submission is May 2025. If the research is published data will be stored for 4-7 years. Under freedom of information legislation, you are entitled to access the information you have provided at any time.

WHAT WILL HAPPEN TO THE RESULTS OF THE STUDY?

All dissertation research projects, and their content will be made accessible in the college library and could potentially be made available in online e-journals or repository.

WHO SHOULD YOU CONTACT FOR FURTHER INFORMATION?

Chaitanya Potharaju, Student Griffith College Dublin.

chaitanya.potharaju@student.griffith.ie or +353892000548

THANK YOU

Appendix C: Informed Consent Form



GRIFFITH COLLEGE DUBLIN

Consent to take part in research

TITLE OF THE STUDY:

Evaluating the roles of interoperability and cybersecurity in remote patient monitoring
medical device of chronic disease management

- I [*insert participant name*] voluntarily agree to participate in this research study
- I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer any question without any consequences of any kind
- I understand that I can withdraw permission to use data from my interview within two weeks after the interview, in which case the material will be deleted.
- I have had the purpose and nature of the study explained to me in writing and I have had the opportunity to ask questions about the study
- I understand that participation involves 20 to 40 minutes one-on-one interview to respond to a series of questions.
- I understand that I will not benefit directly from participating in this research
- I understand that all information I provide for this study will be treated confidentially
- I understand that in any report on the results of this research my identity will remain anonymous. This will be done by changing my name and disguising any details of my interview which may reveal my identity or the identity of people I speak about.
- I agree to my interview being audio-recorded.
- I understand that disguised extracts from my interview may be quoted in the dissertation, and if published in conference presentations, published papers, ejournals, or in Griffith College Dublin library.
- I understand that I will adhere to all of the codes of conduct and employee confidentiality for company XXX and there is no expectation to breach these by partaking in this research.

- I understand that if I inform the researcher that myself or someone else is at risk of harm, they may have to report this to the relevant authorities - they will discuss this with me first but may be required to report with or without my permission
- I understand that signed consent forms and original audio recordings will be retained on the researcher's password protected laptop until May 2027 or if published up to May 2032.
- I understand that a transcript of my interview in which all identifying information has been removed will be retained for up to two years.
- I understand that under freedom of information legislation I am entitled to access the information I have provided at any time while it is in storage as specified above.
- I understand that I am free to contact any of the people involved in the research to seek further clarification and information.

Researcher Details

Name: Chaitanya Potharaju

Degree Programme: MSc Medical Device Technology and Business

College Details: Griffith College Dublin

Contact number: +353892000548

Contact mail: chaitanya.potharaju@student.griffith.ie

Signature of participant

[Full Name – Printed]

Signature of research participant

----- Date

Signature of researcher

I believe the participant is giving informed consent to participate in this study

----- Date

Signature of researcher

Appendix D: Ethics Application



Ethics Application & Declaration Form

DISSERTATION TITLE: Evaluating the roles of interoperability and cybersecurity in remote patient monitoring medical device of chronic disease management

RESEARCHER'S NAME: Chaitanya Potharaju

PROGRAMME OF STUDY: MSc. Medical Device Technology and Business

SUPERVISOR'S NAME: Brian Kearney

DECLARATION:

The information in this application form is accurate to the best of my knowledge. I undertake to abide by the principles outlined by Innopharma/Griffith College ethics policy in my research dissertation. I confirm that I have completed a full ethics assessment for my research dissertation as per the college guidelines. I will not begin my primary research until such approval from my supervisor and/or ethics Committee has been obtained.

I pledge to carry out my research according to the Innopharma/Griffith College academic integrity standards. Any results presented in my dissertation will be from my own, original research, I will reference and/or acknowledge any material or sources used in its preparation and I will not plagiarise the work of anyone else.

For Student:

STUDENT SIGNATURE:

DATE:

The research contained within this research dissertation proposal has been approved.

For Supervisor:

Ethics Committee Approval Required:

Yes

No

SUPERVISOR SIGNATURE:

DATE:

For Ethics Committee (if required):

Ethics Committee Approval Given:

Yes

No

ETHICS COMMITTEE MEMBER SIGNATURE:

DATE:

NOTE: Supervisors are responsible for ensuring their students fill in this form correctly and that all ethical areas have been considered.

SECTION 1: DESCRIPTION OF RESEARCH STUDY

1.1 Purpose and objectives of research:

This research aims to explore the critical roles of interoperability and cybersecurity incorporated in digital healthcare systems facilitating remote patient monitoring for chronic disease management. The primary objective is to gather in-depth insights from healthcare professionals and various stakeholders involved in the development, utilization, and maintenance of digital healthcare systems. Further steps include analyses and assessment of the drivers, enablers, and barriers relevant to interoperability and cybersecurity meeting patients and users expectations including patient safety, self-management, improved healthcare services access and efficient data exchange (Walker et al., 2019; Machal, 2023). The key emphasis is to understand the effective interoperability criteria to achieve successful data exchange across the devices within the digital healthcare system. Similarly, to understand cybersecurity measures for protecting patient data and integrity.

The research summarizes the factors influencing the interoperability and cybersecurity on digital healthcare systems for chronic disease management. Furthermore, this study will identify potential considerations that could improve integration and data security of the different digital healthcare components, fostering healthcare practices, patient care and outcomes in chronic disease management.

Objective #1: Identify the current standards available for interoperability and cybersecurity in remote monitoring medical devices.

Objective #2: Assess drivers, enablers, and barriers relevant to interoperability in remote monitoring medical devices.

Objective #3: Assess drivers, enablers, and barriers relevant to cybersecurity in remote monitoring medical devices.

Objective #4: Assess the current state of interoperability and cybersecurity frameworks in remote monitoring medical devices.

Objective #5: Identify the potential considerations that could improve integration and data security of the different digital healthcare components.

1.2 Research methodology:

A qualitative exploration of information through interviewing experienced healthcare professionals, and stakeholders specialised in different roles such as healthcare professionals, research and development engineers, regulatory affairs specialists, and cybersecurity involved in development, usage and maintenance of digital healthcare systems facilitating in remote monitoring and managing patients with chronic disease conditions. The interviews focus on gathering knowledge and experience on interoperability and cybersecurity of digital healthcare systems used to remotely monitor and manage patients with chronic disease conditions. Assess the information gathered through the interviews to evaluate the drivers, enablers, and barriers related to interoperability and cybersecurity in digital healthcare systems that influence the patient outcomes and efficacy.

SECTION 2: POSSIBLE ETHICAL ISSUES

Answer 'yes' or 'no' to the following questions.

SUBJECT MATTER

Does the research proposal involve:

Research into specific company activities that would be deemed sensitive or confidential	Yes No
Research into politically and/or racially/ethnically and/or commercially sensitive areas	Yes No
Sensitive, personal, professional or corporate issues	Yes No

RESEARCH PROCEDURES

Does the research proposal involve:

Research that might damage the reputation of companies or participants	Yes No
Research that may negatively affect the reputation of Griffith College/Innopharma	Yes No
Use of personal records without consent	Yes No
Use of company data without consent	Yes No
The offer of any inducements to participate	Yes No
Audio or visual recording without consent	Yes No
Using a language other than English	Yes No

PARTICIPANTS

Does the research proposal involve:

People who are not competent and/or fluent in English	Yes No
---	-------------------

Does your research group include any of the following vulnerable groups

Yes No

If you have answered NO to ALL questions, please go straight to Section 4.

If you have answered YES to ANY question in SECTION 2, you must fill in SECTION 3.

SECTION 3: STEPS TAKEN TO AVOID ETHICAL ISSUES

3.1. If your ethics relates to **Subject Matter**, outline your action plan to work around any sensitive issues.

3.2. If your ethics relates to **Research Procedures**, outline your action plan to deal with possible ethical issues in your research procedures.

3.3. If your ethics relates to **Participants**, outline how you will protect vulnerable persons or those that do not have English as their first language.

SECTION 4: ABOUT YOUR PARTICIPANTS

4.1. Outline your participant profile and why you have chosen them for this study.

The selected cohort for this study comprises

- A qualified physician leading medical affairs team with 10 plus years of experience
- A qualified research and development (R&D) systems engineer with 10 plus years of experience
- A qualified R&D software engineer involved in connected medical device development with 10 plus years of experience in healthcare or other regulated industry
- A qualified R&D software engineer involved in medical device development with 5 plus years of experience
- A qualified marketing professional with 10 plus years of experience
- A qualified cybersecurity professional with 10 plus years of experience
- A qualified regulatory affair specialist with 5 plus years of experience
- A qualified manufacturing/operations specialist with 5 plus years of experience
- A qualified program/project manager with 10 plus experience
- A qualified quality systems engineering professional with 5 plus years of experience.
- A qualified healthcare professional with 5 plus years of experience

The profiles chosen to have extensive experience in at least one of the life cycle phases of remote patient monitoring devices or similar devices development, usage and maintenance that aid in gathering the valuable insight to assess considerations associated with interoperability and cybersecurity that influence the patient outcomes and efficacy.

4.2 How do you plan to gain access to/contact/approach your participant(s).

The plan is to contact participants by email or professional networking platforms with whom I collaborated at previous organisations, educational institutions, and professional networks, specifically those involved in remote patient monitoring medical devices or similar technologies.

SECTION 5: INFORMATION, CONSENT AND CONFIDENTIALITY

5.1 Participant Information Letter (PIL) for participants

Please confirm below that your information letter covers:

Description of the research topic and method	Yes No
Details of what participation will involve	Yes No
Rights to anonymity	Yes No
Confidentiality	Yes No
Rights to withdraw from the research	Yes No
The contact details of the researcher and supervisor (if necessary)	Yes No

5.2 Informed Consent Form (ICF) for participants

Please indicate below if your research requires a signed consent form by selecting the relevant option only:

Yes: my research requires signed consent and I have attached an ICF in the appendices of my application.

~~**No:** my research study involves an online survey only and/or does not require signed consent~~

SECTION 6: STORAGE OF DATA

[Please ensure that you are abiding by GDPR and the national Data protection laws <https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/>].

*The student is responsible for storage of data and this will be handed over to the college in an electronic format as part of the thesis submission i.e. primary data and completed ICFs where applicable will be added to the primary data folder on moodle. The rationale is to keep data **as long as it is still useful** and there is an intention to use it further **for research** so if this is not the case then this can be stipulated here and a shorter retention period given.]*

6.1. How will you store the research data and for how long? How will you manage data protection issues?

Signed consent forms and original audio recordings will be retained in a password protected laptop stored in a cabinet, whose sole use is by the researcher. It will be stored for 2 years after the dissertation is submitted, expected date of submission is May 2025. If the research is published data will be stored for 4-7 years. Under freedom of information legislation, you are entitled to access the information you have provided at any time.

SECTION 7: NON-DISCLOSURE AGREEMENT & STUDENT CONSENT

7.1 Non-Disclosure Agreement (NDA)

Will the final dissertation contain any information pertaining to any source what would warrant the use of a Non-Disclosure Agreement (NDA) e.g. industry-based research?

~~Yes~~ No

7.2 Student consent

If a Non-Disclosure Agreement (NDA) is not required, does the Student consent to allow their completed dissertation to be held/published by Innopharma/Griffith College?

~~Yes~~ No

SECTION 8: RECORDING AND RETENTION OF DISSERTATION VIVA

8.1 Viva Recording

The Dissertation viva will be recorded. This recording may be used to facilitate assessment by Innopharma staff, a third reader if necessary and/or if requested by the external examiner for the Programme. The recording will be held in line with current GDPR guidelines and will not be made publicly available.

SECTION 9: DOCUMENT CHECKLIST

NOTE: Applicants must attach the following documents in electronic format to the appendix.

Which documents are added to the appendix? Please tick N/A if not applicable:

- | | |
|--|--------------------|
| 9.1 Participant Information Letter (PIL) for participant | Yes N/A |
| 9.2 Informed Consent Form (ICF) for participant | Yes N/A |
| 9.3 Questions/survey for interviewees/focus groups etc (<i>can be in draft form</i>) | Yes N/A |
| 9.4 Any other documents e.g. Non-Disclosure Agreement | Yes N/A |

I confirm that this application is complete and all required documents are included in the appendix.

For Student:

STUDENT SIGNATURE:

DATE:
