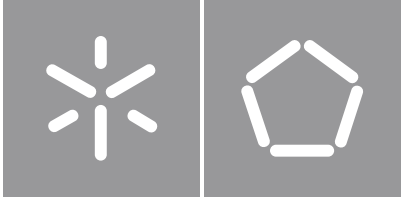
Universidade do Minho
Escola de Engenharia

João Adriano Teixeira Ferreira

Security in remote monitoring devices in critical areas

december 2020



Universidade do Minho
Escola de Engenharia

João Adriano Teixeira Ferreira

Security in remote monitoring devices in critical areas

Masters Dissertation
Integrated Master in Engineering and Management of Information Systems
Cybersecurity

Work done on the orientarion of the
Doctor Professor Henrique Manuel Dinis dos Santos,
Doctor Professor Carlos Filipe Portela

december 2020

Acknowledgements

In life, it is always important to be thankful to those who help us achieve our goals, so I want to perform some acknowledgments:

I want to thank Ph.D. Henrique Santos and Ph.D. Carlos Filipe Portela for accepting being my supervisors and helping me to perform this scientific research. Without them and their knowledge, this work could not be completed.

I want to thank my family for always believe me and always support my choices no matter what they were.

I want to thank the "Casa da Ostia" team for always be there as friends and colleagues in this journey. Without them, I could not be writing these words.

I want to thank my friends for all the help they give me these years. No names are needed because they know who they are.

Finally, I want to thank my work colleagues for all the support.

Abstract

The use of Information Technologies has grown exponentially over the past years affecting many critical sectors from the industrial to the financial, energy, and health sectors.

The ability to track and remotely monitor people and objects in real-time is one of the changes made possible by Information Technologies.

Although those Information Technologies innovations sprang several significant advantages for people and organizations, there are also some security and privacy concerns regarding the monitoring of people, objects, and processes in critical areas.

Every day new and more effective cyberattacks are discovered which steal sensitive information from their holders and affect people and organizations. Computational power is increasing and organizations are emerging whose main objective is to profit from the sale of the stolen information assets.

These attacks can impact critical areas, such as health and energy; they may even jeopardize the physical integrity of individuals.

In Healthcare, a Critical Area, the number of Remote Patient Monitoring Devices Systems is increasing, and the number of patients using them increases as well. At the same time, there have been identified new security vulnerabilities on high technological medical devices. People privacy is also being called into question.

Several privacy gaps have forced governments to take action with the main objective of safeguarding the privacy of their citizens, as was the case with the much-discussed General Data Protection Regulation of the European Union.

Standards and Frameworks play an important role in the improvement o security. In this scientific work, it was developed and validated a proposal of a sector-specific Security Framework that can be applied to Remote Patient Monitoring Devices Systems to improve their overall security. That framework is based on the best widely spread Security Standards and Frameworks. The Framework define 30 requirements divided into 5 assets. Each requirement has one or more functions, in a total of 4 available. It was also defined 8 implementation groups. To validate the Framework it was developed a Remote Patient Monitoring Device System Simulator composed by a Micro-controller NodeMCU with an ESP8266 Wi-Fi chip connected to a Heart Rate Analog Sensor, and an Interface. When applied to the Framework, the developed simulator obtained a score of 9 in 29 available requirements for that implementation group device. The selected research method used to guide this scientific research was the Design Science Research.

Keywords: Critical Areas, Devices, Framework, Healthcare, Patients, Remote Monitoring, Security, Privacy.

Resumo

A utilização das Tecnologias de Informação tem crescido exponencialmente ao longo dos últimos anos afetando vários setores críticos que vão desde a indústria, passando pelo setor financeiro, energético e até mesmo pela saúde. A capacidade de acompanhamento e monitorização remota de pessoas e objetos em tempo real é uma das mudanças potenciadas pelas Tecnologias de Informação.

Embora destas inovações ao nível das Tecnologias de Informação advenham um conjunto de vantagens significativas para pessoas e organizações, surgem também algumas preocupações ao nível da segurança e privacidade no que concerne à monitorização de pessoas, objetos e processos em áreas críticas.

Diariamente são identificados e descritos novos e mais eficazes ataques cibernéticos, a pessoas e organizações com o intuito de roubar informação sensível para os seus detentores. O poder computacional é crescente e insurgem-se organizações cujo principal objetivo é lucrar com a venda de ativos informacionais roubados. Estes ataques podem atingir áreas tão críticas, como o setor da saúde e energético, podendo mesmo colocar em causa a integridade física de pessoas.

Nos cuidados de saúde, uma área crítica, o número de Sistemas de Dispositivos de Monitorização Remota esta a crescer, bem como o número de pacientes que os usam. Ao mesmo tempo, têm sido identificadas novas vulnerabilidades de segurança em dispositivos médicos altamente tecnológicos. A privacidade das pessoas está também a ser comprometida.

É possível assistir-se a várias falhas ao nível da privacidade que obrigou os governos a tomar medidas com o principal objetivo de salvaguardar a privacidade dos seus cidadãos como foi o caso do tão falado Regulamento Geral de Proteção de Dados da União Europeia.

Standards e Frameworks desempenham um papel importante na melhoria da segurança. Neste trabalho de investigação foi desenvolvida e validada uma proposta de Framework de Segurança específica para o setor da Saúde e que pode ser aplicada em Sistemas de Dispositivos de Monitorização Remota com o objetivo de aumentar a sua segurança. Esta Framework é baseada nas melhores e mais usadas Frameworks e Standards. A Framework define 30 requisitos divididos em 5 ativos. Cada requisito tem uma ou mais funções, de um total de 4. Foi também definido 8 grupos de implementação. Para validar a Framework foi desenvolvido um Simulador composto por um micro controlador NodeMCU com um chip Wi-FI ESP8266 conectado a um Sensor Analógico de Frequência Cardíaca. Quando aplicado à Framework, o simulador obteve um score de 9 em 29 requisitos disponíveis para aquele grupo de implementação. A metodologia de investigação selecionada para guiar este projeto foi a *Design Science Research*.

Palavras-Chave: Áreas Críticas, Cuidados de Saúde, Dispositivos, Framework, Monitorização Remota, Pacientes, Privacidade, Segurança.

Index of Contents

Index of Figures

Index of Tables

Acronyms

CAP Composed Assurance Packages.

CEH Certified Ethical Hacker.

CHFI Computer Hacking Forensics Investigator.

CIA Confidentiality, Integrity and Availability.

CIS Center for Internet Security.

CMM Capability Maturity Model.

CSF Common Security Framework.

CUI Controlled Unclassified Information.

DDoS Distributed Denial of Service.

DS Design Science.

DSR Design Science Research.

EAL Evaluation Assurance Level.

ECSA EC-Council Certified Security Analyst.

ETR Evaluation Technical Report.

FIPPs Fair Information Practice Principles.

GDPR General Data Protection Regulation.

HIPAA Health Insurance Portability and Accountability Act.

HITECH Health Information Technology for Economic and Clinical Health.

HTTPS Hypertext Transfer Protocol Secure.

ICT Information and Communications Technology.

IEC International Electrotechnical Commission.

InfoSec Information Security.

IoT Internet of Things.

IS Information Systems.

ISM Information Security Manual.

ISMS Information Security Management System.

ISO International Organization for Standardization.

IT Information Technologies.

LPT License Penetration Tester.

NIST National Institute of Standards and Technology.

NZISM New Zealand Information Security Manual.

PII Personally Identifiable Information.

PP Protection Profile.

PSR Protective Security Requirements.

RPM Remote Patient Monitoring.

SFPs Security Functional Policies.

SFRs Security Functional Requirements.

SP special Publication.

SQL Structured Query Language.

SSC Systems Security Engineering.

SSL Secure Sockets Layer.

ST Security Target.

SWOT Strengths, Weakness, Opportunities and Threats.

TCP/IP Transmission Control Protocol / Internet Protocol.

TLS Transport Layer Security.

TOE Target of Evaluation.

TSF TOE Security Functionality.

TSFI TSF Interface.

US United States.

WAF Web Application Firewalls.

WHO World Health Organization.

Glossary

Availability Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and in the correct format.
Retrieved from: https://www.techopedia.com/dictionary.

Confidentiality Confidentiality, in the context of computer systems, allows authorized users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.
Retrieved from: https://www.techopedia.com/dictionary.

Information Security Information security is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions.
Retrieved from: https://www.techopedia.com/dictionary.

Information Technologies Information Technology is a business sector that deals with computing, including hardware, software, telecommunications and generally anything involved in the transmittal of information or the systems that facilitate communication.
Retrieved from: https://www.techopedia.com/dictionary.

Integrity Integrity, in the context of computer systems, refers to methods of ensuring that data is real, accurate and safeguarded from unauthorized user modification.
Retrieved from: https://www.techopedia.com/dictionary.

Internet of Things The internet of things (IoT) is a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it also may include other sensor technologies, wireless technologies or QR codes.
Retrieved from: https://www.techopedia.com/dictionary.

Telehealth Telehealth is the act or process of delivering health care, usually through information and education, through the use of communications technology such as the Internet, videoconferencing, streaming media, and terrestrial and wireless communication. It encompasses a broad technology set, as mentioned, to deliver virtual medical, health and education services. It also still applies to traditional clinical diagnosis and monitoring being done through distance technology.
Retrieved from: https://www.techopedia.com/dictionary.

Telemedicine Telemedicine refers to resources, strategies, methods and installations that help doctors or other medical professionals work remotely to consult, diagnose and treat patients. Through major advancements in technology such as wireless networking and cloud computing, efficiency of data storage, complexity of electronic medical records software, etc., telemedicine is becoming a much more feasible aspect of modern medicine.

Retrieved from: https://www.techopedia.com/dictionary.

Threat A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.

Retrieved from: https://www.techopedia.com/dictionary.

Vulnerabilities Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

Retrieved from: https://www.techopedia.com/dictionary.

1 Introduction

The main goal of this chapter is to detail the context and the motivation of this research project, the research question, main objectives and expected results of the investigation process. The structure of this document is presented at the end of this chapter.

1.1 Context and motivation

Nowadays concerns with Information Security and Personal Privacy are real and affect most organizations and individuals. A 2019 report by the Check Point Software Technologies (Check Point Software Technologies, 2019) points out threatening aspects related to security and privacy:

- 76% of organizations experienced a phishing attack in the past year;
- Over 20% of organizations are impacted by Cryptojacking Malware every week;
- 49% of organizations experienced a Distributed Denial of Service (DDoS) attack in the past year;
- "The United States and United Kingdom formally blamed Russia for the 2017 ransomware attack that caused billions of dollars in damages worldwide";
- 614 GB of data related to weapons, sensor and communication systems stolen from United States Navy contractor, allegedly by Chinese government hackers.

Another report, by Symantec (Symantec, 2018), also presents the following threatening aspects:

- 5.4 billion WannaCry attacks blocked;
- 46% increase in new ransomware variants;
- 600% increase in attacks against Internet of Things (IoT) devices;
- 13% overall increase in reported vulnerabilities;
- 29% increase in industrial control system related vulnerabilities.

According to Statista (Statista, 2019a), a Business Data Platform and, as shown in Figure 1, the number of data breaches in the United States between 2005 and 2018 is increasing, reaching its peak in 2018 with almost half a million records exposed.

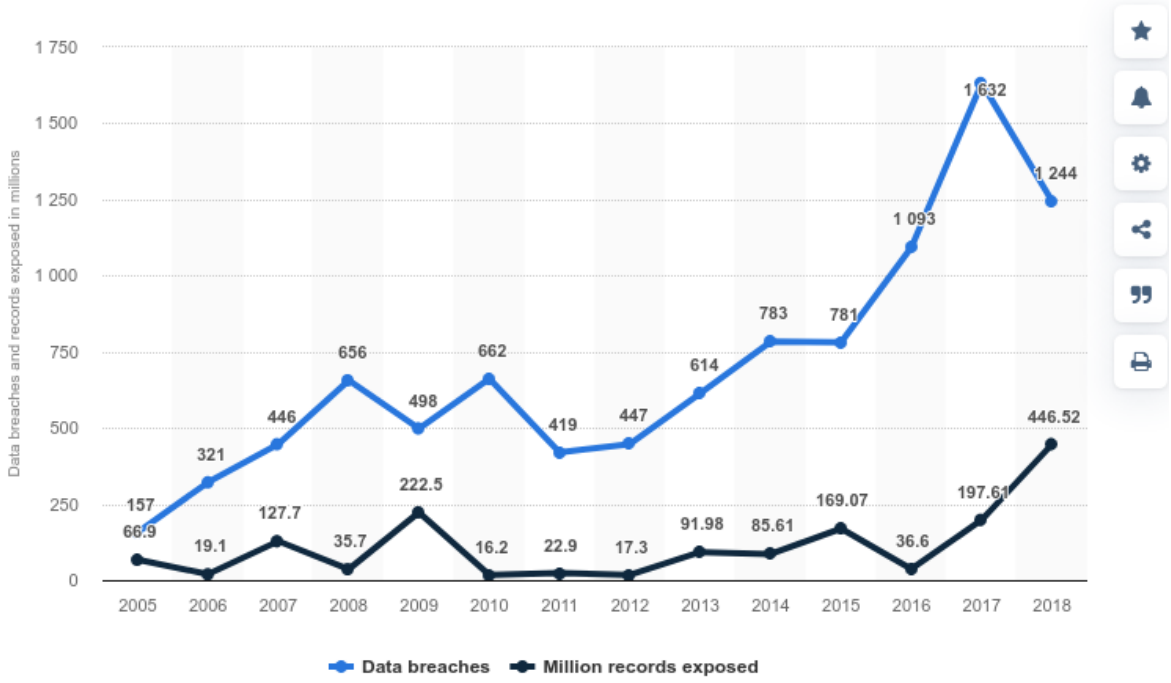


Figure 1: Annual number of data breaches and exposed records in the United States (US) from 2005 to 2018. Retrieved from (Statista, 2019a)

Several sectors are affected (Figure 2) from the Financial through Medical/Healthcare Sectors (Statista, 2019b).

With the advent of concepts like Industry 4.0, Big Data, Real-time decision-making, several industrial and services sectors are investing new technologies that enable them to remotely monitoring the processes and make decisions in real-time. The problem is then, that are security issues that affect organizations and individuals in several critical areas.

The cases of detected and exploited vulnerabilities are not a myth but a reality. The numbers of performed attacks and, consequently, the number of data breaches are increasing. The computational power is also increasing and accessible at increasingly lower prices, allowing hackers to perform better and more powerful attacks. Besides that, the severity of the data breaches and attacks in critical areas is huge.

Data breaches in sectors like the financial or healthcare sectors can endanger the privacy of customers, in industrial sectors can endanger fulfillment of their main goal. In the end, attacks in critical sectors can put people life in danger. Imagine a DDoS in the Energy System of a country capital that shuts down the

	Banking/Credit/Financial	Business	Educational	Government/Military	Medical/Healthcare
2013	35	194	54	60	271
2014	38	263	57	91	332
2016	51	497	97	72	373
2015	71	312	58	63	275
2017	134	907	128	79	384
2018	135	572	77	100	367

Showing entries 1 to 6 (6 entries in total)

Figure 2: Number of data breaches in the US from 2013 to 2018, by industry. Retrieved from (Statista, 2019b)

power supply of the city or a detected vulnerability in a pacemaker that could allow hackers to shut down the pacemaker remotely.

Due to all the presented facts, it can be considered that the scientific research regarding Information Security in Remote Monitoring Devices Systems is current and worthwhile. This scientific research focuses on Healthcare. This was the chosen critical area to be studied. So:

- How can healthcare professionals trust in the information provided from a Remote Patient Monitoring Device System?
- How can patients using a Remote Patient Monitoring Device System be sure that their privacy are ensured?

This research project intends to provide answers to the questions above. There is some personal motivation to answer these questions. Having worked for about five years as a General Nurse, I always wondered about the safety of such devices. As such a first attempt is made to study the security issues in healthcare Remote Patient Monitoring Devices Systems, which represents a critical area.

1.2 Objectives

The following research question was formulated:

"Could a sector-specific Security Framework improve the security of Remote Patient Monitoring Devices Systems?"

This research intends to be relevant in two specific fields. On the one hand, the scientific community that studies this field of knowledge (security in remote monitoring devices in critical areas) and, on the other hand, society itself.

The main objectives are the following:

- Propose a sector-specific Security Framework to apply on Remote Patient Monitoring Devices Systems;
- Validate the proposed sector-specific Security Framework.

As secondary objectives of this research the following were defined:

- Encourage researchers to pursue similar scientific researches and, in the process, identify solutions to the problems found;
- Inform manufacturers about the need of using sector-specific frameworks to improve the security of their products;
- Inform the healthcare society about the importance of measure security of Remote Patient Monitoring Devices Systems.

An expected result of this scientific project is the development and validation of a sector-specific Security Framework proposal that could be applied to Remote Patient Monitoring Devices Systems.

1.3 Document structure

This document is organized in chapters and has the following structure:

- **Chapter 1 - Introduction**: Describes the context and motivation of this research, the research question, the main and secondary objectives and, the expected results/aims of this research project;
- **Chapter 2 - Background**: Review of the main topics, such as, Information Security, Information Security Management, Standards and Regulations, Security Frameworks, Critical Areas, Critical Health and Legislation, Telemedicine and Telehealth, Remote Patient Monitoring, State-of-the-art and Security threats in Remote Patient Monitoring;
- **Chapter 3 - Method**: Describes the selected methodological approach, the Design Science Research, the used materials, and technologies;

- **Chapter 4 - Case Study**: Details all the activities that were performed to fulfill the expected results, that is, all the performed activities needed to develop and validate the proposed Security Framework. It is also detailed all the artifacts produced in this scientific research;
- **Chapter 5 - Conclusion**: Enunciates the major conclusions of this scientific work, and it is presented a critical overview about all the realized work. Presents also a Risk Analysis of this scientific research and the future work to be done;
- **Appendices**: Contains the most important appendices to this document, which are the Security Framework proposal Document and the Security Framework validation result.

2 Background

In this chapter, the theoretical review and the state-of-the-art of the main topics related to this research are presented. To Luna (Luna, 1999), the theoretical review circumscribes the research problem within a theoretical and conceptual framework that can explain it and, the state-of-the-art describe the current state of a particular area of study, namely what is known, the main shortcomings and, the main theoretical/methodological barriers.

The strategy used to write this background consisted of:

- Research of relevant information on books related to topics like Security, Information Security, Remote Monitoring, Healthcare, Telemedicine, Telehealth, etc;
- Research for scientific works about the same topics referred previously on scientific databases like Science Direct, IEEE Explore, B-On, etc;
- Online research of journal articles, thesis, masters dissertations, regulations and legislation, standards, etc, about the relevant topics for this work.

The main criteria used to choosing the bibliographic references was the number of citations, the impact factor of the publication (where available), the authors reputation, the number of editions, the year of edition. References with more than ten citations and less than five years were preferred.

2.1 Information Security

To Elmaghraby & Losavio (Elmaghraby & Losavio, 2014), emerging innovations in Information Technologies (IT) not only create new social and economic opportunities, but also pose new challenges to our security and, create new expectations about our privacy. Still, to Elmaghraby & Losavio (Elmaghraby & Losavio, 2014), humans are currently interconnected through smartphones and other electronic devices. Houses, cars, public spaces, and other social systems are converging to full connectivity.

It is easily understandable that the importance of Information Security (InfoSec) is becoming increasingly important, specially with regard to our personal information, our privacy.

According to Andress (Andress, 2014), InfoSec nowadays has a great presence in society, mainly because of the generalized adoption of IT. Although IT enables the increase of productivity and facilitates access to more and more information, its generalized use also brings security problems.

Andress (Andress, 2014) points out that about 30 years ago, InfoSec concerns associated with the use of IT were rare or nonexistent. This was due to the low level of technology implementation and the

small number of people using it.

Although the technologies change on an incredibly fast rate and every day new specific implementations of IT arise, the theories that address how we should maintain ourselves protected and secure change at a much slower rate, and not always keep up with the technological evolution (Andress, 2014).

"Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction" (Andress, 2014). This definition proposed by Andress in 2014 and based on United States Laws, points to a possible definition of InfoSec and, in its essence, emphasizes the need to protect data and the systems from those who want to misuse them.

For Rao & Nayak (Rao & Nayak, 2014), InfoSec is an extension of computer security and besides physical control, it worries with the logic control, storage media and, means of communication. InfoSec should be one of the most important goals of everyone (Rao & Nayak, 2014).

InfoSec is also a continuous process that involves people, policies and processes, and technology. These three categories can be considered the pillars of InfoSec (Rao & Nayak, 2014).

To Feruza & Tao-Hoon (Feruza & Tao-Hoon, 2007), Confidentiality, Integrity and Availability (CIA), have been the core principles of InfoSec. These core principles compose the CIA Triad (Figure 3).

According to Feruza & Tao-Hoon (Feruza & Tao-Hoon, 2007):

- Confidentiality: refers to the need to prevent the disclosure of information to unauthorized persons or systems;
- Integrity: refers to the fact that certain information cannot be modified without authorization;
- Availability: refers to the capacity of certain information to stay available when is needed.

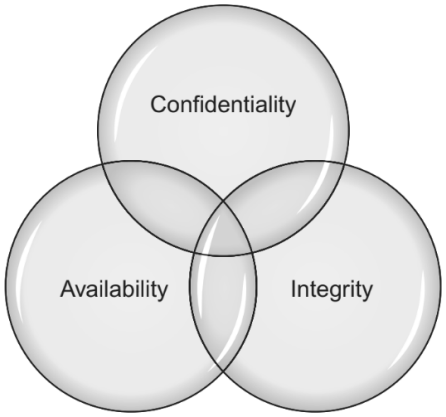


Figure 3: CIA Triad. Retrieved from (Andress, 2014)

2.1.1 Information Security Management

"The purpose of information protection is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization meet its business objectives or mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets" (Peltier et al., 2005).

Peltier et al., (Peltier et al., 2005) identifies eight major elements in which every information protection should be based, namely:

- Information protection should support the business objectives or mission of the enterprise;
- Information protection is an integral element of due care;
- Information protection must be cost-effective;
- Information protection responsibilities and accountabilities should be made explicit;
- System owners have information protection responsibilities outside their own organization;
- Information protection requires a comprehensive and integrated approach;
- Information protection should be periodically reassessed;
- Information protection is constrained by the culture of the organization.

To Ellof & Ellof (Eloff & Eloff, 2003), organizations must change to the "holistic management of information security, requiring a well-established Information Security Management System (ISMS)". This addresses all aspects in an organization that deals with creating and maintaining a secure information environment.

ISMS must address the implementation and maintenance of processes and procedures to manage Information Technology security, including identification of information security needs, implementation of strategies to meet these needs, the measurement of results, and improving both the protection strategies and the ISMS over time (Eloff & Eloff, 2003).

"The domain of Information Security Management is no longer exclusively of a managerial nature, technical aspects also need to be considered on management level" (Eloff & Eloff, 2003). There are several ways to approach Information Security Management. One is from a strategic perspective, addressing amongst others corporate governance, policies and pure management issues. Another, more human,

addresses issues such as security culture, awareness, training, ethics and other human related issues (Eloff & Eloff, 2003).

More importantly, "Information Security Management need to take a holistic approach, requiring a combination and integration of all the above mentioned ISMSs" (Eloff & Eloff, 2003). The holistic approach is illustrated in Figure 4.

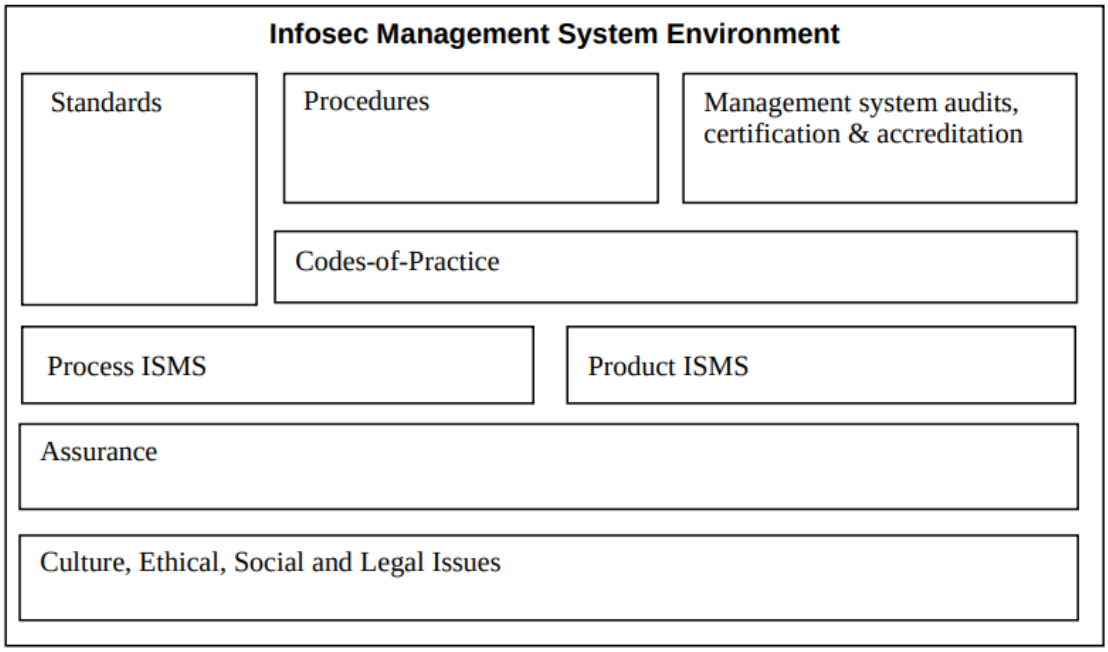


Figure 4: ISMS Holistic Approach. Retrieved from (Eloff & Eloff, 2003)

I) Policies and Procedures

To Peltier et al., (Peltier et al., 2005) "an information protection policy is the documentation of enterprisewide decisions on handling and protection information". To these authors, managers face challenging choices involving resource allocation, competing objectives, and organization strategy concerning the protection of technical and information resources.

It is very important to understand that information is an asset of the organization, and it is owned by the organization. Information reaches beyond the boundaries of IT and is present in all areas of the organization. An effective information protection policy must be part of the organization assets management program and must cross all organization (Peltier et al., 2005).

Every organization needs an information protection policy because the beginning of every information protection program is the implementation of such policy. The policy reflects the organization attitude toward information and how it will be protected against unauthorized access, modification, disclosure, and

destruction (Peltier et al., 2005).

"The cornerstone of effective information security architecture is a well-written policy statement" (Peltier et al., 2005). The policy is the basis for all the other organization directives such as standards, procedures, guidelines, and other supporting documents. (Peltier et al., 2005).

There are two important roles in policies. The internal role tells organization personnel what is expected of them and how their action will be judged, and the external role tells the world how the organization understands the protection of assets (Peltier et al., 2005).

II) Risk Management

"Risk is the possibility of something adverse happening" (Peltier et al., 2005). The identification of the risks, their occurrence likelihood, and the definition of the steps to reduce the risk to an acceptable level is the process of risk management (Peltier et al., 2005).

The primary function of information protection risk management is the identification of the appropriate controls for each identified risk. Controls also need to be aligned with the organization objectives and mission. The goal is to provide a safe and secure environment for management to meet its duty of care (Peltier et al., 2005).

Many factors have to be taken into consideration during the selection of the controls such as the organization information protection policy, legislation, and regulations that apply to the organization. Another aspect that has to be taken into consideration is the short-term and long-term cost of such control (Peltier et al., 2005).

"Risk management is the process that allows business managers to balance operational and economic costs of protective measures and achieve gains in mission capability by protecting business processes that support the business objectives or mission of the enterprise" (Peltier et al., 2005).

The risk analysis allows the organization to take control of their destiny. With an effective risk analysis process, only the needed controls and safeguards will be implemented. Before every task, project, or development cycle, every organization should perform a risk analysis (Peltier et al., 2005).

To Peltier et al., there are six steps in each risk analysis, namely:

1. **Asset Definition:** definition of the process, application, system, or asset that is going to have the risk analysis performed upon it. The key is to define the boundaries of what is to be reviewed;

2. **Threat Identification:** threats are undesirable events that could impact the business objectives and mission. Threats could be natural such as floods or earthquakes, human such as unintentional

acts (e.g. errors and omissions) or deliberate acts (e.g. malicious software, unauthorized access), and environmental such as pollution or chemical spills. The detection of a complete list of all threats that could impact an organization is very important;

3. **Determine Probability of Occurrence:** for each threat it is necessary to determine how likely that threat is to occur;
4. **Determine the Impact of the Threat:** having determined the likelihood of occurrence of each threat it is important to determine the impact that the threat will have on the organization. The impact measures the magnitude of loss or harm to the value of an asset;
5. **Controls Recommended:** having determinate the likelihood and impact of each threat it is important to identify the controls or safeguards that could eliminate or reduce the risk to an acceptable level.
6. **Documentation:** once the risk analysis is complete, the results should be documented in a formal report.

Another important aspect of each risk analysis is risk mitigation. This is a systematic methodology used to reduce organizational risk. To Peltier et al., there are six most common methods of risk mitigation, namely:

1. **Risk assumption:** one acceptable outcome of a risk analysis is to accept the potential risk and continue the normal operation of the organization. In this case, the organization accepts the risk;
2. **Risk alleviation:** implementation of controls that will lower the risk to an acceptable level;
3. **Risk avoidance:** elimination of the processes that causes the risk and thereafter the risk is avoided;
4. **Risk limitation:** implementation of controls that will minimize the adverse impact of a threat;
5. **Risk planning:** development of an architecture that prioritizes, implements, and maintains controls;
6. **Risk transference:** transfer the risk using other options to compensate for a loss such as purchasing an insurance policy.

"Whichever risk mitigation technique is used, the business objectives or mission of an organization must be considered when selecting any of these techniques" (Peltier et al., 2005).

The analysis of the cost/benefit of each implemented control is also very important for the risk analysis process. This process should be conducted for each new or enhanced control to determine if the control recommended is appropriate for the organization. This analysis should determine the impact of implementing the new or enhanced control and the impact of not implementing them.

III) Information Security Measurement and Metrics

"Metrics are tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data" and "measurements provide single-point-in-time views of specific, discrete factors" (Ahmed, 2016).

In other words, measurements are generated by counting, are objective raw data, and metrics are generated from analysis, are either objective or subjective human interpretations of those data. For information system security purposes, the "measures are concerned with aspects of the system that contribute to its security. That is, security metrics involve the application of a method of measurement to one or more entities of a system that possess an assessable security property to obtain a measured value" (Ahmed, 2016).

"The use of security metrics could bring a great number of organizational and financial advantages for the organization. It could improve the sense of responsibility with regard to the organizations' information security. Through the results obtained, organizations' management can locate the technical, operational, or managerial measures which are correctly or incorrectly implemented. These results make it possible to locate the problems and solve them" (Ahmed, 2016).

Standards such as International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27004 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55 are examples of Standards that focuses on Information Security Measurement and Metrics.

2.1.2 Standards and Regulations

InfoSec standards play an important role in the effective implementation of information security and in the development of an effective information security architecture. There are several standards that help the evaluation, development and management of InfoSec. Table 1 presents a short description of some of the most used and worldwide known standards and regulations.

Table 1: Standards and Regulations

Standard or Regulation	Description
ISO/IEC 15408	Develops and identifies criteria for evaluation of IT security.
ISO/IEC 18405	Defines the the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408.
ISO/IEC 27001	Specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System.
ISO/IEC 27002	Defines the guidelines for organizational information security standards and information security management practices.
NIST SP 800-53	Specifies security and privacy controls for Information Systems and Organizations.
GDPR	Regulates processes and activities of personal data which have a link to the European Union territory or market.

In a study performed by Benslimane et al. in 2016 (Benslimane et al., 2016) that investigates the relative role of security standards, professional security certifications and technological tools in the protection of organizational data it is founded that an average of 58% of inquiries refers that knowledge related to security standards is required or desired.

"Cyber security standards can be used to help identify problems and reduce the vulnerabilities in a control system. By knowing the problems and vulnerabilities, standards can be applied to control systems and to minimize the risk of intrusion" (Idaho National Laboratory, 2005).

I) ISO/IEC 15408

The ISO/IEC 15408 - Information technology - Security techniques - Evaluation Criteria for IT Security standard, created by the ISO and the IEC, is the result of a series of efforts to develop criteria for evaluation of IT security, and is one of the most accepted by the international community.(Aizuddin, 2019).

The ISO/IEC 15408 series is divided in three parts: ISO/IEC 15408-1:2009 - Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, ISO/IEC

15408-2:2008 - Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components and ISO/IEC 15408-3:2008 - Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.

The ISO/IEC 15408-1:2009 establishes "the general concepts and principles of IT security evaluations and specifies the general model of evaluation given" (ISO, 2009). It also defines the terms and abbreviations to be used in all 15408 documents.

The ISO/IEC 15408-2:2008 defines "the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408. It contains a comprehensive catalogue of predefined security functional components that will meet the most common security needs of the marketplace" (ISO, 2008a).

Finally, the ISO/IEC 15408-3:2008 defines the assurance requirements of the evaluation criteria, that includes the evaluation assurance levels, the composed assurance packages, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of protection profiles and security targets (ISO, 2008b).

II) ISO/IEC 18045

The ISO/IEC 18045:2008 - Information technology - Security techniques - Evaluation criteria for IT security "defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408. ISO/IEC 18045:2008 does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance" (ISO, 2008c). To conclude, this standard is very helpful to perform the evaluation recommended by the ISO/IEC 15408 standard.

III) ISO/IEC 27000

The ISO/IEC 27000 is a family of standards to help organizations manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties (ISO, 2013a).

There are several standards in the ISO/IEC 27000 family divided in Vocabulary Standards, Requirement Standards, Guidelines Standards, Sector-specific Guidelines Standards, and Control-specific Guideline Standards (Figure 5). To this research, the most important ISO/IEC 27000 family standards are the ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management

systems — Requirements and ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls.

The ISO/IEC 27001:2013 standard "specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization" (ISO, 2013a).

The ISO/IEC 27002:2013 standard "gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s)" (ISO, 2013b).

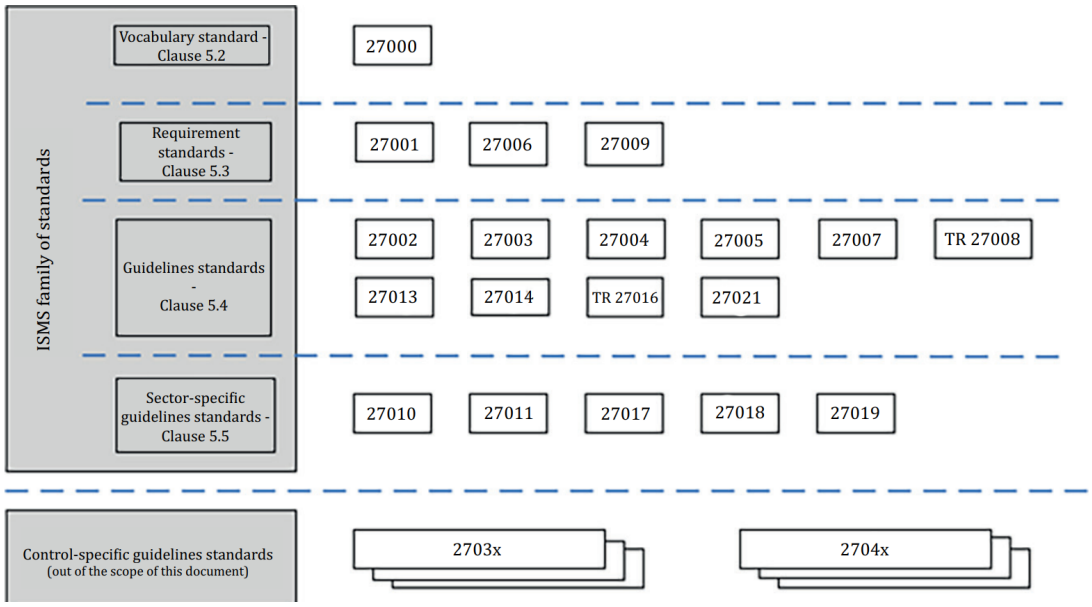


Figure 5: ISO/IEC 27000 standards family. Retrieved from (ISO, 2018)

IV) NIST SP 800-53

NIST SP 800-53 - Security and Privacy Controls for Information Systems Organizations "provides a catalog of security and privacy controls for federal information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, natural disasters, structural failures, human errors, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk" (National Institute of Standards and Technology, 2020a).

This standard addresses security and privacy from a functionality and assurance perspective. "Addressing both functionality and assurance ensures that Information Technology products and the Information Systems that rely on those products are sufficiently trustworthy" (National Institute of Standards and Technology, 2020a).

V) General Data Protection Regulation

General Data Protection Regulation (GDPR) is the name given to the European Union Regulation 2016/679 approved by the European Parliament and the Council of 27 April 2016. The GDPR regulates processes and activities of personal data which have a link to the European Union territory or market.

According to Albrecht, (Albrecht, 2016) "GDPR will bring more legal certainty and coherence than today, where 28 different legal systems as well as 28 different judicial and enforcement cultures define the regulatory environment."

As can be seen on Article 1 of GDPR (European Parliament and the Council & of 27 April 2016, 2016), this regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data and protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

"This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system" (European Parliament and the Council & of 27 April 2016, 2016).

This regulation is one of the most important regulations currently enforced in the member states of the European Union concerning the protection of personal data and citizens own privacy.

According to Soleve (Solove, 2008), "privacy is an issue of profound importance around the world. In nearly every nation, numerous statutes, constitutional rights, and judicial decisions seek to protect privacy. In the constitutional law of countries around the globe, privacy is enshrined as a fundamental right". Accordingly, it is fair to say that privacy is critical.

2.1.3 Frameworks

Information Security Frameworks play an important role, they "provide guidance for the effective implementation of Information Security in the organization and development of an effective Information Security architecture, which in turn, provides assurance that information security has been effectively employed in the organization" (Rao & Nayak, 2014).

Information Security Frameworks enables organizations to either prevent or detect and react to attacks or to recover from attacks. In Table 2 are listed some of the most important Information Security Frameworks.

Table 2: Security Frameworks

Security Framework	Version	Description
Center for Internet Security Controls (CIS)	7.1	The CIS Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.
HITRUST Common Security Framework (CSF)	9.31	The HITRUST CFS provides the structure, transparency, guidance, and cross-references to authoritative sources organizations globally need to be certain of their own data protection compliance as well as that of the many organizations with whom they inter-operate.
Information Security Manual (ISM)	NA	The purpose of the Australian Government ISM is to outline a cybersecurity framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats.
NIST Framework for Improving Critical Infrastructure Cybersecurity	1.1	This Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively.
Protective Security Requirements (PSR)	NA	The New Zealand PSR sets out what an organizations must do to manage security effectively.

I) CIS Controls

The CIS Controls "are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks." (Center for Internet Security, 2019). This framework receives the knowledge and expertise from several sectors such as retail, manufacturing, healthcare, education, government, and defense, among others. One important characteristic of CIS Controls is that they "are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on

actions" (Center for Internet Security, 2019).

"The CIS Controls are a relatively small number of prioritized, well-vetted, and supported security actions that organizations can take to assess and improve their current security state. They also change the discussion from "What should my enterprise do?" to "What should we ALL be doing?" to improve security across a broad scale" (Center for Internet Security, 2019).

II) HITRUST CSF

The mission of HITRUST is to provide "a common security and privacy framework which provides the structure, transparency, guidance, and cross-references to authoritative sources organizations globally need to be certain of their own data protection compliance as well as that of the many organizations with whom they interoperate" (HITRUST, 2019b). To do that HITRUST developed the HITRUST CFS, a common security and privacy framework, "which allows organizations in any sector globally to create, access, store, or transmit information safely and securely–with confidence" (HITRUST, 2019b).

HITRUST CFS core structure is based in ISO/IEC 27001 and 27002 that was already summarized on the previous section and incorporates more than forty other security regulations, standards, and frameworks (HITRUST, 2019b).

To summarize "The HITRUST CSF is a framework that normalizes security and privacy requirements for organizations, including federal legislation (e.g., HIPAA), federal agency rules and guidance (e.g., NIST), state legislation (e.g., California Consumer Privacy Act), international regulation (e.g., GDPR), and industry frameworks (e.g., PCI, COBIT); and simplifies the myriad of requirements by providing a single-source solution, tailored to the needs of the organization" (HITRUST, 2019b).

III) Information security Manual

The purpose of the ISM "is to outline a cybersecurity framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats" (Australian Cyber Security Center, 2020). The ISM is intended for Chief Information Security Officers, Chief Information Officers, cybersecurity professionals, and information technologies managers (Australian Cyber Security Center, 2020).

This framework is composed of cybersecurity principles that "provide strategic guidance on how organisations can protect their systems and information from cyber threats" and cybersecurity guidelines that "provide practical guidance on how organisations can protect their systems and information from

cyber threats" (Australian Cyber Security Center, 2020).

IV) NIST Framework for Improving Critical Infrastructure Cybersecurity

One of the main goals of NIST is the identification of "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including Information Security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks" (National Institute of Standards and Technology, 2018). This goal was formalized on the NIST Framework for Improving Critical Infrastructure Cybersecurity.

This framework uses "business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes". Also, this Framework "provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today" (National Institute of Standards and Technology, 2018).

This Framework could be implemented on "organizations relying on technology, whether their cybersecurity focus is primarily on Information Technology, industrial control systems, cyber-physical systems, or connected devices more generally, including the Internet of Things". It can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties (National Institute of Standards and Technology, 2018).

V) Protective Security Requirements

The PSR is a New Zealand public and private Framework that "sets out what your organisation must do to manage security effectively. It also contains best-practice guidance you should consider following". This Framework follow a risk-based approach for flexible implementation (Protective Security Requirements, n.d.).

The PSR defines 20 mandatory requirements that should be adopted by organizations as best-practices. "The PSR provides you with management protocols, lifecycle models, and guidance on how to meet the mandatory requirements" (Protective Security Requirements, n.d.).

2.2 Critical Areas

To identify critical areas, one of the largest Portuguese companies dedicated to developing software and information systems, Critical Software, can be used as an example: "We work across some of the most demanding industries, providing software and system services for safety, mission and business-critical applications" ("Critical Software", 2019).

Critical Software works in ten critical industry areas, that are: aerospace, automotive, defense, energy and utilities, finance, government, medical devices, railway, space and telecoms ("Critical Software", 2019). To them, "We depend on medical devices to care for people across the world. Patient monitoring systems, life support machines, defibrillators, implants and more all rely on increasingly complex software to work. With the margins for error tiny, the stakes could not be higher and healthcare professionals need to trust the technology they use" ("Critical Software", 2019). Thus emerges the importance of talking about critical health.

2.2.1 Critical Health

According to Portela (Portela, 2013) there are several environments in healthcare characterized as places where the decision process is fundamental to their success. "Critical environments demand for decisions in real-time, which require efficient, secure and ubiquitous processes. This kind of environments includes, for instance, intensive care units, operation rooms, emergency rooms, decision rooms and services where decision making can jeopardize a number of factors due to the urgency of action, and delicacy and type of the variables used in those situations. Typically, they deal with critical variables which are in constant change." (Portela, 2013).

According to Tang et al. (Tang et al., 2007), "intensive care units remote monitoring was designed to leverage the power of health Information Technology to help intensivists access clinical data and interact with bedside caregivers from a remote site, thereby promoting continuous and proactive patient management in intensive care units". This example provided by Tang et al. could not exist without Telemedicine and Telehealth.

I) Telemedicine and Telehealth

According to Darkins & Cary (Darkins & Cary, 2000) "Telemedicine and Telehealth promise to bring untold change to the healthcare industry and radically improve the delivery of care to patients".

One way to define Telemedicine is: "Telemedicine involves the use of modern Information Technology, especially two-way interactive audio/video communications, computers, and telemetry, to deliver health services to remote patients and to facilitate information exchange between primary care physicians and specialists at some distances from each other" (Darkins & Cary, 2000). Another possible definition is: "The use of advanced telecommunications technologies to exchange health information and provide healthcare services across geographic, time, social and cultural barriers" (Darkins & Cary, 2000). Both these definitions have elements in common: they both indicate the use of technology and point out the possibility of exchanging patient information no matter the distance between health providers and patients.

Darkins & Cary (Darkins & Cary, 2000) cited the differences between Telemedicine and Telehealth, proposed by the World Health Organization (WHO), for better understanding: "If Telehealth is understood to mean the integration of telecommunications systems into the practice of protecting and promoting health, while Telemedicine is the incorporation of these systems into curative medicine" (Darkins & Cary, 2000). Figure 6 graphically represents this differences.

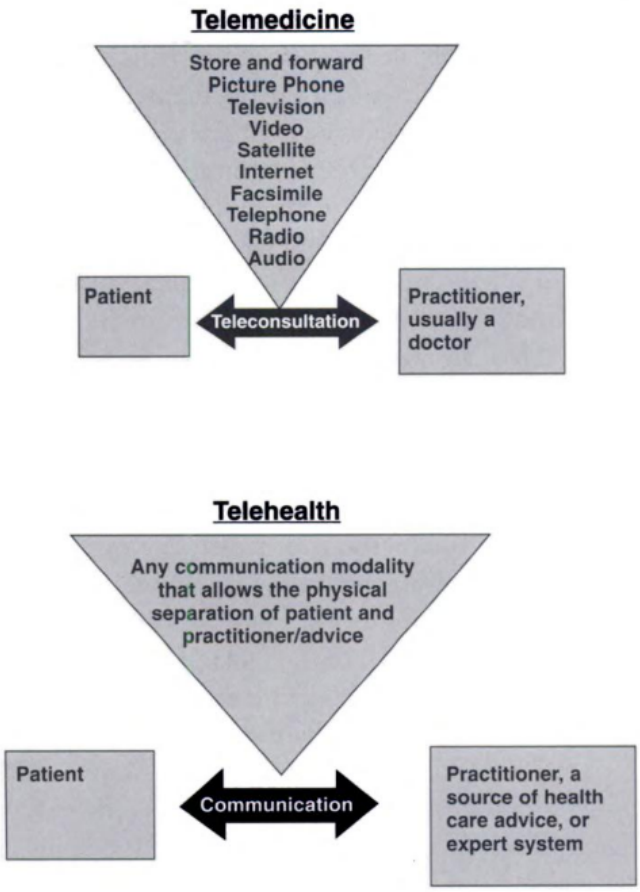


Figure 6: Telemedicine and Telehealth. Retrieved from (Darkins & Cary, 2000)

To conclude, while Telemedicine is the use of IT technologies to allow remote consultation between a patient and a healthcare provider, Telehealth is the use of any means of communication that allows the physical separation between patient and healthcare provider.

Fong et al., (Fong et al., 2011) summarize several healthcare services that can be supported by the use of Telemedicine (Figure 7).

- Tele-Assistance and Emergency services allows the remote communication between Ambulances, Paramedics and Patients;
- Tele-Consulting allows the remote medical consultation of patients by their healthcare provider;
- Tele-Diagnosis allows the remote diagnosis by sharing information between several healthcare providers;
- Tele-Monitoring allows nurses to monitor the health status of the patient remotely;
- Tele-Surgery allows surgeons to perform surgeries remotely.

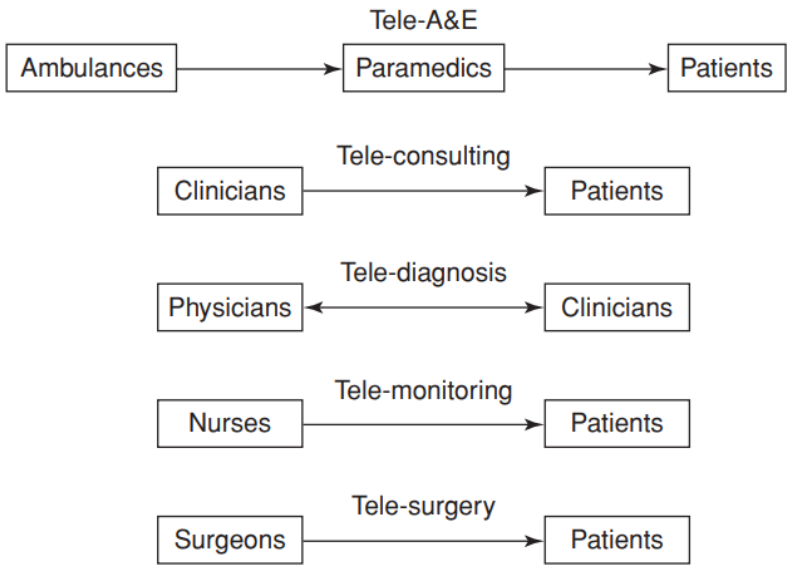


Figure 7: Applications of Telemedicine. Retrieved from (Fong et al., 2011)

Looking carefully at Figure 7 there is one common characteristic in all the applications of Telemedicine: all of them feature transmission of medical information from one entity to another.

This research focuses on Telehealth, specifically in the devices that remotely exchange information with healthcare professionals.

The GDPR (European Parliament and the Council & of 27 April 2016, 2016) points out, some special categories of personal data in Art.9: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited" (European Parliament and the Council & of 27 April 2016, 2016).

Health information is thus a special category of personal data, so it follows that exchanging and sharing these sensitive data brings with it security concerns.

II) Remote Patient Monitoring

According to NEJM Catalyst (NEJM Catalyst, 2018), Remote Patient Monitoring (RPM) "involves the reporting, collection, transmission, and evaluation of patient health data through electronic devices such as wearables, mobile devices, smartphone apps, and internet-enabled computers".

One of the most significant advantages of RPM is that it can allow earlier detection of complications and the identification of patients who need to seek medical attention before in-person appointments (NEJM Catalyst, 2018).

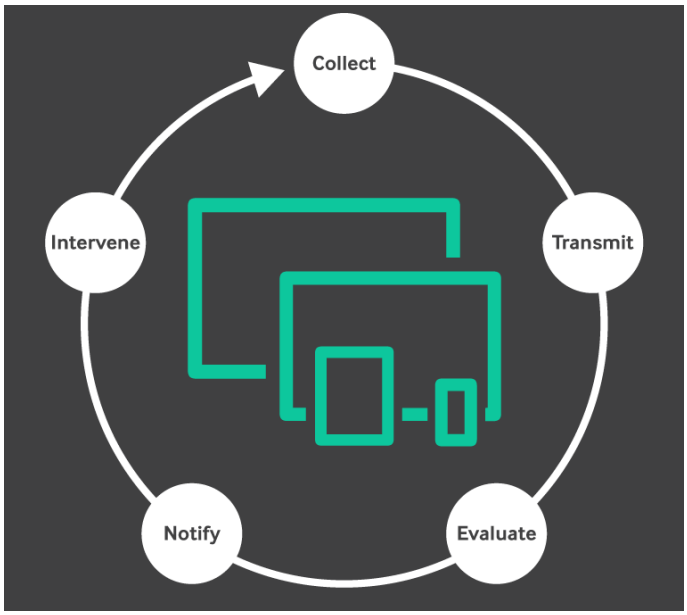


Figure 8: RPM Cycle for Telehealth, adapted from (NEJM Catalyst, 2018)

The RPM Cycle includes the collection, transmission, evaluation, notification, intervention phases (Figure 8).

RPM Systems are designed to collect several physiological information from patients such as electrocardiography tracing, electroencephalography tracing, heart rate, respiration rate, oximetry, blood pressure, nervous system signals, body temperature, blood glucose rate (Malasinghe et al., 2019). These are only some of the physiological data that can be made accessible with RPM.

III) Remote Patient Monitoring Systems

According to Malasinghe et al. (Malasinghe et al., 2019) RPM Systems are designed to obtain several physiological data from patients such as electrocardiogram, electroencephalogram, heartbeats and respiration rate, oxygen volume in blood or pulse oximetry, signals from the nervous system, blood pressure, body/skin temperature, and blood glucose level, among others.

Malasinghe et al. (Malasinghe et al., 2019) describes two groups of RPM Systems:

- Contact-based RPM Systems - RPM Systems that use different sensors, processing technologies, communication technologies, post-processing actions, databases and receivers/end-terminals that can address several diseases.
- Contactless RPM Systems - These RPM Systems can be categorized mainly into two sections:
  - Image-based systems - These systems analyze images of patients as their data and detect illnesses or falls.
  - Radar-based systems - These systems used radio frequencies to get inputs for their systems and also sometimes have patient localization capability.

Malasinghe et al. (Malasinghe et al., 2019) also presents a disease-based classification for RPM Systems:

- Heart and blood-related diseases monitoring systems - These are the most common RPM systems. The reason for that is that vital signs associated with the heart could relate to many illnesses such as cardiac arrhythmia, chronic heart failure, strokes, blood clots, and high blood pressure.
  - Contact-based systems - RPM Systems that use hardware and software devices to monitor various heart-related illnesses.
  - Contactless systems - Systems that can remotely access heart rate by skin color processing or cuffless blood pressure monitoring systems or the use of Kinect cameras to measure the

heart and respiratory rates are examples of contactless heart and blood-related diseases monitoring systems.

- Fall detection and mobility-related diseases monitoring systems - Fall detection systems are an essential type of system, especially for elderly persons monitoring. These systems too appear as contact-based and contactless as these systems target mainly elderly community and post-accident recovery patients.

- Monitoring system for the brain, neurological system-related diseases, and mental health - RPM Systems that can be used to detect brain, neurological and mental diseases as well monitor is status.

  - Contact-based systems - There are several RPM Systems based in sensors such as, for example, a textile-based autonomic nervous sensor or can be used to detect mental or neurological changes.
  - Contactless systems - Systems that for example track activity of patients with Alzheimer disease through the use of Kinetic cameras is an example of contactless RPM Systems.

- Diabetes Monitoring Systems - RPM Systems that monitor the Glucose levels of patients with Diabetes.

  - Contact-based systems - Glucose sensors that monitor the glucose level on blood and determine the among of insulin that the patient has to administer.
  - Contactless systems - Some systems use contactless methods on diabetic retinopathy screening through the sporadic photographs of patients retina.

IV) Security Issues

According to Olanrewaju et al. (Olanrewaju et al., 2013), the protection of personal information like health information must be ensured. The advent of Telehealth and/or Telemedicine allows the connection between healthcare professionals and patients through ubiquitous and cloud computing over electronic networks. Confidentiality, Integrity and, Authentication of patient data are three of the key factors to be considered.

Many healthcare organizations implement an *ad hoc* management of Telemedicine. This creates ineffective management of patient privacy and security issues that may compromise the overall success of the health system (Olanrewaju et al., 2013).

There are several potential risks related with privacy in any health care activity that requires the exchange of patient information and organizations or individuals. "The potential for protected health information to be exposed when organizations or individuals cooperate in a Telehealth/Telemedicine interaction may be greater than face-to-face interactions, particularly when Telehealth activities are not integrated into an organization's usual practice patterns" (Olanrewaju et al., 2013).

For Hall & McGraw (Hall & Mcgraw, 2014), the success of Telehealth could be put in danger if serious privacy and security risks are not addressed.

Hall & McGraw (Hall & Mcgraw, 2014) identify potential privacy and security risks on Telehealth. Privacy risks involve "lack of controls or limits on the collection, use, and disclosure of sensitive personal information", and security risks "include breach of confidentiality during collection of sensitive data or during transmission to the provider's system; unauthorized access to the functionality of supporting devices as well as to data stored on them; and untrusted distribution of software and hardware to the patient".(Hall & Mcgraw, 2014)

According to Hale et al. (Hale et al., 2014), "concerns about the privacy and security of Telehealth systems may adversely affect people's trust in Telehealth and threaten the ability of these systems to improve the accessibility, quality, and effectiveness of healthcare".

Hall & McGraw (Hall & Mcgraw, 2014) identify important privacy and security controls for Telehealth implementations. With regard to security controls, Hall & McGraw (Hall & Mcgraw, 2014) point out that the most important controls are the laws or operation policies that implement Fair Information Practice Principles (FIPPs). These practices are widely accepted and include the ability to establish limitations on health information collection, use and disclosure, and allow people to make choices about their own health information. Hall & McGraw (Hall & Mcgraw, 2014) point out some important security controls, namely:

- Encryption: can ensure that if the attacker gains access to raw data it will be meaningless;
- Prohibition of installation of non-approved or non-examined software: medical and consumer devices typically used by patients for Telehealth can pose serious risks and can be under constant attack from threats like malware;
- Face-to-face setting and distribution of Telehealth software and hardware: this is a way of identifying the patient and authenticating the device that he/she is using.

2.2.2 Legislation

Two important laws concerning Health Information privacy and security are relevant to this research: the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and Health Information Technology for Economic and Clinical Health (HITECH) of 2009.

I) Health Insurance Portability and Accountability Act

According to Wilkinson & Reinhardt (Wilkinson & Reinhardt, 2015), HIPAA led to several standards about privacy, security and transaction of Individual Protected Health Information. These standards identify 18 different elements that are considered Protected Health Information, for example, the name, the street address, birthdate, admission date, discharge date and so on.

The Privacy Rule of HIPAA was developed to address the electronic transfer of private patient information. The main goal of the Privacy Rule is to prevent the dissemination of Protected Health Information (Sanger, 2009).

According to Wilkinson & Reinhardt (Wilkinson & Reinhardt, 2015), the entities to which HIPAA applies, have a list of requirements and suggested privacy and security measures that must be fulfilled to protect Private Health Information. Failure to do so could result in serious fines.

The problem is that business associates of covered entities were not directly regulated. These business associates are external entities that provide services for, or to, the covered entity using Protected Health Information (Sanger, 2009).

In the HITECH Act, Congress extended HIPAA to all business associates, or in other words, to all entities that create, receive, maintain, or transmit identifiable health information to perform a function or service to a covered entity (Hall & Mcgraw, 2014).

II) Health Information Technology for Economic and Clinical Health Act

On February 13, 2009, Congress passed the HITECH Act. "This addresses consumer access to their Electronic Health Records, increases application of HIPAA privacy standards to business associates of covered entities, and implements a tiered system of civil monetary penalties for HIPAA violations" (Sanger, 2009).

HITECH Act defines a personal health record as an "electronic record of identifiable information drawn from multiple sources and managed, shared, and controlled by the patient" (Hall & Mcgraw, 2014).

One of the most important characteristics of this law is the fact that business associates are now responsible for complying with HIPAA standards and requirements and are directly answerable to the government for HIPAA breaches. This also means that business associates are now also directly liable for civil and criminal penalties (Sanger, 2009).

Another important characteristic of HITECH is the fact this Act "established an expectation that professionals in health care must be familiar with technology, specifically as it relates to policies guiding the storage and transmission of Personal Health Information". The goals of HITECH include the electronic exchange and use of health information and the enterprise integration of such information (Wilkinson & Reinhardt, 2015).

According to Aman & Snekkenes (Aman & Snekkenes, 2013) eHealth involves "critical information exchange and requires a number of security services to make this information reliable, confidential, available and trustworthy".

RPM Systems "will no doubt greatly improve the quality of healthcare. However, it still have to face a number of challenges concerning security and privacy" (Aman & Snekkenes, 2013).

2.3 State-of-the-art

The Veterans Health Administration Care Coordination/Home Telehealth program started in 2003 cover, in 2008, 30000 patients managing common conditions such as diabetes, hypertension, heart failure, chronic obstructive pulmonary disease, and depression. To monitor these patients, the program uses at-home monitoring devices, self-care tools and audio-video consultations at home (Goodwin, 2010).

In 2012, Canadian Telehealth programs reported the use of RPM by more than 2500 Canadians. Besides that, in Canada and internationally, the number and range of evaluations of RPM programs are growing quickly (Gheorghiu & Ratchford, 2015).

In 2015, the World Health Organization Regional Officer for Europe published the "From Innovation to Implementation - eHealth in the WHO European Region" report based on data provided by the Member States in the 2015 WHO global survey on eHealth. Table 3 presents the most relevant findings from that report.

Table 3: From Innovation to Implementation - eHealth in the WHO European Region key findings adapted from (World Health Organization Regional Office for Europe, 2016)

Category	Threats
eHealth foundations	• "89% (40 Member States) have universities or technical colleges providing students with training on how to use information and communication technologies and eHealth"; • "82% (37 Member States) provide training to professionals on how to use information and communication technologies and eHealth".
Telehealth	• "27% of respondents (12 Member States) have a dedicated policy or strategy for Telehealth; an additional 36% (16 Member States) refer to Telehealth in their national eHealth policies or strategies"; • 72% (33 Member States) use Remote Patient Monitoring services which is the second most prevalent Telehealth programme.
Continued on next page	

Category	Threats
Legal frame-works	• "89% of respondents (36 Member States) have legislation to protect the privacy of an individual's health-related data in electronic format in electronic health records"; • "53% (24 Member States) do not have legislation that allows individuals electronic access to their own health data in their electronic health records"; • "50% (22 Member States) report that individuals have the legal right to specify which health-related information in their electronic health records can be shared with health professionals of their choice"; • "43% (19 Member States) have policies or legislation that defines medical jurisdiction, liability or reimbursement of eHealth services".

In 2016 the Department of Health and Human Services estimates that more than 60% of all healthcare institutions and between 40% to 50% of all hospitals in the United States currently use some form of Telehealth (Tuckson et al., 2017).

According to a study performed by the Consumer Technology Association (Cassagnol, 2019), 68% of the surveyed physicians strongly intend to use RPM technology to manage their patients health in the future. These intentions include the use of for example, continuous glucose or blood pressure monitors.

The biggest benefits of using technology to manage health were pointed out in a survey applied to 2004 United States citizens, 100 primary care physicians, 60 endocrinologists and 40 nurses and pointed by Cassagnol (Cassagnol, 2019) were:

- The improvement of patient outcomes in 49%;
- The improvement of compliance rates in 44%;
- The increase of ownership of patient health feeling in 42%.

The surveyed patients point as the biggest benefits:

- The more detailed information in personalized health in 43%;

- The faster access to health care services in 42%;
- The increased influence on their own well-being through ownership of health data in 33%.

In this same study (Cassagnol, 2019):

- 52% of consumers would use a connected health device as part of their treatment if a physician made the recommendation;
- 31% indicate that they would be influenced by pharmacist recommendations or by a health insurance company.

One very important conclusion of Consumer Technology Association is that 56% of "consumers would be happy to share health data with their doctor in order to get more accurate diagnosis and treatment solutions but, they also cite data security as their biggest concern, putting emphasis on the need for clear guidance and reassurance on patient data safety". Another important conclusion from this study is that 39% of the surveyed physicians believe that in future patients will track every aspect of their health via technology.(Cassagnol, 2019).

The use of Telehealth and RPM is increasing and is already a major part of healthcare provided services. The Consumer Technology Association survey also points to some concerns about privacy and security issues and the "From Innovation to Implementation - eHealth in the WHO European Region" report points to some lack of legislation concerns with digital health information.

Newman (Newman, 2017) on an article titled "Medical Devices Are the Next Security Nightmare" explains that medical devices with wireless connectivity, remote monitoring, and near-field communication tech create potential points of exposure compromising patients safety.

On 31 August 2017 Sturmer & Branley (Sturmer & Branley, 2017) published an article in ABC News site stressing that thousands of Australians may have pacemakers models that have been recalled in the United States because they were vulnerable to hacking. The United States Food and Drug Administration has recalled 465000 pacemakers from the Abbott manufacturer because hackers could remotely cause the batteries to rapidly go flat or force the pacemakers to run at potentially deadly speeds.

According to the same article (Sturmer & Branley, 2017) "Medicare statistics indicated there were about 11375 pacemakers and 3500 implantable cardioverter defibrillators implanted in Australia in 2016".

In an article published by Lovelace Jr. (Lovelace Jr., 2019) on 1st of October 2019 in CNBC News site Lovelace Jr. refers that the "Food and Drug Administration issued a warning to consumers about potentially serious cybersecurity flaws in some medical devices that could allow hackers to take control of

them remotely". According to the same article, researchers have identified eleven vulnerabilities that may allow "anyone to remotely take control of the medical device and change its function, cause a denial of service, or cause information leaks or logic flaws, which may prevent device function".

In 2019, the Ecri Institute releases a report titled "2019 Top 10 Health Technology Hazards" that identifies as the first Health Technology Hazards the fact that "Hackers Can Exploit Remote Access to Systems, Disrupting Healthcare Operations" (Ecri Institute, 2019).

According to that report, the cyberattacks can turn devices or systems inoperative, degrade their performance, or expose or compromise the data they hold. All of these can severely hinder the delivery of patient care and put patients at risk (Ecri Institute, 2019).

There is a pattern here: the number of RPM program implementations is increasing and the number of patients affected by these programs increases as well. At the same time, there have been identified new security vulnerabilities on high technological medical devices.

2.4 Security Threats in Remote Patient Monitoring

As a summary of what was previously discussed, and justifying this research relevance an analysis of the weakness and threats that relates security and data privacy with Telehealth (more precisely with RPM) follows:

- The growth of IT Technologies is faster than the growth of the theories that address how people should keep secure;
- The lack of dedicated policy or strategies for Telehealth combined with the fact that Telehealth is broadly used and Remote Patient Monitoring represents the most prevalent Telehealth programs;
- The lack of legislation that allows individual electronic access to their own health data;
- The lack of policies and legislation that define medical jurisdiction, liability or reimbursement of eHealth services;
- The existence of detected vulnerabilities on medical devices that can provide attackers remote access to the devices;
- The increase of computational power at lower prices that can makes attackers capable of increasingly powerful attacks.

3 Method

In this chapter, it is presented the scientific methodological approach that was chosen to guide this scientific research and the materials and technologies used to complete it.

3.1 Design Science Research

According to Peffers et al., (Peffers et al., 2007), the Design Science Research (DSR) incorporates the principles, the practices, and the procedures that are required to perform scientific research in Information Systems (IS) and meets three objectives: it is consistent with prior literature, it provides a nominal process model for doing DSR and, it provides a mental model for presenting and evaluating DSR in IS.

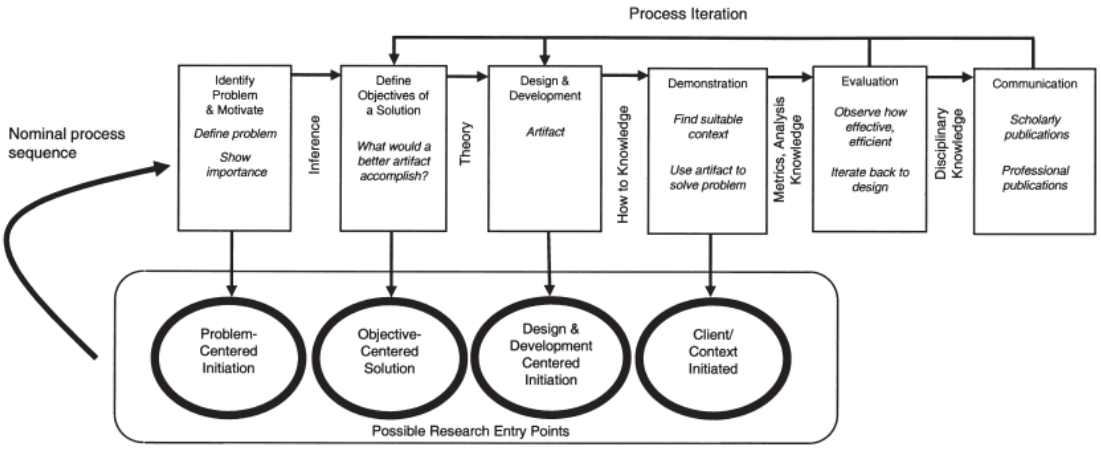


Figure 9: Design Science Research Model. Retrieved from (Peffers et al., 2007)

The DSR process includes six activities (Figure 9) which according to Peffers et al., (Peffers et al., 2007), are:

- Problem identification and motivation: in this iteration, it is expected that the researcher is able to define the specific research problem and justify the value of a solution. In this research project this iteration was fulfilled with the literature review described in Chapter 2. The result of this iteration could be seen in Section 1.1 of this document;

- Define the objectives for a solution: in this iteration, it is expected that the researcher is able to infer the objectives of a solution for the identified problem. It is desirable that the defined objectives be feasible. In this research project, these objectives can be found in Section 1.2 of this document, and Chapter 3 presents the strategy used in achieve the objectives and the expected results;

- Design and development: in this iteration, it is expected that the researcher can create a scientific research artifact. Such artifacts are constructs, models, methods, or instantiations. In this research project, this phase culminates with the creation of the Framework Proposal and can be founded in Subsection 4.3.7;

- Demonstration: in this iteration, it is expected that the researcher can demonstrate the use of the artifact to solve the identified problem. This demonstration could be achieved with the use of experimentation, simulation, case study, proof, or other appropriate activity. In this research project, in this iteration, it was created an RPM Device System Simulator and was performed a security assessment using the proposed Framework. This iteration can be founded in Section 4.3.8 of this document;

- Evaluation: in this iteration, it is expected that the researcher is able to observe and measure how well the produced artifact supports the solution to the problem. In this research project, in this iteration, the objectives initially defined and the expected results are compared with the result from the previous iteration. This iteration can be founded in Section 4.3.8 of this document;

- Communication: in this iteration, it is expected that the researcher is able to communicate the problem and its importance, the produced artifact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences. In this research project, this iteration produce the dissertation report and one scientific paper. These will be presented and evaluated by a jury and by the scientific community.

3.2 Materials and Technologies

Table 4 enumerates all the Materials and Technologies used during the realization of this scientific work. The materials are pieces of hardware used. The Technologies are programming and markup languages, software, or platforms used.

Table 4: Materials and Technologies

Name	Type	Purpose
LaTeX	Technology	Markdown language used to write all the documents.
Overleaf	Platform as a Service	Platform used to write, edit, and compile all the LaTeX documents.
Draw.IO	Platform as a Service	Platform used to draw all the diagrams and flows presented in all documents.
HTML, CSS, and JavaScript	Technology	Web languages used to create the website and the interface of the Remote Patient Monitoring Device System Simulator.
Node.JS	Technology	Server-side framework based in JavaScript used to create all the backend of the Remote Patient Monitoring Device System Simulator.
Heroku	Platform as a Service	Platform used to allocate and deploy the backend of the Remote Patient Monitoring Device System Simulator that was created in Node.JS.
MySQL	Technology	Database Management System used to save all the patient data of the Remote Patient Monitoring Device System Simulator.
Git	Technology	Source control technology used to save and manage all the versions of all coding components of the Remote Patient Monitoring Device System Simulator and all versions of the LaTeX documents.
GitHub	Platform as a Service	Platform used to save and manage the git repositories.
Visual Studio Code	Software	Editor used to write the code of the website, of the backend, and the interface of the Remote Patient Monitoring Device System Simulator.
NodeMCU	Material	Micro-controller with an ESP8266 WiFi Module used to simulate the Remote Patient Monitoring Device. Responsible for reading the information received from the Heart Rate Sensor and send it to the backend of the system (Figure 10).

Continued on next page

Name	Type	Purpose
Heart Rate Analogic Sensor	Material	Sensor used to capture the Heart Rate of the patient (Figure 11).
Arduino Code Editor	Software	Editor used to write and compile code to the NodeMCU micro-controller.

Figure 10: NodeMCU Micro-controller with an ESP8266 WiFi Module

Figure 11: Heart Rate Analog Sensor for Arduinos

4 Case Study

In this chapter, is presented and explained all the completed tasks during this scientific work and his importance for the whole project.

4.1 Framework Analysis

The first realized activity was the analysis of several Security Frameworks to understand its core and structure, to find their similarities and their differences. The selection of the next summarized Frameworks was due to two major factors: all of them are free, which means that everyone or every organization could access and use them, and all of them are widely known and adopted in many countries for many organizations. These Frameworks are often referred to as the best Security Frameworks to use in Information Security specialized forums and websites such as Info-Security Magazine (Infosecurity Magazine, 2019), IT Governance USA Blog (IT Governance USA Blog, 2019), and Cyber Experts (Cyber Experts, 2020).

4.1.1 Center for Internet Security Controls

According to what was referred on Section 2.2 of this document, the Center for Internet Security (CIS) Controls "are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks" (Center for Internet Security, 2019).

"The CIS Controls are a relatively small number of prioritized, well-vetted, and supported security actions that organizations can take to assess and improve their current security state. They also change the discussion from "What should my enterprise do?" to "What should we ALL be doing?" to improve security across a broad scale" (Center for Internet Security, 2019).

Related to the core structure of the CIS Controls Framework it is important to retain the following aspects:

- CIS Controls defines three Implementation Groups (Center for Internet Security, 2019) that are:
  - IG1 - Implementation Group 1: small to medium-sized organization with limited Information Technologies (IT) and cybersecurity expertise to dedicate toward protecting IT assets and personnel;
  - IG2 - Implementation Group 2: organization with the ability to employ individuals exclusively to manage and protect IT infrastructure;

  - IG3 - Implementation Group 3: organizations with the ability to employ security experts that specialize in the different facets of cybersecurity such as risk management or penetration testing.

- CIS Controls defines three control layers. Each layer has specific controls and each Control as specific sub-controls. Each sub-control has a specific security function and protects one asset type. Each sub-control could be implemented in one or more Implementation Groups;
- CIS Controls Layers:
  - Basic Layer: composed by 6 controls and 47 sub-controls;
  - Foundational Layer: composed by 10 controls and 88 sub-controls;
  - Organizational Layer: composed by 4 controls and 36 sub-controls.
- CIS Controls Security Functions: Identify, Detect, Protect and Respond;
- CIS Controls Assets Types: Applications, Devices, Users, Data and Network.

4.1.2 HITRUST Common Security Framework

Fundamental to HITRUST mission "is the availability of a common security and privacy framework which provides the structure, transparency, guidance, and cross-references to authoritative sources organizations globally need to be certain of their own data protection compliance as well as that of the many organizations with whom they interoperate" (HITRUST, 2019b).

To do that HITRUST developed the HITRUST Common Security Framework (CSF) which "allows organizations in any sector globally to create, access, store, or transmit information safely and securely–with confidence" (HITRUST, 2019b).

This Framework intends to normalize security and privacy requirements for organizations, including federal legislation such as HIPAA, federal agency rules, and guidance such as National Institute of Standards and Technology (NIST) Standards, state legislation, international regulation such as GDPR, and industry frameworks such as COBIT (HITRUST, 2019b). "The HITRUST CSF is the only framework built to provide scalable security and privacy requirements based on the different risks and exposures of each unique organization" (HITRUST, 2019b).

Related to the core structure of the HITRUST CFS Framework it is important to retain the following aspects:

- HITRUST CFS core structure is based on ISO/IEC 270001 and ISO/IEC 27002 standards and incorporates more than 40 other security and privacy-related regulations. Standards and Frameworks;
- HITRUST CFS is segmented in 14 Control Categories;
- According to HITRUST (HITRUST, 2019b) each HITRUST CSF Control Category has the following architecture:
  - Control Objective: statement of the desired result, or purpose to be achieved, by one or more control within the control category;
  - Control Reference: control number and title;
  - Control Specification: policies, procedures, guidelines, practices, or organizational structures, which can be managed, operational, technical, or legal, required to meet the control objective;
  - Risk Factor Type: predefined organizational, regulatory, or system risk factors that increase the inherent risk to an organization or system, necessitating a higher level of compliance;
  - Topics: keywords indicating relevant categories associated with the control reference;
  - Implementation Requirements: detailed information to support the implementation of the control to meet the control objective. Requirements are defined based on relevant factors through three progressive implementation levels, or by specific segment;
  - Implementation Requirement Levels: three levels of requirements are defined based on organizational, regulatory, or system risk factors. Level 1 provides the minimum baseline control requirements; each subsequent level encompasses the lower level and includes additional requirements, commensurate with increasing levels of risk;
  - Segment Specific Requirement Levels: certain industries, or segments of industries, have specific requirements. The HITRUST CSF contains specific implementation levels that provide additional requirements for these segments such as GDPR;
  - Control Standard Mapping by Level: documented mapping to the related authoritative source(s).
- HITRUST CSF is composed of 14 control categories, 49 control objectives, and 156 control references (HITRUST, 2019a);

4.1.3 Information Security Manual

The Information Security Manual (ISM) is a cybersecurity Framework developed by the Australian Government that can be applied by the organizations to protect their systems and information from cybersecurity threats (Australian Cyber Security Center, 2020).

The intended audience of this Framework includes the Chief Information Security Officers, Chief Information Officers and cybersecurity professionals and information technology managers (Australian Cyber Security Center, 2020).

Related to the core structure of the ISM Framework it is important to retain the following aspects:

- ISM is a risk-based Framework, and it is divided in cybersecurity principals and cybersecurity guidelines;
- Cybersecurity principals: the purpose of the cybersecurity principals is to provide strategic guidance on how organization can protect systems and information from cybersecurity threats. The cybersecurity principals are grouped in four key activities (Australian Cyber Security Center, 2020):
  - Govern: identifying and managing security risks (5 principals);
  - Protect: implementing security controls to reduce risks (14 principals);
  - Detect: detecting and understanding cybersecurity events (1 principal);
  - Respond: responding to and recovering from cybersecurity incidents (3 principals).
- Cybersecurity guidelines: the purpose of cybersecurity guidelines is to provide practical guidance on how organizations can protect systems and information from cybersecurity threats. The cybersecurity guidelines cover the following matters (Australian Cyber Security Center, 2020):
  - Governance;
  - Physical Security;
  - Personal Security;
  - Information and Communications Technology Security.
- Each guideline has one or more targets and for each of them is defined one or more possible security controls.

4.1.4 NIST Framework for Improving Critical Infrastructure Cybersecurity

One of the objectives of the NIST comprehends the identification of a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that can be adopted to identify, assess, and manage cybersecurity risks (National Institute of Standards and Technology, 2018).

The NIST Framework for Improving Critical Infrastructure Cybersecurity intends to respond to the previously presented NIST objective. This framework "focuses on using business drivers to guide cybersecurity activities and cybersecurity risks as part of the organization's risk management processes" (National Institute of Standards and Technology, 2018)-

The NIST Framework provides a "common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively" (National Institute of Standards and Technology, 2018). This Framework offers a flexible way to address cybersecurity, and it is applicable to organizations relying on technology and organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties (National Institute of Standards and Technology, 2018).

- NIST Framework for Improving Critical Infrastructure Cybersecurity is structured in three parts (National Institute of Standards and Technology, 2018):
  - Framework Core: set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors;
  - Framework Implementation Tiers: provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. They describe the degree to which an organization cybersecurity risk management practices according to the framework specifications;
  - Framework Profile: represents the outcomes based on business needs that an organization has selected from the Framework categories and subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario.
- The Framework Core comprises four elements (National Institute of Standards and Technology, 2018):

  - Functions: basic cybersecurity activities at their highest level;
  - Categories: Subdivisions of functions into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities;
  - Subcategories: subdivisions of categories into specific outcomes of technical and/or management activities;
  - Informative References: specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory.

- The Framework identifies five concurrent and continuous functions (National Institute of Standards and Technology, 2018):
  - Identify: develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities;
  - Protect: develop and implement appropriate safeguards to ensure the delivery of critical services;
  - Detect: develop and implement appropriate activities to identify the occurrence of a cybersecurity event;
  - Respond: develop and implement appropriate activities to take action regarding a detected cybersecurity incident;
  - Recover: develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

- The defined Framework Implementation Tiers are (National Institute of Standards and Technology, 2018):
  - Tier 1 - Partial: related to the Risk Management process the organization does not have formalized cybersecurity risk management practices. Related to the Integrated Risk Management Program there is limited awareness of cybersecurity risk at the organizational level. Which concerns with External Participation, the organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents;
  - Tier 2 - Informed: related to the Risk Management process risk management practices are approved by management but may not be established as organizational-wide policy. Related

to the Integrated Risk Management program there is an awareness of cybersecurity risk at the organization level, but an organization-wide approach to managing cybersecurity risk has not been established. Which concerns with external participation, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both;

- Tier 3 - Repeatable: Related to the Risk Management process the organization risk management practices are formally approved and expressed as policy. Related to the Integrated Risk Management program, there is an organization-wide approach to manage cybersecurity risk. Which concerns with external participation, the organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community broader understanding of risks;
- Tier 4 - Adaptive: related to the Risk Management process, the organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Related to the Integrated Risk Management program, there is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Which concerns with external participation, the organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community broader understanding of risks.

- This Framework identifies two important profiles, namely:
  - As-Is: the current organization profile;
  - To-Be: the target or desired organization profile.

4.1.5 Protective Security Requirements

The Protective Security Requirements (PSR), defined by the New Zealand Government "outlines the government expectations for security governance, for personnel, information, and physical security" (Protective Security Requirements, n.d.). The PSR sets "out what your organization must do to manage security effectively. It also contains best-practice guidance you should consider following" (Protective Security Requirements, n.d.).

PSR could be used by public and private sector organizations. To successfully manage security risks, organizations must ensure that security is part of the organizational culture, practices, and operational

plans.The New Zealand government defines 20 mandatory requirements that organizations should meet to improve the management of security risks. The PSR also provides management protocols, lifecycle models, and guidance on how organizations should act to fulfill the requirements (Protective Security Requirements, n.d.).

- PSR defines 20 mandatory requirements and four categories (Protective Security Requirements, n.d.):
  - Security Governance (GOVSEC) - contains 8 requirements;
  - Personal Security (PERSEC) - contains 4 requirements;
  - Information Security (INFOSEC) - contains 4 requirements;
  - Physical Security (PHYSEC) - contains 4 requirements.
- New Zealand Protective Security Requirements is a complement document that contains detailed processes and controls essential for the protection of information and systems.

4.1.6 Common Aspects

After the previous framework analysis, it was important to identify the common aspects of the studied Frameworks. To do that, it was selected some key categories in a way that the common aspects could be grouped. Table 5 presents all the common aspects grouped by the selected key categories.

Table 5: Common aspects between the studied Frameworks

Category	**Common Aspects**
Granularity	**CIS Controls**, **HITRUST CFS** and **Information Security Manual** has the control as the smallest element. They define and indicate a set of controls to be used to improve Information Technologies (IT) Security on organizations. **NIST Framework for Improving Critical Infrastructure cybersecurity** and **Protective Security Requirements** has the activity/requirement as the smallest element. They define a set of activities to perform or requirements to achieve in order to improve Organizations IT Security.
	Continued on next page

Category	Common Aspects
Functions	**CIS Controls**, **Information Security Manual**, and **NIST Framework for Improving Critical Infrastructure cybersecurity** define a set of functions in order to aggregate controls or activities: **Identify** (appear in 2 Frameworks); **Detect** (appear in 3 Frameworks); **Protect** - (appear in 3 Frameworks); **Respond** - (appear in 3 Frameworks); **Govern** (appear in 1 Framework); **Respond** (appear in 1 Framework).
Layers	**CIS Controls** and **Protective Security Requirements** define some layers. The layers allows the framework to group the controls, the activities or requirements in some kind of structure. **CIS Controls** defines 3 layers: Basic; Foundational; Organizational. **Protective Security Requirements** defines 4 layers: Security Governance; Personal Security; Information Security; Physical Security.
Profile	**NIST Framework for Improving Critical Infrastructure cybersecurity** and **Protective Security Requirements** distinguishes the current organization profile from the target profile. The target organization profile represents the profile of the organization after the implementation of the framework.
Segregation	**NIST Framework for Improving Critical Infrastructure Cybersecurity** defines 4 tiers to define the level of Risk Management maturity: Tier 1 - Partial; Tier 2 - Informed; Tier 2 - Repeatable; Tier 4 - Adaptive. **CIS Controls** defines 3 implementation groups to know: IG1; IG2; IG3. This segregation of the organizations allows a better knowledge of the organization and thereafter a better framework implementation.

4.2 Standards Analysis

After finished the Framework analysis, it was time to analyze several important Standards to understand its core and structure, to find their similarities and their differences. All the selected Standards are related to Information Security and play an important role.

4.2.1 NIST Special Publication 800-53

The NIST Special Publication (SP) 800-53 Security and Privacy Controls for Information Systems and Organizations "provides a catalog of security and privacy controls for federal information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, natural disasters, structural failures, human errors, and privacy risks" (National Institute of Standards and Technology, 2020b).

Related to the core structure of the NIST SP 800-53 standard, it is important to retain the following aspects:

- NIST SP 800-53 Controls are organized in 20 families;
- Each family contains specific security and privacy controls, in a total of 320 controls;
- Families of controls contains base controls and control enhancements. Control enhancements add functionality or specificity to the base control. The use of control enhancements always requires the use of the base control;
- Security and privacy controls have the following structure:
  - Base Control Section;
  - Discussion Section;
  - Related Controls Section;
  - Control Enhancements Section;
  - Reference Section.

4.2.2 ISO/IEC 15408

The ISO/IEC 15408 - Information Technology - Security Techniques - Evaluation criteria for IT Security is composed by three parts:

- Part 1 - Introduction and General Model;
- Part 2 - Security Functional Components;
- Part 3 - Security Assurance Components.

The ISO/IEC 15408 provides "a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software" (ISO, 2009).

This standard represents a useful guide for development, evaluation and/or procurement of IT products with security functionality (ISO, 2009).

I) ISO/IEC 15408 Part 1 - Introduction and General Model

The first part of ISO/IEC 15408 standard "establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products" (ISO, 2009). This part:

- Describes the various parts of the standard;
- Defines the terms and abbreviations used;
- Establishes the core concept of o Target of Evaluation (TOE)[1];
- Establishes the evaluation context and describes its audience;
- Introduces the basic concepts necessary for evaluation of IT products.

Part 1 of ISO/IEC 15408 identifies four types of target audience: consumers, developers. evaluators, and others.

Related to the general model of ISO/IEC 15408 it is important to retain the following (ISO, 2009):

- Assets are entities that someone places values such as, for example, the content of a file server, the availability of an electronic commerce process or a local area network;
- Countermeasures protects the assets from threats that can compromise the confidentiality, integrity or availability of these assets. The countermeasures can be sufficient or correct;
- There are four types of permitted operations: iteration, assignment, selection, and refinement.

[1]Examples of TOE includes: a software application; an operating system; a smart card integrated circuit; a local area network; a database, among others.

II) ISO/IEC 15408 Part 2 - Security Functional Components

Security functional components, "are the basis for the security functional requirements expressed in a Protection Profile (PP) or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP or an ST. These requirements describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the IT or by the IT response to stimulus" (ISO, 2008a).

Related to the part 2 of ISO/IEC 15408, it is important to retain the following (ISO, 2008a):

- This represents a catalog of security functional components that can be specified for a TOE;
- TOE evaluation should ensure that a defined set of security functional requirements (SFRs) are enforced by the TOE resources;
- The SFRs may define multiple Security Function Policies (SFPs) that represents the rules that certain TOE must enforce. Each SFP must specify its scope of control;
- TOE Security Functionality (TSF) are the portions of a TOE that must be relied on for the correct enforcement of the SFRs;
- TSF Interface (TSFI) defines the boundaries of the TOE functionality that provide for the enforcement of the SFRs;
- The functional requirements of ISO/IEC 15408 are expressed in classes, families, and components;
- Each functional class includes a class name, class introduction, and one or more functional families;
- Each functional family includes a family name, family behavior, component levelling, management, audit, and one or more components;
- Each component includes a component identification, dependencies, and one or more functional elements.

III) ISO/IEC 15408 Part 3 - Security Assurance Components

Security assurance components, "are the basis for the security assurance requirements expressed in a Protection Profile (PP) or a Security Target (ST). These requirements establish a standard way of

expressing the assurance requirements for TOEs. This part of ISO/IEC 15408 catalogs the set of assurance components, families and classes" (ISO, 2008b).

This part of ISO/IEC 15408 includes the Evaluation Assurance Levels (EALs) that defines a scale for measuring assurance for component TOE, the Composed Assurance Packages (CAPs) that define a scale for measuring assurance for composed TOEs (ISO, 2008b).

Related to the part 3 of ISO/IEC 15408, it is important to retain the following (ISO, 2008b):

- This defines the assurance requirements and EALs that define a scale for measuring assurance;
- The assurance components of ISO/IEC 15408 are expressed in classes, families, and components;
- Each assurance class includes a class name, class introduction, and one or more assurance families;
- Each assurance family includes a family name, objectives, component levelling, application notes, and one or more assurance components;
- Each assurance component includes a component identification, objectives, application notes, dependencies, and one or more assurance elements;
- Each EAL includes an EAL name, objectives, application notes, and one or more assurance components;
- There are seven defined EALs:
  - EAL1 - Functionally tested;
  - EAL2 - Structurally tested;
  - EAL3 - Methodically tested and checked;
  - EAL4 - Methodically designed, tested, and reviewed;
  - EAL5 - Semiformally designed and tested;
  - EAL6 - Semiformally verified design and tested;
  - EAL7 - Formally verified design and tested.
- Each CAP includes a CAP name, objectives, application note, and one or more assurance components;
- There are three defined CAPs:

- CAP-A - Structurally composed;
- CAP-B - Methodically composed;
- CAP-C - Methodically composed, tested and reviewed.

4.2.3 ISO/IEC 18405

The ISO/IEC 18405 - Information Technology - Security Techniques - Methodology for IT Security Evaluation standard is a companion document to the ISO/IEC 15408 standard and defines the minimum actions to be "performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408" (ISO, 2008c).

Related to the core structure of the ISO/IEC 18405 standard it is important to retain the following aspects:

- It describes the general evaluation tasks:
  - Each evaluation, follows the same process, and has four evaluation common tasks: input task, output task, evaluation sub-activities, and the demonstration of the technical competence to the evaluation authority task;
  - The evaluator shall provide and Evaluation Technical Report (ETR) to justify the verdicts for each PP evaluation or TOE evaluation;
- It addresses the work necessary to reach an evaluation result on a PP;
- It defines the evaluation activities, organized by Assurance Classes:
  - For each assurance class and families defined in the ISO/IEC 15408 standard, this standard defines the evaluation activities. Each evaluation contains:
    * Objectives - the objectives of the activity;
    * Input - the evaluation evidence;
    * Action - the evaluator action element;
    * Work Units - the most granular level of the evaluation work.

4.2.4 ISO/IEC 27001

The ISO/IEC 27001 - Information Technology - Security Techniques - Information Security Management Systems - Requirements Standard provides a set of "requirements for establishing, implementing, maintaining and continually improving an information security management systems". This Standard also includes "requirements for the assessment and treatment of information security risks tailored to the needs of the organization" (ISO, 2013a).

The specified requirements are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

Related to the core structure of the ISO/IEC 27001 standard it is important to retain the following aspects:

- ISO/IEC 27001 Requirements are organized in seven groups;
- Each group contains the requirements related to the general requirement in a total of 22 requirements.

4.2.5 ISO/IEC 27002

The ISO/IEC 27002 - Information Technology - Security Techniques - Code of practice for information security controls Standard is "designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System based on ISO/IEC 27001 or as a guidance document for organizations implementing commonly accepted information security controls" (ISO, 2013b).

Related to the core structure of the ISO/IEC 27002 standard, it is important to retain the following aspects:

- ISO/IEC 27002 contains 14 security control clauses;
- Each clause contains one or more security categories in a total of 35 categories;
- Each control category contains a control objective and one or more controls in a total of 114 controls.

4.3 Design of the Framework Proposal Core

After the fulfillment of the Frameworks analysis in Section 4.1 and Standards analysis in Section 4.2 of this document, it was time to define the core structure of the Framework Proposal under development. To do that it was selected some characteristics founded in the previous Frameworks analysis. Those characteristics were documented in the previous Table 5 in Subsection 4.1.6 of this document.

4.3.1 Selected Granularity

The selected granularity for this Framework Proposal was the requirement. Due to the complexity and lack of time, it was decided not to lower the granularity to the control level. The validation of a Framework whose granularity is in the control level demands a large amount of time that it is not available in this kind of scientific research.

4.3.2 Selected Layers

CIS Controls and PSR were the Frameworks that serve as basis for this selection because, in both of them the controls or requirements are divided into layers. This layering allows a better understating of the control or requirement target.

Transposing to Remote Patient Monitoring (RPM) Devices, and because these devices are part of RPM Systems that also are Integrated Systems, it was decided that the layers of the Framework Proposal are the assets. These assets are:

- Device (DEV) - the piece of hardware (e.g. sensor or microprocessor) that collects, process, store and/or transmit the collected data from a patient;
- Communication (COM) - the used means of communication to transmit the collected data (e.g. Bluetooth or Wi-Fi);
- Data (DAT) - the collected data from a patient (e.g. Heart Rate, or Blood Glucose Level);
- Interface (INT) - the piece of software or hardware that allows health personal to collect and/or view the collected data from a patient;
- User (USE) - the person (e.g. physician or nurse) that has the access to the interface and the patient data.

4.3.3 Selected Segregation

Due to the fact that there are many kinds of RPM Devices and Systems in the market and the trend is for this number to grow as can be seen in section 2 of this document, it is easy to understand that it is very difficult to produce one solution that fits all devices and systems.

It was decided to use a segregation approach such as used in the CIS Controls and NIST Framework for Improving Critical Infrastructure Cybersecurity frameworks.

The first defined segregation was between active and passive RPM Devices. An active device is a device that is constantly and actively collecting data such as, for example, a Heart Rate Sensor. A passive device is a device that only collects data on demand such as, for example, a Blood Glucose Sensor that is triggered by an interface.

The second defined segregation was between RPM Devices with and without memory. It is easily understood that the security requirements for a device with memory are different from those defined for a device without memory. For example, in case of loss of an RPM device with memory, it is very important to ensure that data are encrypted or at least anonymized to ensure patient confidentiality.

Finally, the last segregation was between contactless and wired RPM devices. The security requirements for a device that uses contactless means of communication such as Wi-Fi or Bluetooth are different from those defined for a device that transmits its data through a cable.

To conclude, with this three segregation levels it was defined eight implementation groups to know:

- A1.1 - RPM Wired Active Devices without Memory - Devices that actively collects the patient information without the ability to store the information and that has to be plugged to the interface to perform the transmission of data;
- A1.2 - RPM Contactless Active Devices without Memory - Devices that actively collects the patient information without the ability to store the information and that can transmit the patient data wireless (e.g. RFID, Bluetooth or Wi-Fi);
- A2.1 - RPM Wired Active Devices with Memory - Devices that actively collects the patient information with the ability to store the information and that has to be plugged to the interface to perform the transmission of data;
- A2.2 - RPM Contactless Active Devices with Memory - Devices that actively collects the patient information with the ability to store the information and that can transmit the patient data wireless (e.g. RFID, Bluetooth or Wi-Fi);

- P1.1 - RPM Wired Passive Devices without Memory - Devices that collects the patient information on demand without the ability to store the information and that has to be plugged to the interface to perform the transmission of data;
- P1.2 - RPM Contactless Passive Devices without Memory - Devices that collects the patient information on demand without the ability to store the information and that can transmit the patient data wireless (e.g. RFID, Bluetooth or Wi-Fi);
- P2.1 - RPM Wired Passive Devices with Memory - Devices that collects the patient information on demand with the ability to store the information and that has to be plug-in to the interface to perform the transmission of data;
- P2.2 - RPM Contactless Passive Devices with Memory - Devices that collects the patient information on demand with the ability to store the information and that can transmit the patient data wireless (e.g. RFID, Bluetooth or Wi-Fi).

For each requirement, was defined in which Implementations Group that requirement must be fulfilled.

4.3.4 Selected Functions

The identification of functions is common in several Security Frameworks. In this context, CIS Controls, ISM and NIST Framework for Improving Critical Infrastructure Cybersecurity identifies a set of functions. These functions are usually linked.

The selected requirement functions for this Framework Proposal are:

- Protect - requirements that ensures the implementation of the appropriate safeguards for the continuity of the critical activities and to mitigate the risks;
- Detect - requirements that ensures the implementation of the appropriate activities to identity the occurrence of cybersecurity events;
- Respond - requirements that ensures the implementation of the appropriate activities to take action regarding a detected cybersecurity incident;
- Recover - requirements that ensures the implementation of the appropriate activities to maintain and restore any capabilities or services that were impaired due to a cybersecurity incident.

4.3.5 Selected Requirements

From all studied frameworks and standards, it was selected one Standard and one Framework to provide the foundations for the selection and design of the requirements for this Framework Proposal. The selected standard was the ISO/IEC 15408 - Part 2 and the selected framework was the NIST Framework for Improving Critical Infrastructure Cybersecurity.

This selection was made based on the following aspects:

- The organizations that create the standard and the Framework namely ISO and NIST are recognized and accepted worldwide;
- The selected Standard and Framework are also recognized, accepted, and used worldwide;
- The level of detail founded in these documents allows the selection and the design of the requirements that fit on the desire to create a sector-specific and detailed Framework.

Next, it is presented all the selected and designed requirements aggregated by assets (Table 6). For each of them, it is presented his origin, the respective function(s), the justification for its pertinence in this context, and if it happens, the Implementation Groups from which the requirement is excluded and, the justification for his exclusion.

Table 6: Framework Proposal Requirement List by Asset

Asset	**Requirement**
Device (DEV)	DEV.REQ-1: Ensure replay detection DEV.REQ-2: Ensure fault tolerance DEV.REQ-3: Ensure resource allocation DEV.REQ-4: Ensure hardware integrity DEV.REQ-5: Ensure event data collection DEV.REQ-6: Ensure incident alert
Communication (COM)	COM.REQ-1: Ensure non-repudiation of origin and receipt COM.REQ-2: Ensure a trusted channel COM.REQ-3: Ensure a trusted path COM.REQ-4: Ensure network integrity
Continued on next page	

Asset	Requirement
	COM.REQ-5: Ensure monitorization of communications and unauthorized connections
Data (DAT)	DAT.REQ-1: Ensure data authentication DAT.REQ-2: Ensure data integrity DAT.REQ-3: Ensure data confidentiality DAT.REQ-4: Ensure data availability DAT.REQ-5: Ensure data protection at rest state and during transmission
Interface (INT)	INT.REQ-1: Ensure access policies INT.REQ-2: Ensure replay detection INT.REQ-3: Ensure limitation of multiple concurrent sessions INT.REQ-4: Ensure management of remote access INT.REQ-5: Ensure software integrity INT.REQ-6: Ensure incident alert INT.REQ-7: Ensure unauthorized users monitorization INT.REQ-8: Ensure management of user's attributes, functions, security attributes and data INT.REQ-9: Ensure users activity monitorization
User (USE)	USE.REQ-1: Ensure user authentication USE.REQ-2: Ensure control of authentication failures USE.REQ-3: Ensure session locking and termination USE.REQ-4: Ensure access history USE.REQ-5: Ensure training

- Asset: Device (DEV)

  - DEV.REQ-1: Ensure replay detection.

    Origin: ISO/IEC 15408 - Part 2 - FPT_RPL.

    Description: Ensure the detection of replay for messages, service requests or/and services responses and prevent it.

    Functions: Detect and Respond.

    Justification: According to Luan & Gligor (Luan & Gligor, 1990) service-request messages could be replayed by intruders to clients and servers. The detection of replayed messages is important for performance, reliability, and security reasons. Replayed messages may cause superfluous executions of programs. These executions could cause degradation in the performance and delay the access of clients to these programs (Luan & Gligor, 1990). In this context, the degradation of the performance of the device, due to a replay attack could limit the performance of the device and worse, could limit the transmission or access to the patient data.

  - DEV.REQ-2: Ensure fault tolerance.

    Origin: ISO/IEC 15408 - Part 2 - FRU_FLT.

    Description: Ensures that the device will maintain correct operation even in the event of failures.

    Functions: Respond and Recover.

    Justification: "Fault tolerance is the use of techniques to enable the continued delivery of services at an acceptable level of performance and safety after a design fault becomes active" (Torres-Pomales, 2000). One of the goals of the fault tolerance is to include safety features on the software and/or hardware (Torres-Pomales, 2000). In this context, is easy to understand the importance of fault tolerance in the RPM devices. It is important that they continue to perform their major activities nevertheless the hardware faults.

- DEV.REQ-3: Ensure resource allocation.

  Origin: ISO/IEC 15408 - Part 2 - FRU_RSA.

  Description: Ensure the control of resources to prevent a denial of service due the unauthorised monopolisation of resources.

  Functions: Protect.

  Justification: According to Lyu et al. (Lyu et al., n.d.) "reliability is a prime concern, and adequate test and resource allocation are therefore very important". An optimal resource allocation increases the overall system reliability (Lyu et al., n.d.). In this context, which is the collection of sensitive and critical data, it is very important that the device makes an optimal allocation of resources to preserve the reliability of the major activities.

- DEV.REQ-4: Ensure hardware integrity.

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.DS-8.

  Description: Ensure the use of integrity checking mechanisms to verify the device hardware integrity.

  Functions: Protect.

  Justification: The hardware integrity checking it is important to ensure the device security, and it is justified by Forler et al. (Forler et al., 2016) "At present, most attacks aiming to hijack digital devices focus on software but as the robustness of secure software will continue to increase, attacks will increasingly focus on hardware. Attacks based on hardware tampering by removing, adding or swapping one or more integrated circuits or other hardware components in a device or emulating such hardware components with an external device are known. It will therefore be increasingly important to verify device integrity at a hardware level. This is particularly the case where the integrity of the device is crucial to protect revenue streams, such as in conditional access systems, for example in television set-top boxes, or digital rights management, but also in all general purpose computing platforms such as personal computers and portable devices such as laptops, mobile phones, smart phones, tablets, etc, which are increasingly used for sensitive applications including privacy and security concerns, such as electronic banking or e-health. With the increasing connectivity of almost all everyday devices (internet of things), the need for hardware integrity checks will become pervasive".

- DEV.REQ-5: Ensure event data collection.

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.AE-3.

  Description: Ensure that event data are collected and correlated from multiple sources and sensors.

  Functions: Detect.

  Justification: "Most modern, high-performance processors have special, on-chip hardware that monitors processor performance. Data collected by this hardware provides performance information on applications, the operating system, and the processor" (Sprunt, 2002). "Resource utilization events let users monitor how often a processor uses certain resources (for example, the number of cycles spent using a floating-point divider)" (Sprunt, 2002). This information could be used either to increase the performance of future devices either to detect for example bad resource allocation.

  Exclusions: A1.1, A1.2, P1.1, and P1.2.

  Exclusion Justification: Devices without memory would not be able to store the collected data.

- DEV.REQ-6: Ensure incident alert.

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.AE-5.

  Description: Ensure that incident alert thresholds are established.

  Functions: Detect.

  Justification: A computer security incident "is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices" (Cichonski et al., 2012). According to these authors, attacks could compromise personal data, and it is critical to respond quickly and effectively (Cichonski et al., 2012). It is only possible to respond to a security incident if there is an efficient security incident alert.

  Exclusions: P1.1, P1.2, P2.1, and P2.2.

  Exclusion Justification: Passive devices only collect data on demand through the action of a person or another device and are not actively collecting data, so there is no need to fulfill this requirement.

- Asset: Communication (COM)

  - COM.REQ-1: Ensure non-repudiation of origin and receipt.

    Origin: : ISO/IEC 15408 - Part 2 - FCO_NRO and FCO_NRR.

    Description: Ensure that the originator of information (Device) cannot successfully deny having sent the information and that the recipient of the information (Interface and User) cannot successfully deny its reception.

    Functions: Protect

    Justification: According to Coffey & Saidha (Coffey & Saidha, 1996) "Non-repudiation allows an exchange of data between two principals in such a manner that the principals cannot subsequently deny their participation in the exchange". Repudiation is the negation by one of the entities involved in an exchange of messages of having participated in all or part of that communication. Non-repudiation is all about preventing such a denial (Coffey & Saidha, 1996). In this context, non-repudiation is important to ensure that either the device either the interface/user could deny having exchange patient information.

  - COM.REQ-2: Ensure a trusted channel.

    Origin: ISO/IEC 15408 - Part 2 - FTP_ITC.

    Description: Ensure the creation of a trusted channel between the device and the Interface and/or User for the performance of security critical operations.

    Functions: Protect

    Justification: Agreeing with Akram et al. (Akram et al., 2016), a trusted channel "is a secure channel that is cryptographically bounded to the current state of the communication parties" either they are software or hardware. Several protocols allow the creation and maintenance of trusted channels such as Transport Layer Security (TLS) protocols and Secure Sockets Layer (SSL) protocols (Akram et al., 2016). The maintenance of this secure channel during the transmission of messages between the device and the interface/user is very important to ensure the confidentiality and integrity of the messages.

    Exclusions: A1.1, A2.1, P1.1, and P2.1.

    Exclusion Justification: These implementations groups contain devices that only exchange data when connected through a cable, so this requirement is not applicable.

- COM.REQ-3: Ensure a trusted path.

  Origin: ISO/IEC 15408 - Part 2 - FTP_TRP.

  Description: Ensure the establishment and maintenance of a trusted communication path to or from the Device and Interface/Users.

  Functions: Protect

  Justification: "A trusted path is a protected channel that assures the secrecy and authenticity of data transfers between a user's input/output (I/O) device and a program trusted by that user" (Zhou et al., 2012). Contrary to the previous requirement this is very important even to wired devices. According to Zhou et al. "Without a trusted path, an adversary could surreptitiously obtain sensitive user-input data by recording keystrokes, modify user commands to corrupt application program operation, and display unauthentic program output to an unsuspecting user to trigger incorrect user action".

- COM.REQ-4: Ensure network integrity.

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.AC-5.

  Description: Ensure the protection of the network integrity.

  Functions: Protect

  Justification: Networks faces several security issues such as viruses, spam, network intrusions, and denial-of-service attacks. These are some examples of the threats that can adversely affect a network (IT Direct, 2012). Network integrity is related to the definition of integrity itself, namely the quality of being sound, complete, and incorruptible (IT Direct, 2012). The network integrity could be ensured by mechanisms that prevent data from becoming lost, garbled, or modified without authorization (IT Direct, 2012) and this is the major aspect for this requirement to be ensured.

  Exclusions: A1.1, A2.1, P1.1, and P2.1.

  Exclusion Justification: These implementations groups contain devices that do not have the ability to connect to networks.

- COM.REQ-5: Ensure monitorization of communications and unauthorized connections.

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.CM-1 and DE.CM-7.

  Description: Ensure that the communications between the Devices and Interfaces/Users are monitored to detect potential cybersecurity events and that unauthorized connections are detected.

  Functions: Detect.

  Justification: "Network monitoring describes systems that continuously monitors the whole network topology for jamming, slowing down or failing components" (Rahmi Hamid et al., 2017) and to detect unauthorized connections. The access of unauthorized users or devices to the network could endanger the maintenance of the confidentiality, integrity, and availability of the transmitted data.

  Exclusions: A1.1, A2.1, P1.1, and P2.1.

  Exclusion Justification: These implementations groups contain devices that do not have the ability to connect to networks.

- Asset: Data (DAT)

  - DAT.REQ-1: Ensure data authentication.

    Origin: ISO/IEC 15408 - Part 2 - FDP_DAU.

    Description: Ensure authenticity of data stored or transmitted from the Device providing a guarantee of the validity of the information.

    Functions: Protect.

    Justification: Steinebach & Dittmann (Steinebach & Dittmann, 2003) claim that there have been a recent interest in data authentication in order to ensure an increase in data integrity. To the authors "data manipulation has become more and more simple and undetectable by the human audible and visual system due to technology advances in recent years" (Steinebach & Dittmann, 2003). This is an important aspect in favor of the importance of ensure the data authenticity. Data authentication is nothing more than the ability of detect the origin of the data and data alterations.

- DAT.REQ-2: Ensure data integrity.

  Origin: ISO/IEC 15408 - Part 2 - FDP_SDI, FDP_UIT, FPT_ITI, and NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.DS-6.

  Description: Ensure integrity of data stored or transmitted from the Device providing a guarantee that the information was not tampered.

  Functions: Protect.

  Justification: In agreeing with Samonas & Coss, (Samonas & Coss, 2014) for almost forty years that the terms of confidentiality, integrity, and availability have been widely used in Information Security practices. These three concepts refer originally to the fundamental elements of security controls in Information Systems. There are several security practices focused on technical controls that protect the confidentiality, integrity, and availability of information (Samonas & Coss, 2014). That is the main reason for the existence of this requirement. Data integrity is a basis for information security and should be fulfilled.

- DAT.REQ-3: Ensure data confidentiality.

  Origin: ISO/IEC 15408 - Part 2 - FDP_UCT and FTP_ITC.

  Description: Ensure confidentiality of data stored or transmitted from the Device providing a guarantee that the information was not accessible to unauthorized Interfaces/Users.

  Functions: Detect.

  Justification: The justification for the existence of this requirement is the same presented in the previous requirement.

- DAT.REQ-4: Ensure data availability.

  Origin: ISO/IEC 15408 - Part 2 - FPT_ITA, and NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.DS-4.

  Description: Ensure the prevention of loss of availability of data stored or transmitted from the Device.

  Functions: Protect.

  Justification: The justification for the existence of this requirement is the same presented for the requirement entitled ”Ensure data integrity”.

- DAT.REQ-5: Ensure data protection at rest state and during transmission.

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.DS-1 and PR.DS.

  Description: Ensure that data, in a rest state and during transmission, is protected.

  Functions: Protect.

  Justification: Agreeing with Warren, J. (Warren, n.d.) data transmission threats come in many ways. In an unsecured transmission, an eavesdropper could intercept, read, manipulate, and impersonate the data stream. This is the reason why the quality of data transmission security chosen should protect sensitive and unclassified data (Warren, n.d.). This is the case of the health information of the monitored patient.

- Asset: Interface (INT)

  - INT.REQ-1: Ensure access policies.

    Origin: : ISO/IEC 15408 - Part 2 - FDP_ACC, FMT_REV, FMT_SRM, NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.AC-1, PR.AC-4, and PR.AC-7.

    Description: Ensure that identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. Ensure that users, devices, and other assets are authenticated.

    Functions: Protect.

    Justification: According to Samarati & De Capitani Di Vimercati (Samarati & De Capitani Di Vimercati, 2001), an important requirement of any Information System is to protect data and resources against unauthorized disclosure or improper modifications, and, at the same time ensure their availability to users. Access control is the process of "mediating every request to resources and data maintained by a system and determining whether the request should be granted or denied" (Samarati & De Capitani Di Vimercati, 2001). The access control decision is enforced by a mechanism implementing regulation established by a security access policy (Samarati & De Capitani Di Vimercati, 2001). Finally, "enforcing protection, therefore, requires that every access to a system and its resources be controlled and that all and only authorized accesses can take place". Due to all of these facts and the fact that these interfaces receive sensitive patient data, access policies should be granted.

- INT.REQ-2: Ensure replay detection.

  Origin: ISO/IEC 15408 - Part 2 - FPT_RPL.

  Description: Ensure the detection of replay for messages, service requests or/and services responses and prevent it.

  Functions: Detect and Respond.

  Justification: According to Luan & Gligor (Luan & Gligor, 1990) service-request messages could be replayed by intruders to clients and servers. The detection of replayed messages is important for performance, reliability, and security reasons. Replayed messages may cause superfluous executions of programs. These executions could cause degradation in the performance and delay the access of clients to these programs (Luan & Gligor, 1990). In this context, the degradation of the performance of the device, due to a replay attack could limit the performance of the device and worse, could limit the access of patient data.

- INT.REQ-3: Ensure limitation of multiple concurrent sessions.

  Origin: ISO/IEC 15408 - Part 2 - FTA_MCS.

  Description: Ensure the limitation on the number of concurrent sessions that belong to the same user.

  Functions: Protect.

  Justification: According to Mylrea et. al, multiple concurrent sessions should not be allowed using the same authentication credentials (Mylrea et al., 2019). The danger of allowing multiple concurrent sessions are real. According to Tyagi (Tyagi, 2018), it is a recommendation that applications do not allow a user to have more than one active session at a time and that the application should expire previous sessions when a new authentication occurs. To the author, an attacker could use stolen credentials to access the system and the user does not know. Malicious software could create a denial of service through the creation of numerous concurrent sessions (Tyagi, 2018). In this particular context, the limitation of multiple concurrent sessions is important to detect attempts of unauthorized access and attempts of denial of service.

- INT.REQ-4: Ensure management of remote access.

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.AC-3.

  Description: Ensure the management and control of remote access to the Interface.

  Functions: Protect.

  Justification: Remote access technologies allow access to protected resources from external networks and external hosts and place a higher risk than similar technologies only accessed from inside the organization (Scarfone et al., 2009). It is important that "remote access solutions, including client devices, remote access servers, and internal resources accessed through remote access, should be secured against expected threats, as identified through threat models" (Scarfone et al., 2009). Remote access to the interface and patient data could be very useful to the healthcare professionals, but for the presented reasons such accesses should be managed to mitigate the associated security risks.

- INT.REQ-5: Ensure software integrity

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.DS-6.

  Description: Ensure the use of integrity checking mechanisms to verify the software integrity.

  Functions: Protect.

  Justification: In agreeing with Chen et al., (Chen et al., 2002) "tamper-resistance techniques traditionally took advantage of software and hardware-specific features that were often undocumented. Unfortunately, special features are invariably limited in quantity and unchangeable over time. Typically, it did not take long before an unrelenting hacker uncovered the "trick" and completely defeated the protection". Software integrity checking is one of the main weapons used against software tampering (Chen et al., 2002). This is the main reason for the existence of this requirement.

- INT.REQ-6: Ensure incident alert

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.AE-5.

  Description: Ensure that incident alert thresholds are established.

  Functions: Detect.

  Justification: A computer security incident "is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices" (Cichonski et al., 2012). According to these authors, attacks could compromise personal data, and it is critical to respond quickly and effectively (Cichonski et al., 2012). It is only possible to respond to a security incident if there is an efficient security incident alert.

- INT.REQ-7: Ensure unauthorized users monitorization.

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.CM-7.

  Description: Ensure that the access to unauthorized users are monitored.

  Functions: Detect.

  Justification: To Peterson, (Peterson, 2004), "a strong information security program will include a variety of technical and administrative controls designed to prevent intrusions and unauthorized activities from both internal and external threat agents". In this particular scenario where we exchange sensitive data, the interface should monitor the existence of unauthorized access to the system.

- INT.REQ-8: Ensure management of user's attributes, functions, security attributes and data.

  Origin: ISO/IEC 15408 - Part 2 - FIA_ATD, FMT_MOF, FMT_MSA, and FMT_MTD.

  Description: Ensure that authenticated users have only access to authorized functions, attributes, and data in agreement with the user's profile and roles.

  Functions: Protect.

  Justification: Attribute-Based Access Control is a model that controls access to objects by evaluating rules against the attributes of the entities and the environment relevant to a request. (Hu et al., 2013). Leveraging consistently defined attributes, authentication, and authorization activities can be executed and administered in the same or separate infrastructures while maintaining appropriate levels of security (Hu et al., 2013). This model and the definition of the correct attributes, functions to users improve the quality of the security level of the RPM System.

- INT.REQ-9: Ensure users activity monitorization

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.CM-3.

  Description: Ensure that users activity is monitored to detect potential cybersecurity events.

  Functions: Detect.

  Justification: According to Lord (Lord, 2018), the "purpose of user activity monitoring is to protect information while ensuring availability and compliance with data privacy and security regulations". The goal of any user activity monitoring program "should be to find and filter out actionable information that's vulnerable in data protection efforts". In the healthcare context, this gains more importance because we are dealing with sensitive data.

- Asset: User (USE)

  - USE.REQ-1: Ensure user authentication.

    Origin: : ISO/IEC 15408 - Part 2 - FIA_UAU.

    Description: Ensure secure user authentication mechanisms.

    Functions: Protect.

    Justification: According to Townsend (Townsend, 2020) "Controlling access is the basis of all security. The right people should be allowed in, and the wrong people kept out. This is done by confirming – or authenticating – the identity of the person seeking access, and then checking that the person is authorized to enter". This is the basis of any application that has access to sensitive data and that only certain users have access to it, and in this context, such need is also verified.

  - USE.REQ-2: Ensure control of authentication failures.

    Origin: ISO/IEC 15408 - Part 2 - FIA_AFL.

    Description: Ensure control of authentication attempts and limit the number of unsuccessful attempts to prevent brute force attacks.

    Functions: Protect, Detect and Respond.

    Justification: "The most obvious way to block brute-force attacks is to simply lock out accounts after a defined number of incorrect password attempts. Account lockouts can last a specific duration, such as one hour, or the accounts could remain locked until manually unlocked by an administrator" (Sowmya & Naveen Kumar, 2013). This is an important

technique and easy to implement and that could prevent brute-force attacks and consequently leak of sensitive data to unauthorized users.

- USE.REQ-3: Ensure session locking and termination.

  Origin: ISO/IEC 15408 - Part 2 - FTA_SSL.

  Description: Ensure the ability to user to initiate, lock, unlock and terminate session and the ability to system to lock and/or terminate session in case of long inactivity detected.

  Functions: Protect, Detect and Respond.

  Justification: "Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined" (NIST, n.d.-a). In contrast, "session termination terminates all processes associated with a user's logical session. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use" (NIST, n.d.-b). These are two requirements that increase the level of security of the overall system and protect the patient sensitive data.

- USE.REQ-4: Ensure access history.

  Origin: ISO/IEC 15408 - Part 2 - FTA_TAH.

  Description: Ensure the ability to display to a user, upon successfully session establishment, a history of successful and unsuccessful attempts to access the user's account.

  Functions: Protect.

  Justification: Access to the history of successful and unsuccessful attempts to log in to the system plays an important role in security. In agree with (Saleem, 2019) checking the access history is important to know if someone has accessed or tried to access the system.

- USE.REQ-5: Ensure training.

  Origin: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.AT-1 and PR.AT-2.

  Description: Ensure that all users are informed and trained and that privileged users understands their roles and responsibilities.

  Functions: Protect.

  Justification: According to Hight (Hight, 2005), security training programs are designed to reduce the number of security breaches that occur through a lack of user awareness. Yet, to the author, education and training are crucial to security management practices. (Hight, 2005). Training programs "reduces the risk of people making mistakes and causing problems that affect everyone in the organization" (Hight, 2005). In this particular case, the lack of training and awareness of healthcare professionals could endanger the patient sensitive data.

4.3.6 Selected Document Structure

The selected document structure for the Framework Proposal was the structure used on ISO Standards such as ISO/IEC 27001 and 27002. ISO standards are widely known and used all over the world. A document with the same structure facilitates the adoption and understanding of its users. The structure of the document is composed by:

- Foreword: a small note about the origin and some brief disclaimers about the Framework Proposal;
- Introduction: an introduction about the Framework Proposal itself, its objectives and structure;
- Remote Patient Monitoring Devices Security Assessment Framework
  - Scope: the main goal of the Framework Proposal;
  - Normative Reference: the list of Standards and Frameworks used and needed to complement this Framework Proposal;
  - Acronyms: the list of used Acronyms;
  - Core Structure: the core structure and explanation of the Framework Proposal.
- Appendices: important appendices to the document.

4.3.7 Artifacts

In the next sections, are presented all the produced artifacts during the execution of this scientific research.

I) Framework Proposal

The most relevant produced artifact in this scientific work is the Framework Proposal that summarizes all the presented aspects in Section 4.3 of this document. Figure 12 intends to schematically represent the Framework Proposal core. In the vertical rows, it can be seen the distribution of requirements by assets of the Framework namely: Device, Communication, Data, Interface, and User. In the horizontal row, for each Implementation Group, and for each Asset is declared how many requirements should be fulfilled. The final column of the horizontal rows defines the minimum and maximum score that each Implementation Group could achieve. Finally, at the bottom of the figure are represented the four functions that each Requirement could have, which are: Protect, Detect, Respond, and Recover.

In Appendix A can be found the whole document of the Framework Proposal.

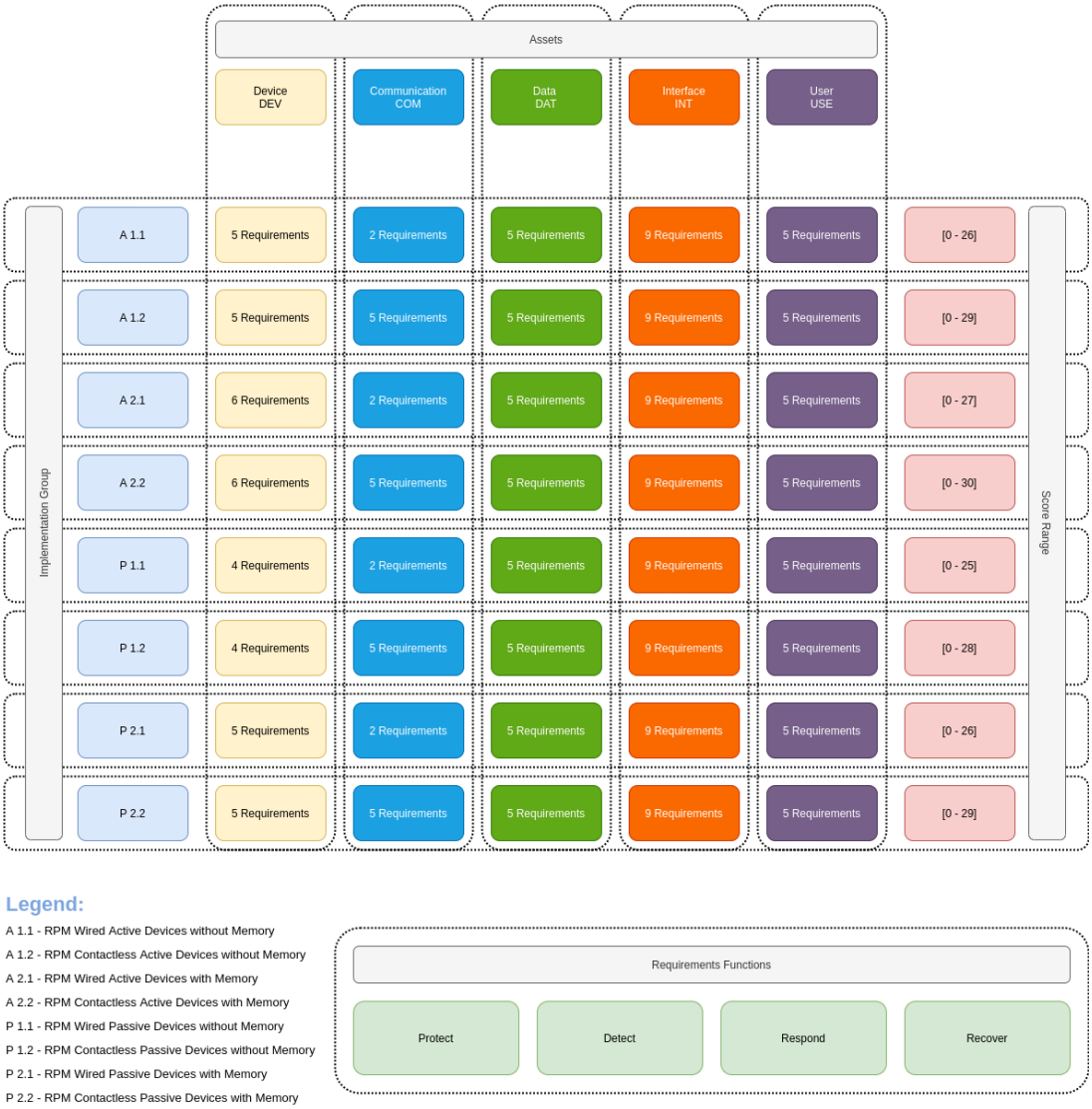


Figure 12: Framework Proposal Core

II) RPM Device System Simulator and Security Assessment

To perform a validation of the Framework Proposal it was created an RPM Device System Simulator as a proof-of-concept. The Framework Proposal was applied to the Simulator and, after this implementation it was obtained a Security Assessment of such Simulator.

In Subsection 4.3.8 can be found all the details about the RPM Device System Simulator and in Appendix B can be found the Security Assessment that was performed on the simulator.

III) Website

Although it cannot be considered an artifact it was also developed a website. The website compiles the information about this Framework Proposal and promotes them (Figure: 13). The website is online and accessible through this URL: https://joaoferreira.eu/rpm/. It is also possible to perform an RPM Device Security Assessment using the presented Framework Proposal (Figure: 14, 15, and 16). This assessment could be done through the "Try Now" option. The source code can be requested to the author through the email joaoferreira@joaoferreira.eu.

The main objective of the website is the publication and materialization of the Framework Proposal in something simple, informative, practical, and easy to use, that can be assessable for everyone and everywhere.

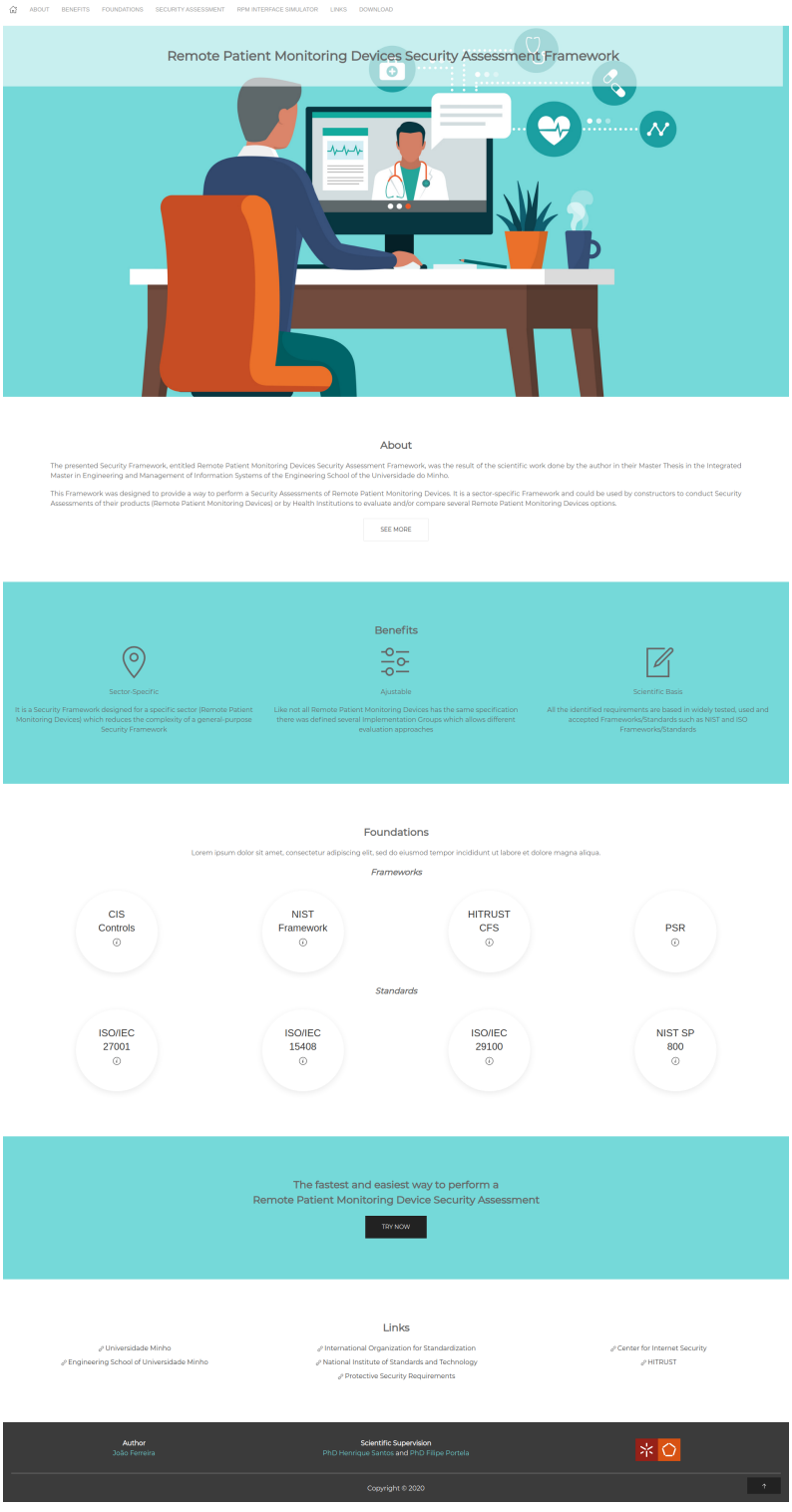


Figure 13: Website Screenshot

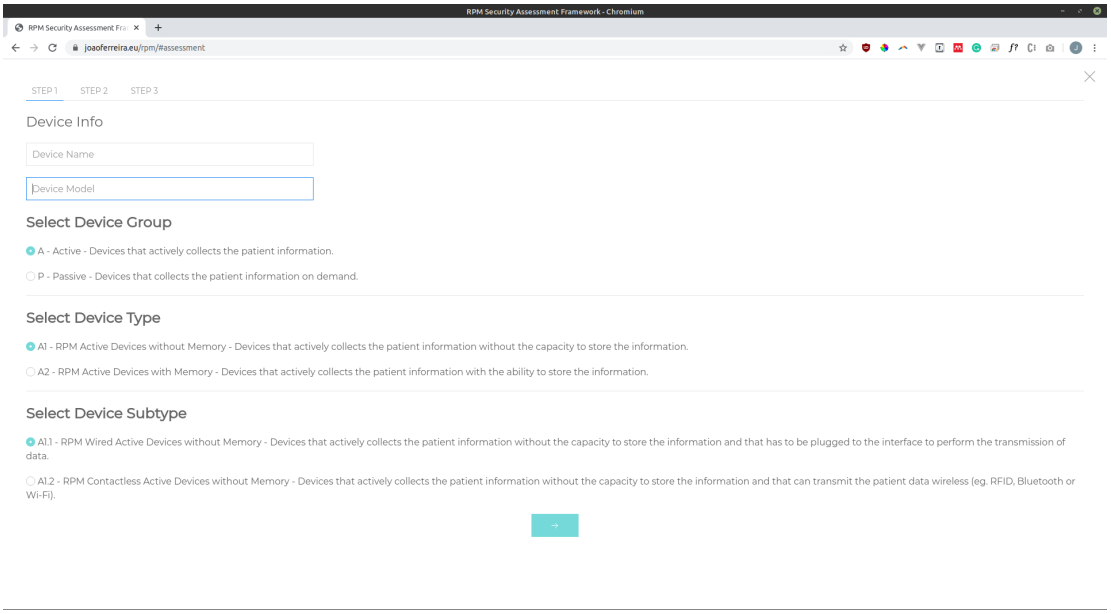


Figure 14: Online Security Assessment - Stage 1

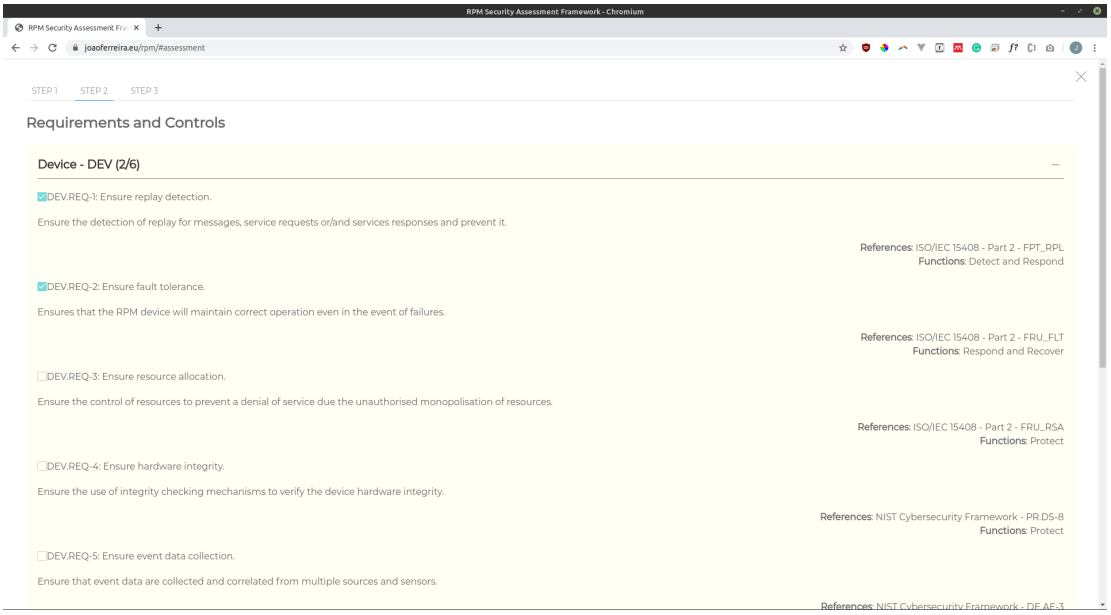


Figure 15: Online Security Assessment - Stage 2

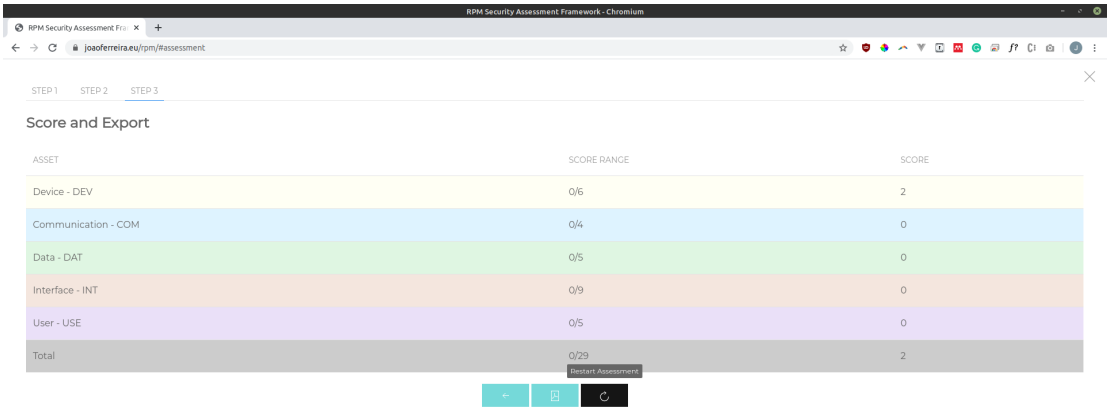


Figure 16: Online Security Assessment - Stage 3

4.3.8 Framework Validation - Proof of Concept

In order to perform a validation of the Framework Proposal and in the absence of a real RPM Device System it was developed a simulator. This RPM Device System Simulator is composed by all the assets covered by the Framework Proposal, that is: Device, Communication, Data, Interface, and User.

- **The Device:** to simulate an RPM Device, it was used a Heart Rate Analogic Sensor for Arduinos (Figure 11) and a NodeMCU Micro-controller with an ESP8266 Wi-Fi Module (Figure 10). The two combined running a small c++ application, in agreement with the Framework Proposal classification, creates an A.1.2 - RPM Contactless Active Devices without Memory Device Simulator (Figure 17). The source code can be requested to the author through the email joaoferreira@joaoferreira.eu.
- **Communications:** the fact that the NodeMCU Micro-controller comes with an ESP8266 Wi-Fi Module allows that all the communication goes through an Internet connection, and it was used HTTPS instead of HTTP connections.
- **Data:** all the data collected is stored in a MySQL Database.
- **Interface:** the interface simulator has two components. The frontend developed in HTML, CSS, and JavaScript and allows users to see patient information, and the backend developed in NodeJS is responsible for getting and store the patient information. The frontend is accessible through the URL: https://joaoferreira.eu/rpm/rpm_interface.html (Figure 18, 19, and 20) and the backend is

stored in the Heroku App Engine provider. The source code can be requested to the author through the email joaoferreira@joaoferreira.eu.

- **User:** the users can access to patient information through the interface. It was used username and password authentication through JSON Web Tokens emission.

Table 7 summarizes all the characteristics of the environment test, the RPM Device System Simulator.

Table 7: RPM Device System Simulator Specifications

Assets	**Description**
Device	Heart Rate Analogic Sensor and NodeMCU Micro-controller (Figure 17). The source code can be requested to the author through the email joao-ferreira@joaoferreira.eu.
Communication	ESP8266 Wi-Fi Module and HTTPS connections
Data	MySQL Database
Interface	Frontend (Figure 18, 19, 20) in HTML, CSS and JS and running on https://joaoferreira.eu/rpm/rpm_interface.html Backend in Node.JS and running in Heroku. The source code can be requested to the author through the email joaoferreira@joaoferreira.eu.
User	Authentication with username and password through Json Web Tokens emission

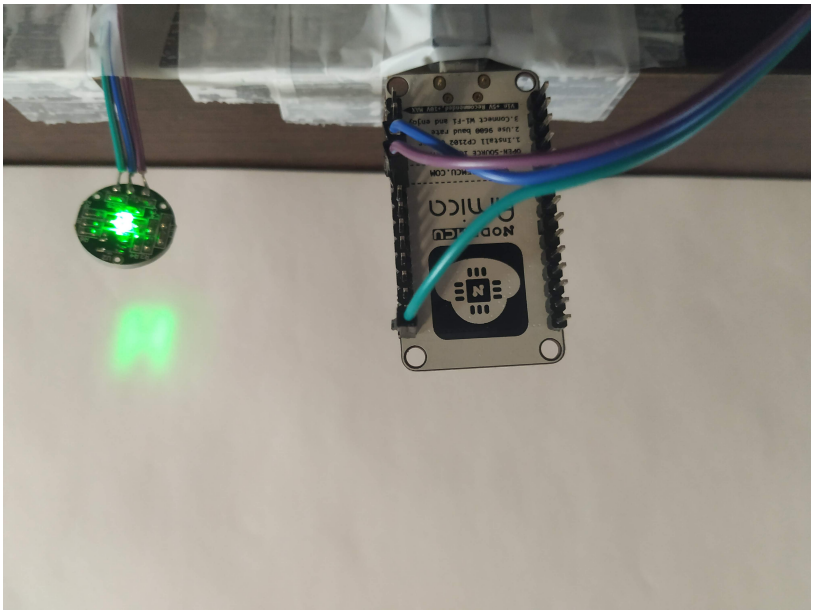


Figure 17: RPM Contactless Active Devices without Memory Device Simulator

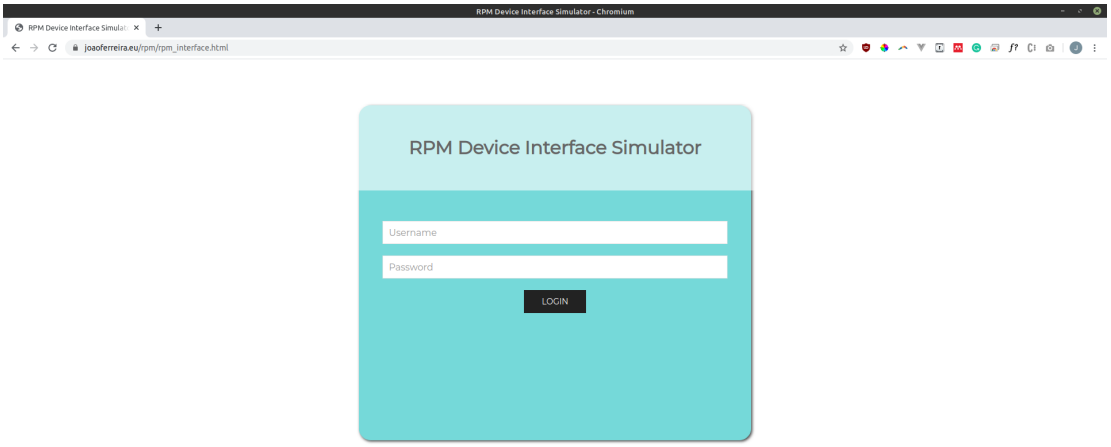


Figure 18: RPM Device Interface Simulator - Login

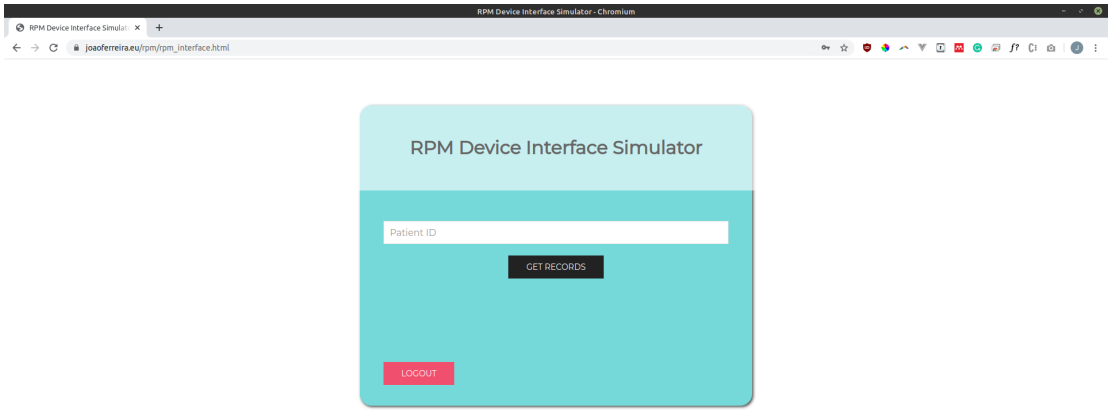


Figure 19: RPM Device Interface Simulator - Get Patient

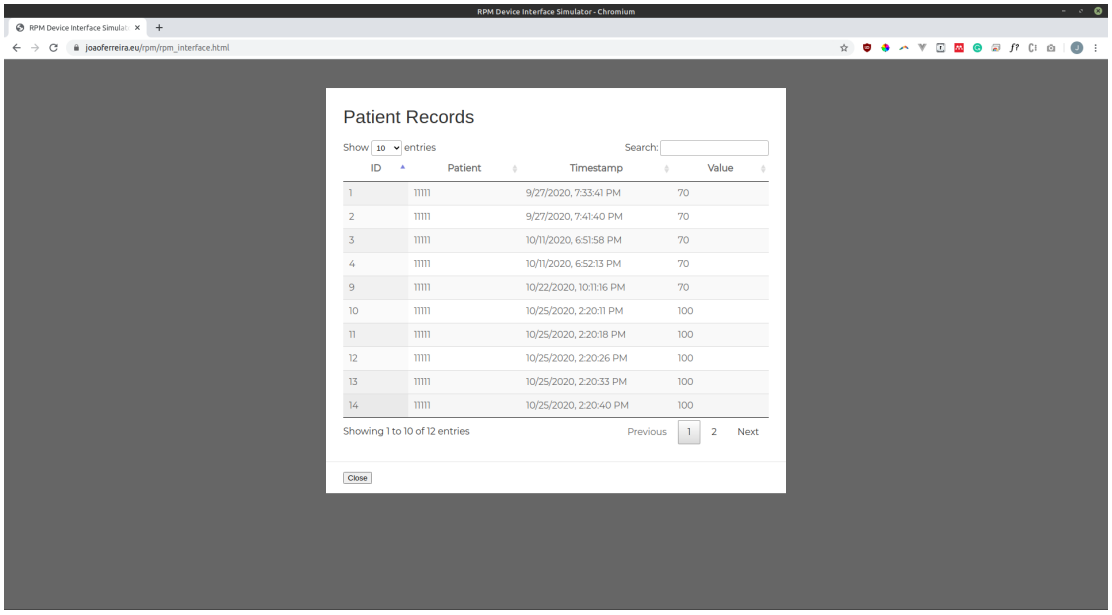


Figure 20: RPM Device Interface Simulator - Patient Data

Information Flow: Periodically the Heart Rate Sensor sends a Hypertext Transfer Protocol Secure (HTTPS) request to the backend with the Heart Rate value (number 1 of Figure 21). The backend is responsible for saving that information on the Database (number 2 of Figure 21). To access the patient information the user has to perform a login to the Interface (number 3 of Figure 21). Through an HTTPS request performed by the interface (number 4 of figure 25) and through a validation of the user (number 5 of Figure 21) the user is authenticated and the interface receives an authentication token. The user can

now access patient information (number 6 of Figure 21). The interface makes another HTTPS request to the backend to get the patient data (number 7 of Figure 21). The backend has the responsibility of validating if the patient is valid and if the user has clearance to access that patient information. If the users obtains clearance to see the patient data, the backend loads the patient information (number 8 of Figure 21) and sends it to the interface in the HTTPS response.

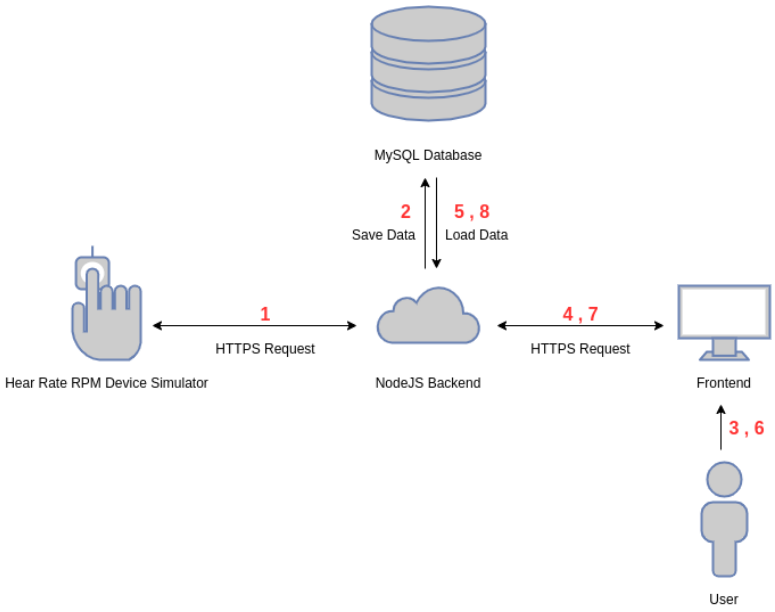


Figure 21: RPM Device System Simulator - Architecture and Flow

It is time to perform a Security Assessment using the Framework proposal. The system obtains a score of 9 fulfilled requirements in a total of 29 requirements. Detailing the score by the asset, the score is distributed in the following way (Table 8):

Table 8: Framework Validation - RPM Device System Simulator Security Assessment Result

Assets	**Number of Possible Requirements**	**Number of Fulfil Requirements**	**Score**
Device (DEV)	5	0	0/5
Communication (COM)	5	2	2/5
Data (DAT)	5	4	4/5
Interface (INT)	9	2	2/9
User (USE)	5	1	1/5
Total	29	9	9/29

In Appendix B can be found the full report of the Security Assessment of the RPM Device System Simulator.

I) Discussion of Results

As can be easily concluded and according to the Framework Proposal this is not a very secure system by the following aspects:

- The Device does not fulfill any of the requirements (0 requirements in 5 possible). It is not protected against replay attacks, does not ensure fault tolerance or resource allocation, does not verify the hardware integrity, and does not ensure incident alert;
- In the realm of Communication, the system ensures a secure channel and a secure path because it is used HTTPS instead of HTTP (2 requirements in 5 possible) but does not ensure non-repudiation of origin or receipt, does not ensure network integrity neither the monitorization of communications and unauthorized connections;
- The Data is the asset that is more protected. It is guaranteed that the authentication, confidentiality, availability is fulfilled and that the data is protected in the rest state (4 requirements in 5 possible). The only requirement that is not fulfilled is the guarantee of the data integrity because it is not used any kind of integrity check;
- In the Interface, the only requirements that are fulfilled are the guarantee of access policies and the management of users attributes, functions, security attributes, and data (2 requirements in 9 possible). Each user has only access to their patients. The replay detection, the limitation of concurrent sessions, the management of remote access, the software integrity, the incident alert, and the users activity monitorization is not fulfilled;
- In the realm of the User Asset it is the guarantee that only authenticated users can access the system (1 requirement in 5 possible) but there is no control of authentication failures, there is no guarantee of session locking or termination after a certain period, there is no history of access and, because it is only a simulator and not a real system, it was not provided training to users.

II) Benefits for Healthcare Sector

As a major contribution to the Healthcare sector, this work offers a sector-specific Security Framework based on the best and worldwide adopted Standards and Frameworks. The Framework Proposal is adjusted to the RPM reality and intends to respond to their specific needs in terms of security.

RPM Devices are increasing and every day more and more patients are covered by this kind of telemedicine. But everyday new and more efficient attacks are performed and new vulnerabilities are detected. The use of this kind of Framework by manufacturers would certainly improve the overall security of the RPM Devices and Systems and more importantly, would increase the overall security of the patient integrity and data.

The use of this Framework by Healthcare professionals would allow them to make a more wisely and informed choice related to the selection of the RPM devices to use with their patients.

III) Framework Proposal Benchmark

In Table 9 can be found a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of the Framework Proposal. The Strengths are positive aspects and the Weaknesses are negative aspects. Both of them are concerned with the internal environment. Opportunities and Threats relates to the external environment. Opportunities are positive aspects and Threats are negative.

Table 9: Framework Proposal SWOT Analysis

	Positive Aspects	**Negative Aspects**
Internal Environment	**Strengths** It is a specific-sector Framework. Based in widely known and accepted Standards and Frameworks. Provide a graphical user interface to apply the Framework. Provide a score range to easily compare results.	**Weaknesses** Lack of validation with real RPM Devices Systems. Lack of the control layer. This fact places some subjectivity in the security assessment,
External Environment	**Opportunities** Increase of detected vulnerabilities in RPM Devices Systems. Increase in the number of RPM Devices Systems in the market and patients using them.	**Threats** It is a new born Framework competing with widely used and accepted Standards and Frameworks. Having been based on other Frameworks and Standards, if this Framework does not follow their changes it can become obsolete.

5 Conclusion

In this section of the document, are presented the major conclusions obtained during the development of this scientific work.

5.1 Critical Reflection

At the beginning of this scientific research, it was defined two major objectives. One of them was to propose a sector-specific Security Framework to apply to Remote Patient Monitoring Devices Systems. The other was to validate that same proposal. Related to these two objectives, I can conclude that these two objectives were fulfilled.

The proposed Security Framework is based on the best practices followed by the most important and widely spread Standards and Frameworks such as ISO/IEC 27000 series, ISO/IEC 15408, NIST Framework for Improving Critical Infrastructure Cybersecurity, and Center for Internet Security (CIS) Controls. This increases the confidence level in the proposal.

The proposed Security Framework has focused on the Remote Patient Monitoring Devices (RPM) Systems itself which creates a sector-specific Security Framework. This increases the guarantee that all the requirements are specific for that field.

The Framework Proposal was divided into 5 assets. Each asset contains several requirements in a total of 30 requirements. Each requirement has one or more functions. There are 4 distinct functions available. It was identified 8 distinct implementation groups. For each implementation group, it was defined which security requirements must be fulfilled for each asset.

To perceive if this Security Framework can be used in the real world it was developed a simulator to validate the Framework. It was concluded that this Security Framework could be used in real systems and covers a wide range of security issues.

Finally and based on that, the use of this Security Framework in the evaluation and construction of Remote Patient Monitoring Device Systems could improve the overall System Security.

The secondary objectives that were defined at the beginning of this scientific research cannot be measure now, because they only can be perceived in the future.

In table 10 could be found a matrix that correlates each of the defined objectives with the results obtained with this scientific work.

Back to the research question that was “Could a sector-specific Security Framework improve the security of Remote Patient Monitoring Devices Systems?”, my answer is yes. With the use of the Framework

Proposal, which is, a sector-specific framework, it could be easily detected which vulnerabilities the device has. The Framework Proposal could be used by manufacturers to solve the detected vulnerabilities and improve the overall security of the device or could be used by healthcare professionals to measure the security of the used RPM devices and create mitigation strategies to protect the sensitive data of patients.

Table 10: Relationship between objectives and results

<table>
<tr><th>Objectives</th><th>Framework Proposal</th><th>RPM Device System Simulator</th><th>RPM Device System Simulator Security Assessment</th></tr>
<tr><td>Propose a sector-specific Security Framework to apply on Remote Patient Monitoring Devices Systems</td><td>The Framework Proposal responds entirely to this objective</td><td></td><td></td></tr>
<tr><td>Validate the proposed sector-specific Security Framework</td><td></td><td colspan="2">Creates a proof-of-concept for the validation of the Framework Proposal with an RPM Device System Simulator</td></tr>
<tr><td>Encourage researchers to pursue similar scientific researches and, in the process, identify solutions to the problems found</td><td colspan="3">All of the results could be an inspiration for other researchers to pursuit similar scientific investigations</td></tr>
<tr><td>Inform manufacturers about the need of using sector-specific frameworks to improve the security of their products</td><td>The Framework Proposal could alert manufacturers for the need for a sector-specific Frameworks</td><td></td><td></td></tr>
<tr><td>Inform the healthcare society about the importance of measure security of Remote Patient Monitoring Devices Systems</td><td colspan="3">All the results could alert the healthcare society for the need of measure the security of such sensitive data collection devices</td></tr>
</table>

To guide this scientific research the Design Science Research (DSR) was chosen as a methodological approach. The DSR proves to be efficient in the guidance of this kind of works.

Related to the phases of this method, the only that is under conclusion and is not reflected in this document, is the communication phase. The communication phase will be concluded with the publication of the scientific paper in the scientific community.

During the execution of this scientific work it was developed three artifacts. The first is this document. It intends to be the glue and the explanation of all the components of this scientific research.

The second and maybe, the most important artifact is the Security Framework proposal document. It represents the result of all the realized activities during this work. The document has an ISO/IEC structure. This structure was chosen because is one of the most know structures in the world and will help people who want to use this Framework because they are more familiar with them.

The third artifact is composed of a Remote Patient Monitoring Device System simulator about which it was performed a security assessment using the Security Framework proposal. This represents the validation of the Framework.

A better validation could be performed using a real Remote Patient Monitoring System, but, because of the limitations imposed by Covid-19, it was impossible to find some partner to provide this kind of systems.

Although it could not be considered an artifact, it was also created a website. This website intends to be a facilitator in the process of communication, explanation, and adoption in the future of this Security Framework. On the website, it is also possible to perform a digital security assessment using the Framework. This is something unusual in the realm of Security Standards and Frameworks.

5.2 Risk Analysis

For this work, it was identified several risks that could compromise the execution and delivery of this scientific research. In Table 11, could be found the identified risks. In the verified risks, it is described which strategy was used to mitigate the risk.

Table 11: Risk Analysis

Risk	P	I	S	Consequences	Verified	Mitigation
Lack of available remote monitoring devices in the selected critical area (health)	4	5	20	This can compromise the fulfilment of the objectives of this project since there are no devices to validate the Framework.	Yes	Due to Covid-19, it was not possible to find a partnership in the healthcare sector to provide a real RPM system. To mitigate the risk it was developed an RPM Device System Simulator to enable the assessment of such a system to perform the validation of the Framework Proposal.
Non-compliance with the objective and expected results	2	4	8	This compromises the quality of the project artifacts.	No	
Lack of communication with supervisors	1	4	4	This can compromise the correct interpretation of the obtained results and quality of the artifacts.	No	
Ineffective planning	1	4	4	This can delay the delivery of the artifacts as well as decrease its quality.	No	

Continued on next page

Risk	P	I	S	Consequences	Verified	Mitigation
Loss of files	1	4	4	This can compromise the timely delivery of the artifacts and force repetition of some activities.	No	
Breakdown of machines or devices	1	3	3	This can put in danger the timely delivery of the artifacts.	No	
High complexity of this science research	3	3	9	This can compromise the timely delivery of the artifacts.	Yes	The creation of a Framework Proposal detailed to the control level demands much time to develop, so, to prevent the delay in the fulfillment of this scientific work it was decided to create a Framework Proposal only with requirements.

5.3 Future Work

This work fulfills all the objectives that were initially proposed but more has to be done to harness the full potential of the Security Framework proposal.

First, it is important that to be accepted by the scientific community, manufacturers, and healthcare society, this framework needs to be validated with real Remote Patient Monitoring Devices Systems. Only with this validation, we can conclude that it responds to real security concerns and improves the security of such systems.

Secondly, it could be very important to add to this framework another layer, that is, the control layer. To increase the level of coverage of this Framework the control layer must be added. For each of the defined requirements could be defined a set of controls that must be fulfilled. The controls could, by one

hand, help manufacturers to construct their systems more secure, and, on the other hand, help evaluators in the assessment of such devices.

The control layer was set aside in this project due to its complexity. The time needed to include all needed controls and justify them was increasing higher than the available time for all the project.

This layer could be added, later, in a Thesis or in another scientific work based on this one.

Bibliography

Ahmed, R. K. A. (2016). Security Metrics and the Risks: An Overview. *International Journal of Computer Trends and Technology*, *41*(2), 106–112. https://doi.org/10.14445/22312803/ijctt-v41p119

Aizuddin, A. (2019). *The Common Criteria ISO/IEC 15408-The Insight, Some Thoughts, Questions and Issues* (tech. rep.). SANS Institute. United States.

Akram, R. N., Markantonakis, K., Mayes, K., Bonnefoi, P.-F., Sauveron, D., & Chaumette, S. (2016). *An Efficient, Secure and Trusted Channel Protocol for Avionics Wireless Networks* (tech. rep.).

Albrecht, J. P. (2016). How the GDPR Will Change the World. *European Data Protection Law Review (EDPL)*, *2*.

Aman, W., & Snekkenes, E. (2013). An Empirical Research on InfoSec Risk Management in IoT-based eHealth ASSET (Adaptive Security for Smart Internet of Things in eHealth)-asset.nr.no View project Automation of Software Security Testing and Assurance Evaluation View project An Empirical Research on InfoSec Risk Management in IoT-based eHealth. https://doi.org/10.13140/RG.2.1.4635.8245

Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practive* (2ª).

Australian Cyber Security Center. (2020). Australian Government Information Security Manual.

Benslimane, Y., Yang, Z., & Bahli, B. (2016). Information Security between Standards, Certifications and Technologies: An Empirical Study. http://iranarze.ir/wp-content/uploads/2017/08/7304-English-IranArze.pdf

Cassagnol, D. (2019). CTA Survey Finds High Demand for Remote Patient Monitoring Devices. https://www.cta.tech/News/Press-Releases/2019/April/CTA-Survey-Finds-High-Demand-for-Remote-Patient-Mo.aspx

Center for Internet Security. (2019). CIS Controls V7.1.

Check Point Software Technologies. (2019). *Cyber Attack Trends Analysis Report* (tech. rep.).

Chen, Y., Venkatesan, R., Cary, M., Pang, R., Sinha, S., & Jakubowski, M. H. (2002). *Oblivious Hashing: A Stealthy Software Integrity Verification Primitive* (tech. rep.).

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Coffey, T., & Saidha, P. (1996). *NON-REPUDIATION WITH MANDATORY PROOF OF RECEIPT* (tech. rep.).

Critical Software. (2019). https://criticalsoftware.com/

Cyber Experts. (2020). 23 Top Cybersecurity Frameworks. https://cyberexperts.com/cybersecurity-frameworks/

Darkins, A., & Cary, M. (2000). *Telemedicine and Telehealth: Principles, Policies, Performances and Pitfalls*. New York, Spinger Publishing Company, Inc.

Ecri Institute. (2019). *Executive Brief A Report from Health Devices* (tech. rep.). www.ecri.org/2019hazards,

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491–497. https://doi.org/10.1016/j.jare.2014.02.006

Eloff, J., & Eloff, M. (2003). *Information Security Management-A New Paradigm* (tech. rep.).

European Parliament and the Council, & of 27 April 2016. (2016). Regulation (EU) 2016/679 - General Data Protection Regulation. Official Journal of the European Union.

Feruza, S., & Tao-Hoon, K. (2007). *IT Security Review: Privacy, Protection, Access Control, Assurance and System Security* (tech. rep. No. 2). Hannam University. Daejeon.

Fong, B., Fong, A. C. M., & Li, C. K. (2011). *Telemedicine Technologies: Information Technologies in Medicine and Telehealth* (Wiley, Ed.; 1ª).

Forler, E., Borgeaud, J., & Seltzer, S. (2016). US20180367317 - HARDWARE INTEGRITY CHECK.

Gheorghiu, B., & Ratchford, F. (2015). Scaling up the use of remote patient monitoring in Canada, In *Studies in health technology and informatics*, IOS Press. https://doi.org/10.3233/978-1-61499-505-0-23

Goodwin, N. (2010). The state of telehealth and telecare in the UK: Prospects for integrated care. *Journal of Integrated Care*, *18*(6), 3–10. https://doi.org/10.5042/jic.2010.0646

Hale, T. M., Kvedar, J. C., Jl, H., & For, M. D. (2014). *IN THE LITERATURE Privacy and Security Concerns in Telehealth* (tech. rep.). www.virtualmentor.org

Hall, J. L., & Mcgraw, D. (2014). For Telehealth To Succeed, Privacy And Security Risks Must Be Identified And Addressed. *Health Affairs*, *33*(2). https://doi.org/10.1377/hlthaff.2013.0997

Hight, S. D. (2005). *The importance of a security, education, training and awareness program (November 2005)* (tech. rep.).

HITRUST. (2019a). HITRUST CFS Version 9.3.1.

HITRUST. (2019b). Intorduction to the HITRUST CFS.

Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2013). *NIST Special Publication 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)* (tech. rep.). http://csrc.nist.gov/publications.

Idaho National Laboratory. (2005). *A Comparison of Cross-Sector Cyber Security Standards* (tech. rep.).

Infosecurity Magazine. (2019). The Most Influential Security Frameworks of All Time. https://www.infosecurity-magazine.com/opinions/most-influential-frameworks-1-1-1/

ISO. (2008a). ISO/IEC 15408-2:2008 - Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components. https://www.iso.org/standard/46414.html

ISO. (2008b). ISO/IEC 15408-3:2008 - Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components. https://www.iso.org/standard/46413.html

ISO. (2008c). ISO/IEC 18045:2008 - Information technology — Security techniques — Methodology for IT security evaluation. https://www.iso.org/standard/46412.html

ISO. (2009). ISO/IEC 15408-1:2009 - Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model. https://www.iso.org/standard/50341.html

ISO. (2013a). ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/standard/54534.html

ISO. (2013b). ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls. https://www.iso.org/standard/54533.html

ISO. (2018). *ISO/IEC 27000:2018* (tech. rep.). ISO/IEC. Switzerland. www.iso.org

IT Direct. (2012). Network Security and Preserving Network Integrity. https://www.gettingyouconnected.com/network-security-and-preserving-network-integrity/

IT Governance USA Blog. (2019). Top 4 cybersecurity frameworks. https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks

Lord, N. (2018). What is User Activity Monitoring? How It Works, Benefits, Best Practices, and More | Digital Guardian. https://digitalguardian.com/blog/what-user-activity-monitoring-how-it-works-benefits-best-practices-and-more

Lovelace Jr., B. (2019). FDA issues warning on medical devices that are vulnerable to cyberattacks. https://www.cnbc.com/2019/10/01/fda-issues-warning-on-medical-devices-that-are-vulnerable-to-cyberattacks.html

Luan, S.-W., & Gligor, V. D. (1990). *On Replay Detection in Distributed Systems* (tech. rep.).

Luna, S. V. (1999). *Planejamento de Pesquisa* (educ, Ed.; 1ª). São Paulo.

Lyu, M. R., Rangarajan, S., & Van Moorsel, A. P. A. (n.d.). *Optimal Allocation of Testing Resources for Software Reliability Growth Modeling in Component-Based Software Development* (tech. rep.).

Malasinghe, L. P., Ramzan, N., & Dahal, ·. K. (2019). Remote patient monitoring: a comprehensive study, *10*, 57–76. https://doi.org/10.1007/s12652-017-0598-x

Mylrea, M., Rotondo, J., & Gourisetti, S. N. G. (2019). Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities. https://www.osti.gov/servlets/purl/1514261

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity.

National Institute of Standards and Technology. (2020a). NIST SP 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

National Institute of Standards and Technology. (2020b). NIST SP 800-53 - Security and Privacy Controls for Information Systems and Organizations.

NEJM Catalyst. (2018). What is Telehealth? https://catalyst.nejm.org/what-is-telehealth/

Newman, L. H. (2017). Medical Devices Are the Next Security Nightmare | WIRED. https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

NIST. (n.d.-a). NVD - Control - AC-11 - SESSION LOCK. https://nvd.nist.gov/800-53/Rev4/control/AC-11

NIST. (n.d.-b). NVD - Control - AC-12 - SESSION TERMINATION. https://nvd.nist.gov/800-53/Rev4/control/AC-12

Olanrewaju, R. F., Ali, N., Khalifa, O., Manaf, A., Ali, B., Khalifa, O., & Manaf, A. A. (2013). *ICT in Telemedicine: Conquering Privacy and Security Issues In Health Care Services* (tech. rep. No. 1).

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *J. Manage. Inf. Syst.*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Peltier, T., Peltier, J., & Blackley, J. (2005). *Information Security Fundamentals* (1st Edition). Florida, Aurbach Publications.

Peterson, D. (2004). *Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks* (tech. rep.). www.isa.org

Portela, C. (2013). *Pervasive Intelligent Decicion Suport in Critical Health Care* (Doctoral dissertation). Universidade do Minho.

Protective Security Requirements. (n.d.). Protectiong our people, information, and assets - what you need to know.

Rahmi Hamid, I. A., Hatun Ab Sukor, N., Feresa Mohd Foozy, C., & Abdullah, Z. (2017). *NETWORK MONITORING SYSTEM TO DETECT UNAUTHORIZED CONNECTION* (tech. rep.). http://www.actaelectronicamalaysia.com

Rao, U. H., & Nayak, U. (2014). *The InfoSec Handbook - An Introduction to Information Security*. California, Apress, Berkeley, CA. https://doi.org/https://doi.org/10.1007/978-1-4302-6383-8

Saleem, H. (2019). Check Successful or Failed Windows Login Attempts. https://www.groovypost.com/howto/check-windows-logon-events-windows-8/

Samarati, P., & De Capitani Di Vimercati, S. (2001). *Access Control: Policies, Models, and Mechanisms* (tech. rep.). http//homes.dsi.unimi.it/%E2%88%BCsamaratihttp//www.ing.unibs.it/%E2%88%BCdecapita

Samonas, S., & Coss, D. (2014). *THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY* (tech. rep.). www.jissec.org

Sanger, L. J. (2009). *HIPAA Goes HITECH* (tech. rep.). http://www.hhs.gov/ocr/

Scarfone, K., Hoffman, P., & Souppaya, M. (2009). *Guide to Enterprise Telework and Remote Access Security* (tech. rep.). https://csrc.nist.rip/library/alt-SP800-46r1.pdf

Solove, D. (2008). *Understanding Privacy* (tech. rep.). http://ssrn.com/abstract=1127888

Sowmya, G., & Naveen Kumar, A. (2013). BRUTE FORCE ATTACK – BLOCKING TECHNIQUE. *International Journal Of Engineering And Computer Science*, *2*(8). http://103.53.42.157/index.php/ijecs/article/view/1810/1674

Sprunt, B. (2002). *The Basics of Performance Monitoring Hardware* (tech. rep.). https://pdfs.semanticscholar.org/76f8/168135dfa76e9f5b296421d0493913af6a30.pdf

Statista. (2019a). U.S. data breaches and exposed records 2018 | Statista. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Statista. (2019b). U.S. data breaches by industry 2018 | Statista. https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/

Steinebach, M., & Dittmann, J. (2003). *Watermarking-Based Digital Audio Data Authentication* (tech. rep.).

Sturmer, J., & Branley, A. (2017). Thousands of Australians could have pacemakers being recalled in US over hacking risk - ABC News (Australian Broadcasting Corporation). https://www.abc.net.au/news/2017-08-31/pacemakers-recall-hacking-risk-australians-could-have-them/8860368

Symantec. (2018). *ISTR Internet Security Threat Report* (tech. rep.).

Tang, Z., Weavind, L., Mazabob, J., Thomas, E. J., Ming, ; Chu-Weininger, Y. L., & Johnson, T. R. (2007). Workflow in intensive care unit remote monitoring: A time-and-motion study*. *Crit Care Med*, *35*(9). https://doi.org/10.1097/01.CCM.0000281516.84767.96

Torres-Pomales, W. (2000). *Software Fault Tolerance: A Tutorial* (tech. rep.). http://www.sti.nasa.gov

Townsend, K. (2020). The Importance of Authentication | Avast. https://blog.avast.com/the-importance-of-authentication-avast

Tuckson, R. V., Edmunds, M., & Hodgkins, M. L. (2017). Telehealth. *New England Journal of Medicine*, *377*(16), 1585–1592. https://doi.org/10.1056/NEJMsr1503323

Tyagi, R. (2018). Prevent Multiple Concurrent Logins in Codeigniter | Lucideus Research. https://blog.lucideus.com/2018/03/prevent-multiple-concurrent-logins-in.html

Warren, J. (n.d.). *THALES E-SECURITY THALES E-SECURITY Data Transmission Security: Securing the Blurry Line between Classified and Unclassified Data* (tech. rep.).

Wilkinson, T., & Reinhardt, R. (2015). Technology in Counselor Education: HIPAA and HITECH as Best Practice. *The Professional Counselor*, *5*(3), 407–418. https://doi.org/10.15241/tw.5.3.407

World Health Organization Regional Office for Europe. (2016). *FROM INNOVATION TO IMPLEMENTATION eHealth in the WHO European Region*. http://www.euro.who.int/en/ehealth

Zhou, Z., Gligor, V. D., Newsome, J., & Mccune, J. M. (2012). Building Verifiable Trusted Path on Commodity x86 Computers. https://doi.org/10.1109/SP.2012.42

Appendices

A Framework Proposal Document

SECURITY FRAMEWORK

REMOTE PATIENT MONITORING DEVICES SECURITY ASSESSMENT FRAMEWORK

First Edition

2020-10

Author

João Ferreira

Scientific Supervision

PhD Henrique Santos

PhD Carlos Filipe Portela

Universidade do Minho
Escola de Engenharia

Contents

1 Foreword

The presented Security Framework, entitled Remote Patient Monitoring Devices Security Assessment Framework, was the result of the scientific work done by the author in his Masters Dissertation in the Integrated Master in Engineering and Management of Information Systems of the Engineering School of the Universidade do Minho.

This work was done under the supervision of the PhD Henrique Santos and PhD Carlos Filipe Portela, both, professors in the Engineering School of the Universidade do Minho.

Has disclaimer it is important to advise the readers that this is a proposal for a possible Security Framework that allows the Security Assessment of Remote Patient Monitoring Devices Systems, and it was done in an academic scope.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

2 Introduction

This Security Framework was designed to provide a way to perform a Security Assessment of Remote Patient Monitoring Devices Systems. It is a sector-specific Framework and could be used by constructors to conduct Security Assessments of their products (Remote Patient Monitoring Devices Systems) or by Health Institutions to evaluate and/or compare several Remote Patient Monitoring Device Systems options.

In this Framework could be found a list of Requirements that should be fulfilled in order to be considered secures. Not all systems demands the fulfillment of all Requirements, so the Frameworks distinct several Implementation Groups and identifies which Security Requirements are expected to be fulfilled for that group.

This Framework also segregates the Requirements into Assets. It was identified five important Assets, namely: Device (DEV), Communication (COM), Data (DAT), Interface (INT), and User (USE). For each of these Assets was defined a set of specific Requirements that should be fulfilled to effectively protect that asset.

Each of the identified Requirement is based in one or more known Frameworks/Standards. This ensures the quality and relevance of the Requirement and conducts the evaluator to their origins. It is recommended that the evaluator read the pointed reference to allow him to perform a better conclusion regarding the compliance of that Requirement for the Studied Remote Patient Monitoring Device System.

3 Remote Patient Monitoring Devices Security Assessment Framework

3.1 Scope

This Security Framework establishes a way to perform a Security Assessment of Remote Patient Monitoring Devices System through the identification of a set of Security Requirements that should be fulfilled to ensure that the system is secure.

3.2 Normative References

The following referenced documents served as the basis for the development and construction of this Security Framework. For a better understanding of the content of this document, the reading of these documents are advised.

- ISO/IEC 15408-1 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 1 - Introduction and General Model (ISO, 2009);
- ISO/IEC 15408-2 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 2 - Security Functional Components (ISO, 2008a);
- ISO/IEC 15408-3 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 3 Security Assurance Components (ISO, 2008b);
- ISO/IEC 18405 - Information Technology - Security Techniques - Methodology for IT Security Evaluation (ISO, 2008c);
- ISO/IEC 27001 Information Technology - Security Techniques - Information Security management Systems - Requirements (ISO, 2013a);
- ISO/IEC 27002 Information Technology - Security Techniques - Code of Practice for Information Security Controls (ISO, 2013b);
- NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations (National Institute of Standards and Technology, 2020);
- Center for Internet Security (CIS) Controls Framework V7.1 (Center for Internet Security, 2019);
- HITRUST Common Security Framework (CFS) V9.3.1 (HITRUST, 2019);

- Information Security Manual (ISM) (Australian Cyber Security Center, 2020);
- NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1 (National Institute of Standards and Technology, 2018);
- Protective Security Requirements (PSR) (Protective Security Requirements, n.d.);

3.3 Acronyms

- CIS - Center for Internet Security
- IEC - International Electrotechnical Commission
- ISM - Information Security Manual
- ISO - International Organization for Standardization
- IT - Information Technology
- NIST - National Institute of Standards and Technology
- PSR - Protective Security Requirements
- RPM - Remote Patient Monitoring
- SP - Special Publication

3.4 Core Structure

Figure 1 intends to schematically represent the Framework Core.

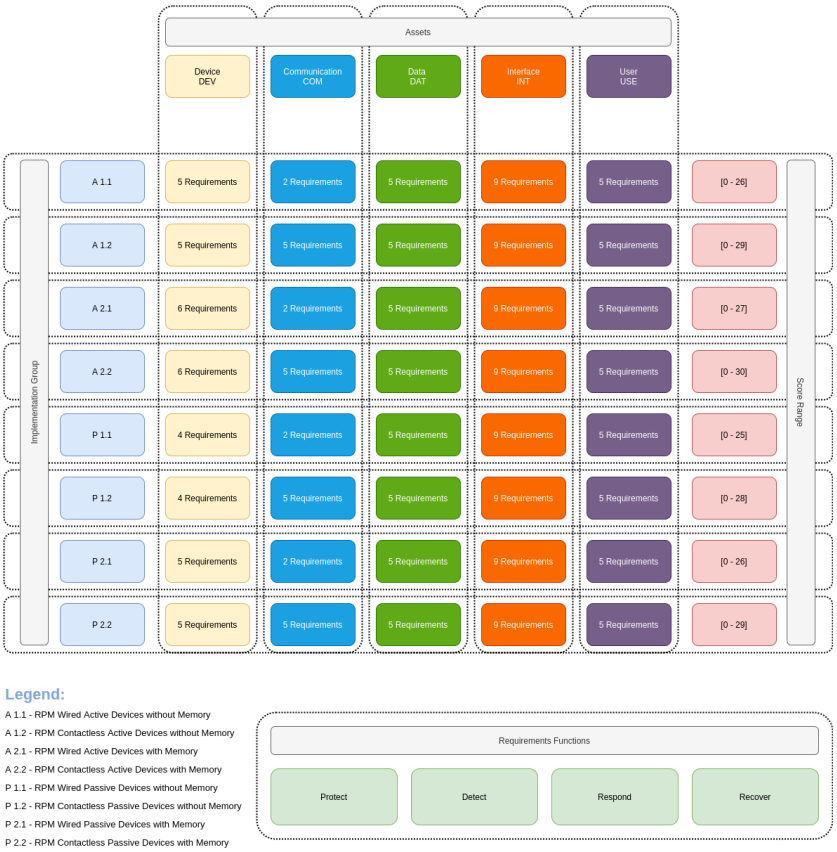


Figure 1: Framework Core

a) Assets Types

An asset could be a piece of software, hardware, or information that plays an important role in the evaluated Information Technology context. For this purpose, this Framework distinguishes five types of assets that will be subject to a security assessment, to know:

- **Device (DEV)** - the piece of hardware (e.g. sensor or microprocessor) that collects, process, store and/or transmit the collected data from a patient;
- **Communication (COM)** - the used means of communication to transmit the collected data (e.g. Bluetooth or Wi-Fi);
- **Data (DAT)** - the collected data from a patient (e.g. Heart Rate, or Blood Glucose Level);
- **Interface (INT)** - the piece of software or hardware that allows health personal to collect and/or view the collected data from a patient;
- **User (USE)** - the person (e.g. physician or nurse) that has access to the interface and the patient data.

b) Implementation Groups

There are several Remote Patient Monitoring Devices Systems in the market, and they are not all the same, so they can not be all evaluated in the same way. The Implementation Groups are categories of Devices based on similar characteristics. The Implementation Groups enables the possibility of performing a similar evaluation and perform a comparison of results. The defined Implementation Groups are:

- A - Active Devices:
  - A1 - RPM Active Devices without Memory:
    - A1.1 - RPM Wired Active Devices without Memory - Devices that actively collects the patient information without the ability to store the information and that has to be plugged to the interface to perform the transmission of data;
    - A1.2- RPM Contactless Active Devices without Memory - Devices that actively collects the patient information without the ability to store the information and that can transmit the patient data wireless (e.g. RFID, Bluetooth or Wi-Fi).
  - A2 - RPM Active Devices with Memory:
    - A2.1 - RPM Wired Active Devices with Memory - Devices that actively collects the patient information with the ability to store the information and that has to be plugged to the interface to perform the transmission of data;
    - A2.2 - RPM Contactless Active Devices with Memory - Devices that actively collects the patient information with the ability to store the information and that can transmit the patient data wireless (e.g. RFID, Bluetooth or Wi-Fi).
- P - Passive Devices:
  - P1 - RPM Passive Devices without Memory:
    - P1.1 - RPM Wired Passive Devices without Memory - Devices that collects the patient information on demand without the ability to store the information and that has to be plugged to the interface to perform the transmission of data;
    - P1.2 - RPM Contactless Passive Devices without Memory - Devices that collects the patient information on demand without the ability to store the information and that can transmit the patient data wireless (e.g. RFID, Bluetooth or Wi-Fi).
  - P2 - RPM Passive Devices with Memory:

* P2.1 - RPM Wired Passive Devices with Memory - Devices that collects the patient information on demand with the ability to store the information and that has to be plug-in to the interface to perform the transmission of data;
* P2.2 - RPM Contactless Passive Devices with Memory - Devices that collects the patient information on demand with the ability to store the information and that can transmit the patient data wireless (e.g. RFID, Bluetooth or Wi-Fi).

c) Functions

This framework defines four concurrent and continuous functions. Each requirement contains one or more specific function. These functions provide a high-level, strategic view of the requirement. The functions are:

- **Protect** - requirements that ensures the implementation of the appropriate safeguards for the continuity of the critical activities and to mitigate the risks;
- **Detect** - requirements that ensures the implementation of the appropriate activities to identify the occurrence of cybersecurity events;
- **Respond** - requirements that ensures the implementation of the appropriate activities to take action regarding a detected cybersecurity incident;
- **Recover** - requirements that ensures the implementation of the appropriate activities to maintain and restore any capabilities or services that were impaired due to a cybersecurity incident.

d) Requirements

- **Device - DEV**

  – **DEV.REQ-1**: Ensure replay detection

  Ensure the detection of replay for messages, service requests or/and services responses and prevent it.

  References: ISO/IEC 15408 - Part 2 - FPT_RPL

  Functions: Detect and Respond

  Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

  – **DEV.REQ-2**: Ensure fault tolerance

  Ensures that the device will maintain correct operation even in the event of failures.

  References: ISO/IEC 15408 - Part 2 - FRU_FLT

  Functions: Respond and Recover

  Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **DEV.REQ-3**: Ensure resource allocation

Ensure the control of resources to prevent a denial of service due the unauthorised monopolisation of resources.

References: ISO/IEC 15408 - Part 2 - FRU_RSA

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **DEV.REQ-4**: Ensure hardware integrity

Ensure the use of integrity checking mechanisms to verify the device hardware integrity.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.DS-8

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **DEV.REQ-5**: Ensure event data collection

Ensure that event data are collected and correlated from multiple sources and sensors.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.AE-3

Functions: Detect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
		X	X			X	X

– **DEV.REQ-6**: Ensure incident alert

Ensure that incident alert thresholds are established.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.AE-5

Functions: Detect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X				

- **Communication - COM**

  – **COM.REQ-1**: Ensure non-repudiation of origin and receipt

  Ensure that the originator of information (Device) cannot successfully deny having sent the information and that the recipient of the information (Interface and User) cannot successfully deny its reception.

  References: ISO/IEC 15408 - Part 2 - FCO_NRO and FCO_NRR

  Functions: Protect

  Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

  – **COM.REQ-2**: Ensure a trusted channel

  Ensure the creation of a trusted channel between the device and the Interface and/or User for the performance of security critical operations.

  References: ISO/IEC 15408 - Part 2 - FTP_ITC

  Functions: Protect

  Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
	X		X		X		X

– **COM.REQ-3**: Ensure a trusted path

Ensure the establishment and maintenance of a trusted communication path to or from the Device and Interface/Users.

References: ISO/IEC 15408 - Part 2 - FTP_TRP

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **COM.REQ-4**: Ensure network integrity

Ensure the protection of the network integrity.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.AC-5

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
	X		X		X		X

– **COM.REQ-5**: Ensure monitorization of communications and unauthorized connections
Ensure that the communications between the Devices and Interfaces/Users are monitored to detect potential cybersecurity events and that unauthorized connections are detected.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.CM-1 and DE.CM.7

Functions: Detect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
	X		X		X		X

- **Data - DAT**

  - **DAT.REQ-1**: Ensure data authentication

    Ensure authenticity of data stored or transmitted from the Device providing a guarantee of the validity of the information.

    References: ISO/IEC 15408 - Part 2 - FDP_DAU

    Functions: Protect

    Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

  - **DAT.REQ-2**: Ensure data integrity

    Ensure integrity of data stored or transmitted from the Device providing a guarantee that the information was not tampered.

    References: ISO/IEC 15408 - Part 2 - FDP_SDI, FDP_UIT, FPT_ITI, and NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.DS-6

    Functions: Protect

    Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **DAT.REQ-3**: Ensure data confidentiality

Ensure confidentiality of data stored or transmitted from the Device providing a guarantee that the information was not accessible to unauthorized Interfaces/Users.

References: ISO/IEC 15408 - Part 2 - FDP_UCT and FTP_ITC

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **DAT.REQ-4**: Ensure data availability

Ensure the prevention of loss of availability of data stored or transmitted from the Device.

References: ISO/IEC 15408 - Part 2 - FPT_ITA, and NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.DS-4

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **DAT.REQ-5**: Ensure data protection at rest state and during transmission

Ensure that data, in a rest state and during transmission, is protected.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.DS-1 and PR.DS-2

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

- **Interface - INT**

  - **INT.REQ-1**: Ensure access policies

    Ensure that identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. Ensure that users, devices, and other assets are authenticated.

    References: ISO/IEC 15408 - Part 2 - FDP_ACC, FMT_REV, FMT_SRM, NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.AC-1, PR.AC-4, and PR.AC-7

    Functions: Protect

    Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

  - **INT.REQ-2**: Ensure replay detection

    Ensure the detection of replay for messages, service requests or/and services responses and prevent it.

    References: ISO/IEC 15408 - Part 2 - FPT_RPL

    Functions: Detect and Respond

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **INT.REQ-3**: Ensure limitation of multiple concurrent sessions

Ensure the limitation on the number of concurrent sessions that belong to the same user.

References: ISO/IEC 15408 - Part 2 - FTA_MCS

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **INT.REQ-4**: Ensure management of remote access

Ensure the management and control of remote access to the Interface.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.AC-3

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **INT.REQ-5**: Ensure software integrity

Ensure the use of integrity checking mechanisms to verify the software integrity.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.DS-6

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **INT.REQ-6**: Ensure incident alert

Ensure that incident alert thresholds are established.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.AE-5

Functions: Detect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **INT.REQ-7**: Ensure unauthorized users monitorization

Ensure that the access to unauthorized users are monitored.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.CM-7

Functions: Detect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **INT.REQ-8**: Ensure management of user's attributes, functions, security attributes and data

Ensure that authenticated users have only access to authorized functions, attributes, and data in agreement with the user's profile and roles.

References: ISO/IEC 15408 - Part 2 - FIA_ATD, FMT_MOF, FMT_MSA, and FMT_MTD

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **INT.REQ-9**: Ensure users activity monitorization

Ensure that users activity is monitored to detect potential cybersecurity events.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - DE.CM-3

Functions: Detect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

- **User - USE**

  – **USE.REQ-1**: Ensure user authentication

  Ensure secure user authentication mechanisms.

  References: ISO/IEC 15408 - Part 2 - FIA_UAU

  Functions: Protect

  Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

  – **USE.REQ-2**: Ensure control of authentication failures

  Ensure control of authentication attempts and limit the number of unsuccessful attempts to prevent brute force attacks.

  References: ISO/IEC 15408 - Part 2 - FIA_AFL

  Functions: Protect, Detect and Respond

  Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **USE.REQ-3**: Ensure session locking and termination

Ensure the ability to user to initiate, lock, unlock and terminate session and the ability to system to lock and/or terminate session in case of long inactivity detected.

References: ISO/IEC 15408 - Part 2 - FTA_SSL

Functions: Protect, Detect and Respond

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **USE.REQ-4**: Ensure access history

Ensure the ability to display to a user, upon successfully session establishment, a history of successful and unsuccessful attempts to access the user's account.

References: ISO/IEC 15408 - Part 2 - FTA_TAH

Functions: Protect

Implementation Groups Applicability

A - Active				P - Passive			
A1		A2		P1		P2	
A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
X	X	X	X	X	X	X	X

– **USE.REQ-5**: Ensure training

Ensure that all users are informed and trained and that privileged users understands their roles and responsibilities.

References: NIST Framework for Improving Critical Infrastructure Cybersecurity - PR.AT-1 and PR.AT-2

Functions: Protect

Implementation Groups Applicability

A - Active				**P - Passive**			
A1		**A2**		**P1**		**P2**	
A1.1	**A1.2**	**A2.1**	**A2.2**	**P1.1**	**P1.2**	**P2.1**	**P2.2**
X	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Bibliography

Australian Cyber Security Center. (2020). Australian Government Information Security Manual.

Center for Internet Security. (2019). CIS Controls V7.1.

HITRUST. (2019). HITRUST CFS Version 9.3.1.

ISO. (2008a). ISO/IEC 15408-2:2008 - Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components. https://www.iso.org/standard/46414.html

ISO. (2008b). ISO/IEC 15408-3:2008 - Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components. https://www.iso.org/standard/46413.html

ISO. (2008c). ISO/IEC 18045:2008 - Information technology — Security techniques — Methodology for IT security evaluation. https://www.iso.org/standard/46412.html

ISO. (2009). ISO/IEC 15408-1:2009 - Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model. https://www.iso.org/standard/50341.html

ISO. (2013a). ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/standard/54534.html

ISO. (2013b). ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls. https://www.iso.org/standard/54533.html

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity.

National Institute of Standards and Technology. (2020). NIST SP 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

Protective Security Requirements. (n.d.). Overview of Protective Security Requirements - Protecting our people, information, and assets.

Appendices

Evaluation Sheet

The Sheet could be user as an example of a way to document a Remote Patient Monitoring Device Security Assessment Evaluation.

Device Name:

Device Model:

Evaluation Date:

Evaluator Name:

	A - Active				P - Passive			
	A1		A2		P1		P2	
Requirement	A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
DEV.REQ-1								
DEV.REQ-2								
DEV.REQ-3								
DEV.REQ-4								
DEV.REQ-5	NA	NA			NA	NA		
DEV.REQ-6					NA	NA	NA	NA
COM.REQ-1								
COM.REQ-2	NA		NA		NA		NA	
COM.REQ-3								
COM.REQ-4	NA		NA		NA		NA	
COM.REQ-5	NA		NA		NA		NA	
DAT.REQ-1								
DAT.REQ-2								
DAT.REQ-3								
DAT.REQ-4								
DAT.REQ-5								
INT.REQ-1								

Continued on next page

Requirement	A1.1	A1.2	A2.1	A2.2	P1.1	P1.2	P2.1	P2.2
INT.REQ-2								
INT.REQ-3								
INT.REQ-4								
INT.REQ-5								
INT.REQ-6								
INT.REQ-7								
INT.REQ-8								
INT.REQ-9								
USE.REQ-1								
USE.REQ-2								
USE.REQ-3								
USE.REQ-4								
USE.REQ-5								
Range	[0-26]	[0-29]	[0-27]	[0-30]	[0-25]	[0-28]	[0-26]	[0-29]
Total								

B Remote Patient Monitoring Device System Simulator Security Assessment

Remote Patient Monitoring Device Security Assessment Report

Device Name: RPM Device System Simulator
Device Model: 1.0.0
Device Type: A1.2 - RPM Contactless Active Devices without Memory

SCORE

Device - DEV		0 in 5
Communication - COM		2 in 5
Data - DAT		4 in 5
Interface - INT		2 in 9
User - USE		1 in 5
	Total:	9 in 29

DETAIL

DEV.REQ-1	0/1
DEV.REQ-2	0/1
DEV.REQ-3	0/1
DEV.REQ-4	0/1
DEV.REQ-6	0/1
COM.REQ-1	0/1
COM.REQ-2	1/1
COM.REQ-3	1/1
COM.REQ-4	0/1
COM.REQ-5	0/1
DAT.REQ-1	1/1
DAT.REQ-2	0/1
DAT.REQ-3	1/1
DAT.REQ-4	1/1
DAT.REQ-5	1/1
INT.REQ-1	1/1
INT.REQ-2	0/1

INT.REQ-3	0/1
INT.REQ-4	0/1
INT.REQ-5	0/1
INT.REQ-6	0/1
INT.REQ-7	0/1
INT.REQ-8	1/1
INT.REQ-9	0/1
USE.REQ-1	1/1
USE.REQ-2	0/1
USE.REQ-3	0/1
USE.REQ-4	0/1
USE.REQ-5	0/1

Automatically generated report at 2020/12/05 in https://joaoferreira.eu/rpm