CYBERSECURITY VULNERABILITIES IN WEARABLE MEDICAL DEVICES: A CROSS-SECTOR ANALYSIS OF RISKS AND MITIGATION STRATEGIES USING IRELAND AS A CASE STUDY

Research dissertation presented in partial fulfilment of the requirements for the degree of MSc in Medical Device Technology and Business

Innopharma Faculty of Pharmaceutical Sciences

Griffith College Dublin

Dissertation Supervisor

Dr. Favour Okosun

Presented by

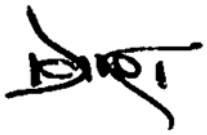
Bridget Epepitimi Kalabo

August 2025.

Candidate Declaration

I hereby declare that the dissertation titled “Cybersecurity Vulnerabilities in Wearable Medical Devices: A Cross-Sector Analysis of Risks and Mitigation Strategies Using Ireland as a Case Study” submitted for the degree of MSc in Medical Device Technology & Business is the result of my own work and that where reference is made to the work of others, due acknowledgement is given.

Candidate Name: Bridget Epepitimi Kalabo

Candidate Signature: 

Date: 24/8/2025

Supervisor Name: Dr. Favour Okosun

Supervisor Signature: Favour Okosun

Date: 24/8/2025

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to God, who gave me strength and carried me through this phase of my life, down to the completion of my thesis in life and good health.

I would like to thank my teachers, especially my supervisor, Favour Okosun, for his guidance, support, timely feedbacks and encouragement throughout the development of this dissertation.

I also appreciate the Innopharma faculty and Griffith College Dublin for providing me with the resources and academic environment that made my research possible.

A deep, heartfelt appreciation goes to my loving family and close friends, for being my constant, supporting me through every phase, helping me when I struggled, listening when I needed to talk, and consoling me when the weight felt heavy. Lastly, I want to appreciate everyone who took out time to respond to, and complete my survey, aiding me to complete this dissertation successfully.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

WMD - Wearable Medical Devices

MITM - Man in the Middle

BLE - Bluetooth Low Energy

IoMT - Internet of Medical Things

IoT - Internet of Things

MFA - Multi-Factor Authentication

GDPR - General Data Protection Regulation

HIPAA - Health Insurance Portability and Accountability Act

MRI - Magnetic Resonance Imaging

CVE - Common Vulnerabilities and Exposure

SPSS - Statistical Package for Social Sciences

FDA - Food and Drug Administration

ISO - International Organization for Standardization

IEEE - Institute of Electrical and Electronics Engineers

NIST - National Institute of Standards and Technology

RFID - Radio Frequency Identification

UX - User Experience

EHR - Electronic Health Record

ECG - Electrocardiogram

OR - Odds Ratio

CI - Confidence Interval

ABSTRACT

Background: Wearable medical devices (WMDs) have become integral to healthcare delivery, providing continuous health monitoring and improving patient outcomes. However, increasing connectivity and data exchange introduces significant cybersecurity vulnerabilities, raising concerns about data privacy, device integrity, and patient safety. Understanding users' perception and practices regarding cybersecurity risks in WMDs is essential for mitigating threats and ensuring safe device usage.

Aim: This study aimed to assess respondents' perceptions and practices on cybersecurity risks associated with wearable medical devices.

Methodology: A cross-sectional descriptive survey was conducted among 108 respondents using a structured questionnaire. The survey collected data on socio-demographics, device usage, perceived vulnerabilities, awareness of cybersecurity risks, and experience of device-related issues. Statistical analyses were performed using SPSS version 27, employing descriptive statistics and chi-square tests for associations. Binary logistic regression was used to identify predictors of good cybersecurity perception, with odds ratios and confidence intervals reported.

Results: The majority of respondents were aged ≤30 years (64.8%), male (61.1%), and postgraduate degree holders (68.5%). Most respondents (63.9%) reported using wearable medical devices, with 41.7% having used them for 2–3 years. Over half (56.5%) had experienced a technical or data-related issue, predominantly device malfunction (48.1%). While 62% were aware of potential cybersecurity risks, only 15.7% believed wearable devices were secure. Significant associations were found between perception and gender ($\chi^2 = 7.115$, $p = 0.029$), occupation ($\chi^2 = 21.346$, $p = 0.006$), educational level ($\chi^2 = 18.507$, $p < 0.001$), and duration of device usage ($\chi^2 = 14.953$, $p = 0.002$). Logistic regression identified educational level and duration of usage as major predictors of perception.

Conclusion: The study highlights a high level of awareness of cybersecurity risks but low confidence in device security among users. Technical issues and perceived vulnerabilities, such as weak passwords and lack of software updates, pose significant concerns. Strengthening cybersecurity measures, implementing user education, and enforcing regulatory compliance are essential to mitigate risks and build trust in wearable medical devices.

Keywords: Wearable Medical Devices, Cybersecurity, User Perception, Data Privacy.

CHAPTER ONE: INTRODUCTION

1.1 Introduction

Glucose monitors, activity trackers, and heart rate monitors are some examples of wearable medical devices (WMDs) that have become indispensable in modern healthcare. Coventry and Branley (2018a) stated that these devices offer real-time health monitoring and remote patient management. Due to technological advancements, there is an increasing demand for continuous health data monitoring especially among the elderly and those with chronic conditions. Although wearable technology has cybersecurity vulnerabilities that jeopardies patient safety, data privacy, and the stability of healthcare systems, its benefits are also significant. (Borges do Nascimento *et al*., 2023). Cybersecurity aims to secure data and electronic assets from theft, misuse, and illegal access. To deliver safe medical care, cybersecurity plays a critical role in maintaining the confidentiality, availability, and integrity of patient records (Mariano, 2020). Despite the digital transformation in healthcare delivery brought about by rapid technological advancement, healthcare organizations face an increasing number of challenges, including data breaches and vulnerabilities in critical infrastructure (Fischer *et al*., 2020). Because of its intricate architecture, links to telemedicine and continuous healthcare services, cyberattacks pose a risk to the wearable medical devices (Schreiweis *et al*., 2019). This study intends to assess the cybersecurity flaws in wearable medical devices by examining the hazards related to these devices in the clinical, regulatory, and technological domains. To inform more thorough, cross-sectorial approaches for safeguarding patient data and device functionality, the dissertation employs Ireland as a case study to identify and evaluate current mitigating strategies.

1.2 Background

The introduction of WMDs, including smartwatches, glucose monitors, and electrocardiogram (ECG) sensors, has completely changed the healthcare sector by making

data-informed diagnosis and real-time patient monitoring possible. Network security protocols, secure firmware updates, user authentication, and data encryption are among the cybersecurity measures now in place for wearable medical devices. These safety measures are meant to ensure device functionality and protect sensitive data. However, there are still flaws due to some device's outdated software, processing power, lack of defined standards, and potential for wireless breaches such Bluetooth hijacking and data interception. Additionally, these defects may lead to data breaches, illegal access, or disruptions in device functionality (Rasool *et al*., 2022). Attackers can intercept, change, or interfere with medical data using man-in-the-middle (MITM) assaults. Similar assaults can be carried out on BLE-enabled devices, such as blood pressure monitors and oximeters, according to research findings. Cybercriminals have used vulnerabilities in fitness trackers to get personal health information, thereby jeopardizing people and compromising medical data (Thapa *et al.,* 2023).

Many devices transmit data in plaintext due to poor encryption or the use of insecure authentication methods, such as default passwords, presenting a considerable risk. The vulnerabilities revealed by the 2018 MyFitnessPal hack, impacting 150 million users, render customers susceptible to ransomware, data breaches, and device hijacking (Mendoza *et al.*, 2018). Williams and Woodward (2015) indicated that several hospitals have seen ransomware attacks traceable to susceptible medical devices. Moreover, wearable devices often serve as channels for extensive network attacks. Yang et al. (2016) characterize mitigating options as multi-tiered security frameworks, including end-to-end encryption, a hardware-based Root of Trust, and artificial intelligence-enhanced threat detection. Hassan et al. (2020) also asserts that the EU Cyber Resilience Act and other legislative measures seek to standardize device security, while technological strategies like network segmentation and multi-factor authentication (MFA) prevent unauthorized access. Despite these attempts, the continued presence of fragmented regulatory requirements and inadequate user understanding highlights the necessity of collaboration between sectors to address vulnerabilities in the rapidly developing Internet of Medical Things (IoMT).

1.3 Justification

According to Addotey-Delove et al. (2023), hospital networks become more vulnerable to malware when WMDs are integrated into them. Compared to other data types, these devices are more vulnerable to abuse and privacy concerns since they continuously gather sensitive health information and are not maximally secure (Alkhaldi *et al*., 2023). Firmware exploitation, poor authentication, data leakage from insufficient encryption, and monitoring of wireless communications (like Bluetooth) are some of these potential vulnerabilities in wearable security.

Cybersecurity vulnerabilities in WMDs may have detrimental consequences as hackers may obtain private medical data from these devices if they are accessed without authority. This might lead to identity theft, insurance fraud, or breaches of patient confidentiality (Bracciale *et al*., 2023). In addition to stealing data, hackers might change device settings, turn off important features, or give healthcare providers erroneous readings that could lead to incorrect diagnosis or ineffective treatments (Thomasian and Adashi, 2021). In extreme circumstances, direct tampering with life-sustaining or health-monitoring devices may risk a patient's physical safety by interfering with insulin supply or heart monitoring, for example. More generally, these kinds of occurrences damage the reputation of healthcare providers and manufacturers, inhibit the adoption of creative solutions, and weaken trust in digital healthcare technologies (Rasool *et al.*, 2022). Successful attacks may also result in financial damages for the organizations involved, expensive legal proceedings, and regulatory penalties. From the standpoint of public health, continuous exploitation of weaknesses may also undermine trust in the country's healthcare system, making it more difficult to successfully incorporate new medical technologies (Park and Lim, 2025).

Numerous devices transmit essential information, including health data and login credentials, without encryption, thereby exposing customers to potential security vulnerabilities (Al-rawashdeh *et al.,* 2022).

The severity of these vulnerabilities is worsened by the different safety precautions used by diverse manufacturers (Ewoh and Vartiainen, 2024). According to Nifakos et al. (2021),

when authentication and encryption protocols are insufficient, hackers may take advantage of system flaws and use compromised devices as access points to larger healthcare networks. Because of fragmentation, it is challenging to integrate security measures extensively while also ensuring compatibility. The issue is made worse by limited device ecosystems and a lack of government regulation (Nifakos *et al*., 2021). Analyzing the cybersecurity flaws of widely deployed WMDs is the main goal of this study which will also look at specific risks and mitigation strategies.

1.4 problem statement

WMDs, like pacemakers, insulin pumps, and fitness monitors, have become a crucial part of contemporary medical care because to their capacity to provide ongoing patient monitoring and enhance therapeutic results. According to Alkhatib et al. (2018), patients are facing an increasing number of cybersecurity risks from the devices, endangering their privacy and general well-being. Hackers are misusing these devices more frequently because of default passwords, inadequate encryption, and inconsistent security standards. This is because device failure or data manipulation may have serious health consequences. Zheng et al. (2019) states that, the possibility of known vulnerabilities is increased by regulatory delays, especially those that take place when patches are approved by agencies such as the FDA. The problem is rendered even more dangerous by the lack of universally established security criteria among manufacturers, which worsens the already escalating threat. This is especially true when combined with a lack of user knowledge. Implementing thorough mitigation techniques, such encryption, multi-factor authentication, and real-time threat monitoring, is crucial to defending hospital infrastructure and patients against ransomware and other attacks on networked wearable technology. These techniques should be incorporated through timely and collaborative efforts across the sectors. With a focus on Ireland, a nation with a rapidly growing MedTech economy, this study's cross-sector approach to analyzing cybersecurity vulnerabilities in WMDs is innovative. This study incorporates views from the healthcare, regulatory, and technology sectors to provide a

thorough understanding of the problem, in contrast to many previous studies that focus either on technical vulnerabilities or regulatory frameworks.

With limited cross-sector analysis that combines healthcare, regulatory, and technology views, current research on cybersecurity risks in WMDs frequently looks at technical flaws or regulatory frameworks separately. This disparity is especially noticeable in Ireland, where there has been little scholarly focus on the unique cybersecurity issues faced by the country's quickly growing MedTech sector and significant presence of global manufacturers like Abbott, Johnson and Johnson, etc. Furthermore, there is little assessment of how well security mechanisms like encryption, authentication, secure firmware updates, and network protections are applied and maintained in the Irish setting, despite the fact that they are generally advised.

Few studies have looked at how manufacturers, healthcare providers, regulators, and patients work together to manage risks and coordination, and responsibility gaps still exist across these groups. The development of focused, long-lasting solutions is also hampered by the lack of useful, context-specific recommendations that are suited to Ireland's legislative framework and healthcare environment, despite the fact that many studies identify risks.

This study closes these important gaps by analyzing the interplay between sector-specific issues, evaluating Ireland's present cybersecurity regulations and practices in the MedTech industry, and suggesting cross-sector solutions to improve patient safety and device security. Improved policy formulation, increased industry standards, and more public knowledge of the significance of preserving WMDs are all possible outcomes of this integrated strategy.

1.5 Objectives

1. To determine and analyze the main cybersecurity vulnerabilities in wearable medical devices used in the healthcare sector.

2. To assess the possible hazards and impact of cybersecurity threats on patient privacy and safety in relation to these devices.

3. To evaluate current cybersecurity frameworks and mitigation techniques relevant to wearable medical devices, emphasizing their effectiveness and challenges.

4. To provide recommendations for enhancing cybersecurity protocols that are specific to the difficulties presented by wearable medical devices in healthcare settings.

1.6 Scope and Limitations

The purpose of this dissertation is to examine and analyze the cybersecurity dangers associated with typical medical devices, such as wearables, and remote patient monitoring systems. In the huge ecosystem, that is the Internet of Things (IoT), there are a number of essential concerns to take into consideration, including data privacy, device manipulation, and network security. The scope of this research includes an investigation of the mitigated measures that are now in place in the areas of organization, legislation, and technology, with a particular focus on the cooperation of experts from other fields. In tandem with the growing risks to data that artificial intelligence poses, legal frameworks such as the EU MDR and GDPR are now being assessed.
The fact that new cybersecurity threats are always emerging is one of the most significant drawbacks, since it may render previously developed research and mitigation techniques worthless. Due to the possibility of having different risk profiles, alternative medical devices and consumer wellness items are not included in the topic of wearables in the healthcare industry. There is a possibility that the generalizability of the results is restricted due to the fact that variations in production processes and local legislation exist.

Since the focus of this study is wearable medical devices, non-wearable medical devices, such as conventional or implanted technologies, will not be examined. Also, security elements will be covered, but in-depth hardware or software engineering procedures will not be part of the research. Furthermore, the analysis will not conduct a thorough comparison analysis at the international level and will be restricted to the Irish context,

with only a brief reference to global cybersecurity regulations or frameworks. Lastly, even though patient safety is a top priority, clinical trials and in-depth analysis of patient health outcomes will not be a part of this study. These exclusions guarantee that the study stays firmly focused on its primary goal, which is to present a cross-sector analysis of cybersecurity flaws and mitigation strategies for wearable medical devices in Ireland.

1.7 Dissertation Structure

The structure of this dissertation includes:

• Chapter 1 Introduction: This chapter gives a short introduction to the research, its importance, aim and objectives, preparing the foundation for the rest of the dissertation chapters

• Chapter 2 Literature Review: This chapter critically reviews current literature on the topic and further expatiates on any gaps identified during the research proposal and in existing literature.

• Chapter 3 Research Methodology: The methodology expatiates on the research design and the justification for each step in the design process, which also includes the philosophical approach used, research strategy, conceptual framework, data collection and analysis and the ethical considerations for the research.

• Chapter 4 Results, Analysis and Discussion: This chapter illustrates the findings from the primary research using visual analytical resources. These results are then analyzed, interpreted and discussed.

• Chapter 5 Conclusion and Recommendations: This chapter summarizes the analysis and discussion in chapter 4, to give an account of the main findings. The chapter also gives recommendations, and the final conclusion.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

Currently, the use of medical devices has become very essential in the healthcare system. These devices include glucose monitors, fitness trackers, heart rate sensors, etc. Coventry and Branley (2018a) assert that these devices provide real-time health monitoring and remote patient management. Due to advancements in technology, there is an increasing need for continuous health data, particularly among the senior population and those with chronic illnesses. While medical devices provide several advantages, they also present considerable cybersecurity risks that might threaten the stability of healthcare systems, patient safety, and data privacy (Borges do Nascimento *et al.,* 2023). The main objective of cybersecurity is to protect the electronic assets and data of healthcare organizations against theft, abuse, and unauthorized access. Healthcare cybersecurity seeks to safeguard the confidentiality, availability, and integrity of patient records to provide secure medical treatment (Mariano, 2020). The healthcare sector is now facing an increasing number of issues, including significant infrastructure risks and data breaches that jeopardize critical patient information. Nonetheless, substantial technology progress has brought about a digital transformation in healthcare delivery (Fischer *et al.,* 2020). Cyberattacks cause a potential threat to the internet due to its complex architecture and connections to telemedicine and ongoing healthcare services (Schreiweis *et al.,* 2019).

A medical device (MD) is described as any apparatus that aids in the diagnosis, treatment, or prevention of illness or injury, as well as in monitoring or sustaining health. This category encompasses a diverse array of technologies that are always evolving due to the growing prevalence of software-enabled devices. Magnetic Resonance Imaging (MRI) equipment uses software to streamline signal processing and data visualization. The firmware of infusion pumps enables regulation and delivery; these devices constitute 38% of an institution's IoT presence. Bracciale et al. (2023) claims that insulin pumps may aid dosage regulation and transmit medical data via wireless connections. Regrettably, all software applications may be vulnerable to attacks. Some MRI scanners reveal confidential medical information, and three out of four intravenous (IV) pumps either expose sensitive

patient data or permit unauthorized access (Farlow *et al.,* 2023). Moreover, certain insulin pumps enable remote assailants to alter pump settings and control insulin administration, potentially resulting in deadly consequences.

Are these cyber dangers acceptable for implementation in medical devices inside our residences or healthcare facilities? This question is challenging to address. The capacity of asset management to identify the presence of a pertinent vulnerability impacting their assets is as crucial as their proficiency in promptly implementing a remedy after its release (product owner or hospital IT manager). Implementing security enhancements on Internet of Things (IoT) devices is very challenging and expensive (Stern *et al.,* 2019). A Common Vulnerabilities and Exposures (CVE) is a unique identifier for a specific vulnerability provided by the MITRE Corporation in the United States. Upon the disclosure of a new vulnerability in medical device software, security professionals worldwide use this resource. The total count of CVEs is 211,890, with more than 2,500 new entries generated monthly. The medical establishment evidently exhibits a lack of concern over these challenges. The US Cybersecurity and Infrastructure Security Agency (CISA) issues Cybersecurity Alerts and Advisories, to notify the public on various CVEs that risk medical equipment. Each warning is assigned a distinct identifier, such as ICSMA-XX-YYY-ZZ. The whole information is accessible on the cisa.org website.

2.2 Wearable Medical Devices

Wearable technologies are being used in various healthcare and biomedical monitoring systems to continually study essential biomarkers for medical diagnosis, physiological health assessment, and evaluation. An aging population is associated with a variety of health challenges, both acute and chronic. The healthcare industry is going through a significant transformation due to the need for real-time monitoring of chronic conditions and point-of-care diagnostics. Wearable technology includes implants, physical attachments, integrated garments, and accessories. The evolution of implanted devices in recent decades has significantly improved the quality and effectiveness of medical services, owing to great advancements in electronics, biocompatible materials, and nanotechnology.

These devices use biological mechanisms and tiny sensors to identify and diagnose illnesses.

2.2.1 Technical Vulnerabilities and Device Design Flaws

Recent technological advancements have significantly impacted healthcare administration, with the capacity to enhance patient care. This phenomena is shown by the growing network of connections across diverse healthcare systems and medical apparatus. Medical equipment, similar to other networked computer systems, is susceptible to security breaches due to its interconnectivity (Heeks, 2006). Unlike other types of networked computer systems, there is increasing concern over the potential jeopardization of patient safety and therapeutic treatment resulting from the connection of these medical devices (Thapa *et al.,* 2023).

The combination of medical devices, operating systems, software, and networking endangers the relative safety of medical equipment. Integration is challenging and entails administrative and security problems. These challenges are referred to as cybersecurity vulnerabilities (Alexander and Baranchuk, 2020). The term "cybersecurity" may refer to several troubling issues, based upon the context. Cybersecurity entails safeguarding data and computer networks against unauthorized access, disruption, and hostile attacks. As we transition from standalone medical devices to integrated systems including equipment, networks, and software, we encounter new issues in management and security. Our civilization necessitates safety certification for medical devices.

The absence of inherent security in these systems is probably more concerning than the events they trigger (2024). A multitude of prevalent vulnerabilities in medical devices has been identified via research. Such devices often possess online interfaces for infusion systems, link to internal networks with Internet access, and come with default hardcoded administrator credentials. The use of unauthenticated or unencrypted web services included within these devices may enable an attacker to achieve global remote control.

2.2.2. Complexity and Opacity of Medical Device Supply Chains

The complex global networks of medical product supply chains consist of people, protocols, technology, and law. In the construction of supply chains for medical products, efficiency and cost-effectiveness are often emphasized above transparency and resilience (Coventry and Branley, 2018a). The COVID-19 pandemic and the annual deficiency of medical supplies in both developed and developing countries have shown the potential consequences for public health and national security (Miller *et al.,* 2021). Analyzing the characteristics of medical product supply networks is essential for devising strategies to improve their resilience.

The nation's supply chains for medical supplies are essential to the health of its populace, irrespective of circumstances. The supply networks in question are dynamic, intricate, and global (Argaw *et al.,* 2019). Instead of being vertically integrated into a single entity, they are distributed and managed by a network of firms. Private, profit-oriented objectives to enhance supply resilience may conflict with public health and safety mandates aimed at protecting essential medical supplies during periods of diminished profit margins (Kruse *et al.,* 2017a).

Congress enacted many measures, and the president declared executive directives to mitigate the severity of these dangers. It is vital to intentionally ensure that the medical product supply chain is adequately prepared for future public health emergencies, notwithstanding the unique capabilities, resources, and infrastructure these technologies provide to enhance resilience. The author claims that investment in a reliable supply chain for medical supplies has been challenging due to ongoing legislative alterations and ambiguity about government policy on public health emergencies (Jalali *et al.,* 2019). There is a deficiency of suitable product categories for evaluating and addressing supply issues in quality and safety management. Consequently, it remains unclear which areas need prioritizing for resilience interventions.

2.2.3 Regulatory Standards Landscape

To protect health care systems against identity theft, cyberattacks, and breaches of health information due to human error, health care organizations must alert the human health office, regulatory authorities, and data owners in compliance with relevant law. This guarantees compliance with ethical and privacy standards, as stated by S. Rubí and L. Gondim (2019). Employing a security compliance officer is necessary for averting such incidents. This individual may supervise critical cyber hygiene protocols and provide guidance. It is also important to encrypt sensitive health information, render it unusable, and maintain backups in both digital and physical formats. Healthcare organizations must guarantee that their personnel undergo sufficient training and establish a thorough protocol to mitigate cyber threats stemming from detrimental human actions, including employee negligence, insufficient skills, or cyber warfare. But this strategy that has been proposed needs a societal view, to put educational programs and standards in place.

2.3 Internet of things (IoT)

From the first eyeglasses in the thirteenth century to the Holter monitor in 1949, which allowed for continuous heart monitoring outside of hospital settings, medical equipment's have advanced significantly. The once simple health aides have evolved into complex gadgets that may provide data in real time as a result of developments in downsizing, wireless connectivity, and sensor technology (Wagan *et al*., 2022). This tendency has been propelled by the growth of the Internet of Things (IoT), which has made it easier to incorporate wearable technology into networked healthcare systems known as the Internet of Medical Things (IoMT). Although connectivity makes customization easier, there are serious cybersecurity dangers associated with it, such as data breaches and device manipulation. The necessity of doing a cross-sectoral assessment of the risks associated with common medical equipment inside IoT networks is emphasized by Wagan et al. (2022). In addition to utilizing the promise of new technologies, this research attempts to investigate ways to reduce these dangers and protect patient privacy and safety.

2.3.1 Cybersecurity Analysis of Wearable Devices

Because of the possibility of bodily harm and potentially fatal outcomes, cyberattacks on IoT devices are considered extremely risky, especially when sensitive health information is involved. According to Zubair et al. (2022), vulnerabilities could affect a person's health as well as the functionality of a gadget. Fundamental security concerns are ignored by manufacturers, who upgrade components to cut costs and focus on minimum functionality, all the while thinking that these gadgets would be commercially viable due to the expected strong market demand. Moreover, several device manufacturers neglect to provide software updates or security modifications that may potentially mitigate or avert additional damage in the event of an attack.

Experts indicate that Shodan identified around 68,000 medical devices that were potentially exposed and accessible on the public internet. The devices included MRI apparatus, pacemakers, and infusion pumps. The devices were configured according to their predetermined parameters. The researchers may get information like default credentials, software versions, operating systems, staff names, and office numbers (Jeng *et al.,* 2022). At times, the attackers were unaware of the equipment they were compromising. Recognizing it would have granted them access to critical data, ultimately endangering the hospital's information technology framework. Clinicians may now oversee a patient's cardiac health by adjusting implanted cardioverter-defibrillators (ICDs). These devices may provide enough electrical stimulation to re-establish normal cardiac rhythm (Rodríguez *et al.,* 2023). It was concluded that malicious individuals may induce failures in these devices, potentially resulting in life-threatening shocks for victims.

The significance of IoT technology has increased during the COVID-19 pandemic because of its many benefits across several sectors, including communication, employment, education, entertainment, health monitoring, and the encouragement of a healthy lifestyle. The worldwide prevalence of IoT devices has surged, owing to high demand from individuals seeking improved lives at reduced expenses. Due to the need of health surveillance to prevent potential repercussions, IoT technology might be crucial in

identifying issues requiring continuous oversight to mitigate harm to a broader population (Rosman *et al.,* 2020).

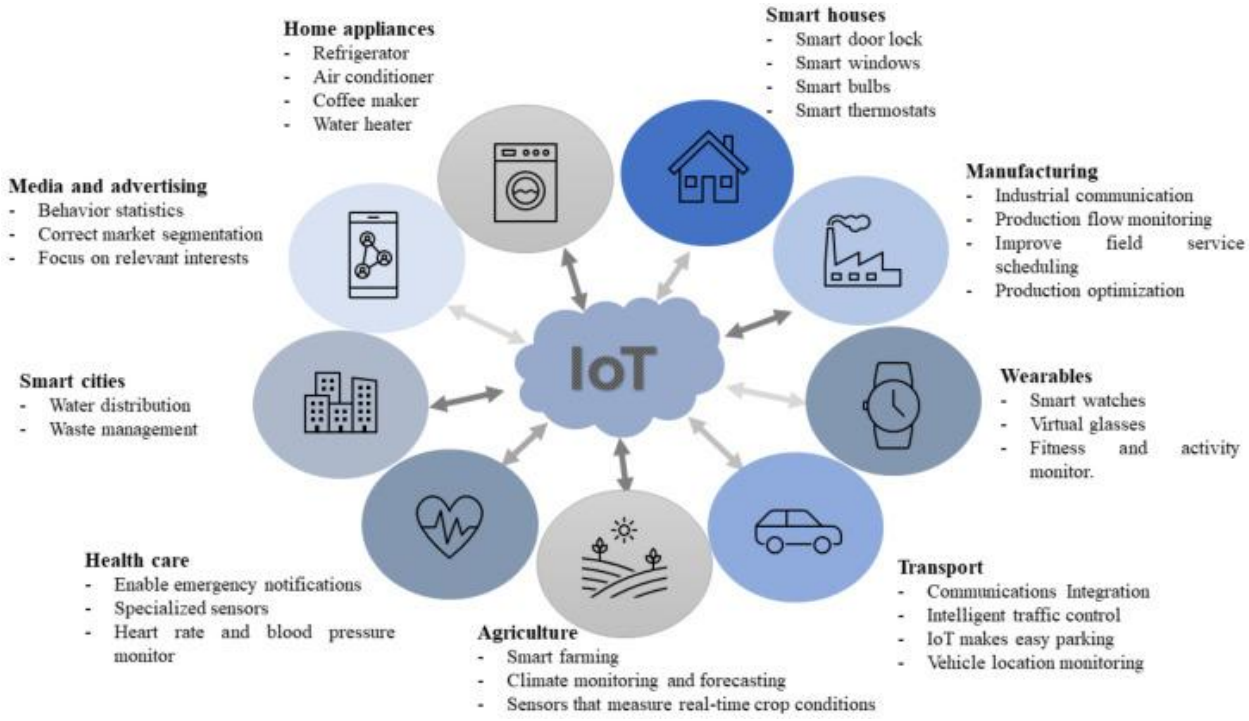


Figure 1: IoT Application areas (Silva-Trujillo et al., 2023)

2.3.2 IoT Vulnerabilities and Challenges

Considering the prevalence of attacks on IoT devices, it is evident that we must implement measures to safeguard these systems (Zubair *et al.,* 2022). Consequently, a person's health and lifestyle may be significantly transformed. The confidentiality of sensitive data stored on devices is concerning, owing to a strategy that entails data transmission between devices and the absence of sufficient authentication measures for those managing such data.

Alternative forms of attacks aim to alter data, so undermining the reliability of the obtained user information. The integrity of the IoT device is compromised. Presently, several medical applications exist for IoT devices that collect data in real time. Neglecting to register may jeopardize the lives of users, perhaps determining life or death for some individuals. Moreover, if they are not consistently accessible, they do not fulfil their intended purpose.

2.3.3 Smartwatches: Bluetooth Communication Attacks

Bluetooth is used by a variety of gadgets, such as speakers, headphones, refrigerators, autos, wearable technology, medical apparatus, and countless more. Central to the Internet of Things (IoT) are little devices equipped with several sensors. Bluetooth is the optimal technology for those pursuing Internet of Things (IoT) functionalities. To safeguard customer privacy, manufacturers must be knowledgeable about the problems and limitations of the Internet of Things (IoT) and the creation of secure solutions. Nonetheless, hackers have been exploiting vulnerabilities in earlier iterations of Bluetooth technology for a long duration, attacking the connection via various methods. These updated communication protocols have enhanced device security against eavesdropping and man-in-the-middle attacks.

The first iterations of Bluetooth introduced were Bluetooth Basic Rate (BR), Enhanced Data Rate (EDR), and High Speed (HS). Bluetooth 1.1 and 1.2 were only compatible with BR owing to their limited capability for data speeds over 1 Mbps. Bluetooth 2.0 enhances EDR, allowing it to achieve transmission speeds of up to 3.0 Mbps. HS, enabling data transfer rates of up to 24 Mbps, was launched with Bluetooth 3.0. Devices capable of greater data rates may also accommodate lower data rates from previous Bluetooth standards. Bluetooth Classic sometimes denotes earlier Bluetooth varieties.

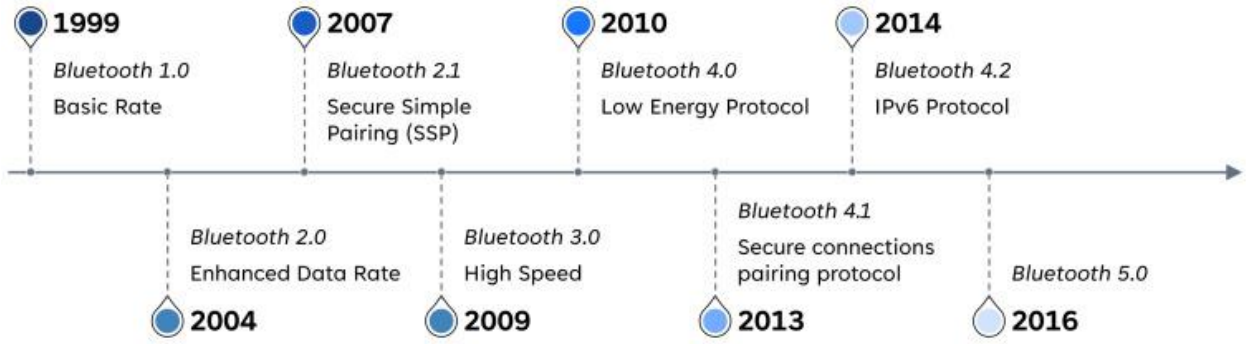


Figure 2: Bluetooth Technologies and Evolution (Silva-Trujillo et al., 2023).

The Bluetooth Low-Energy (BLE) standard was first released in Bluetooth 4.0 and then revised in versions 4.1 and 4.2. This is suitable for wearable medical equipment and sensors

since it was originally designed for devices that use coin-cell batteries. It lowers the demands on power and memory. The core principle is that it will stay in dormant mode until the link is made, at which juncture it will activate. This leads to streamlined protocols, abbreviated packets, and enhanced efficiency in device identification and connection processes (Jeng *et al.,* 2022).

The ability of a Bluetooth 4.0 device to accommodate both Bluetooth Classic and Bluetooth Low Energy is termed dual mode. For example, when you pair your phone with Bluetooth Classic earphones, data transmission will occur continuously. When you link your smartphone to a smart wristband that tracks your physical activity, data transmission is only necessary during synchronization to see your findings.
Survey on Security and Solutions for the Internet of Things 2.3.4
The integration of health characteristics into IoT devices transforms the surroundings into an IoMT. The proliferation of new technologies is driving the increased use of IoMT devices. The COVID-19 pandemic has considerably limited the frequency of in-person consultations between patients and providers. The pandemic has ushered in a new epoch of IoMT as a means of patient treatment, according to Sadhu et al. (2022a). The Internet of Medical Things (IoMT) involves creating a system that connects persons with various medical equipment, including implanted and wireless technologies. It forges links with healthcare providers, hospitals, and other medical institutions using wireless networks (e.g., Bluetooth, 3G, 4G, 5G, and ZigBee) to enable the transfer of patient records (Sadhu *et al.,* 2022b). Contemporary medical apparatus can identify and relay vital indicators such as blood pressure, heart rate, oxygen saturation, and more metrics due to advancements in microelectronics. This groundbreaking innovation in medical technology allows for the implantation of devices in the body as watches, enabling continuous monitoring and treatment of all elderly patients. Post-COVID-19, some patients persist with symptoms, and IoMT may provide immediate treatment if necessary. The IoMT method is extensively used by healthcare organizations globally for patient treatment. According to CyberMDX's 2020 research, around fifty percent of IoMT devices are susceptible to attacks. IoMT networks are unique in their capacity to influence patients' everyday lives and may raise privacy issues if their names are revealed (Austen, 2015). The primary objective of the IoMT system is to provide privacy and security. In 2021, a record amount of patients'

personal health data were exposed due to cybersecurity threats, as reported by the cybersecurity firm Critical Insights. Healthcare attacks impacted a substantial number of persons, increasing from 34 million in 2020 to 45 million in 2021. The analysis indicates an increase from 14 million in 2018 to a substantial triple-digit figure within three years (Sun *et al.,* 2019).

2.4 Historical issues associated with adopting cybersecurity issues globally

The historical context, current status, and association with the designation of wearable medical devices

The thirteenth century saw the emergence of optical lenses, the first instance of wearable technology capable of enhancing health (Escobar-Linero *et al.,* 2023), so initiating a protracted and notable history of wearable medical devices. The Holter monitor was developed in 1949, enabling continuous cardiac observation outside clinical settings. The first implanted pacemaker was created in 1958 (Lu *et al.,* 2020). These advancements laid the foundation for the creation of biosensors, smartwatches, and continuous glucose monitors (CGMs), which offer real-time health data and personalized treatment.

Even though the Internet of Medical Things (IoMT) is largely dependent on numerous medical devices, the improved connectivity they offer also presents cybersecurity risks. As these devices develop from basic monitoring tools to sophisticated, a thorough cross-sector assessment of hazards and mitigation techniques is crucial to guaranteeing patient safety and data integrity. The probability of data breaches and device tampering rises with each cycle (Wagan *et al*., 2022). This development demonstrates the intricate relationship between wearable healthcare cybersecurity concerns and technological advancement.

2.4.1 Resource Constraints and Implementation Challenges on Cybersecurity Vulnerabilities

The development, implementation, and maintenance of digital health technology have greatly improved healthcare quality, efficiency, and transparency and are impacted by cybersecurity implementation challenges and resource limitations (Ewoh and Vartiainen,

2024). To maximize success and accomplish the intended goals, it is crucial to identify and evaluate the project's health risks and enablers at every stage of the design process. According to Giansanti (2021), improving healthcare services and equipment requires the efficient application of digital technology. Systematic management practices, such as planning, resource allocation, and monitoring and evaluation tools, are used to achieve this. Numerous projects have been started in low, middle, and high-income countries to enhance digital health technology for practitioners and other stakeholders in response to these problems (Huang *et al*., 2020).

2.4.2 Security vulnerabilities in healthcare

According to Mejía-Granda et al. (2024), hackers can take advantage of flaws in software applications and devices connected to the internet in order to take over and carry out illegal actions. Perpetrators trying to undermine the normal operation of systems and devices possess many aims, including the ability to propagate attacks to other susceptible systems nearby, sustain persistence, and ensure continued system access. Security flaws can affect automated software-driven medical processes such as temperature monitoring, electrocardiogram (ECG) recording, oxygen saturation measurement, and vital sign monitoring (Langer, 2017). Software-assisted respiratory devices are crucial for the treatment of COVID-19 patients, according to Kruse et al. (2017b). Patient health is put at risk when medical software malfunctions. Historical events such as the Therac-25 accelerator incidents and the potential for pacemaker reconfiguration underscore the risks. Another issue is that a failure in a pharmaceutical delivery technique may result in patient injury or even mortality (Kruse *et al.,* 2017b). Improper configurations, nonadherence to the Secure Software Development Life Cycle (SDLC) methodology, deviation from established standards, and the use of poor coding methods contribute to security vulnerabilities. Cybersecurity is further compromised by the prevalence of healthcare applications using outdated operating systems. Cryptographic attacks, cybercrime, denial of service (DoS) assaults, injection vulnerabilities, malware, privilege escalation, and online security deficiencies are prevalent sources of vulnerabilities in healthcare.

Organizations such as the Open Web Application Security Project (OWASP) and the National Institute of Standards and Technology (NIST) provide valuable resources in the fight against vulnerabilities. OWASP produces a report delineating the top 10 security vulnerabilities in web applications to assist with mitigation efforts. Mejía-Granda et al. (2024) assert that NIST's National Vulnerability Database (NVD) has an extensive repository of vulnerabilities, including the CVE catalogue and CWE.

2.5 Adoption

In light of the substantial increase in the senior demographic, the medical sector has prioritized the development of biosensors that provide personalized treatment for various acute and chronic ailments, alongside real-time health surveillance and preventive measures. Point-of-care technology (POCT) is advantageous for those with restricted access to healthcare, since it facilitates rapid, patient-centered diagnostics, in contrast to traditional, labor-intensive, expensive, and professionally staffed diagnostic methods. The global wearable sensors market is projected to expand at a CAGR exceeding 38% from 2017 to 2025, driven by a heightened emphasis on personalized healthcare treatments. The wristwatch is anticipated to represent a substantial portion of this growth (Gura, 2015).

Over the last ten years, the healthcare sector has spearheaded the widespread biosensor initiative, seeking to derive therapeutically relevant information from physiological signals like heart rate, blood pressure, skin temperature, respiration rate, and body mobility (Choi *et al.,* 2016). Wearable devices may now incessantly monitor individuals due to the presence of noninvasive biosensors that provide real-time information. This data may be used to establish a fundamental medical diagnosis, sufficient for assessing an individual's health. Additionally, physicians may use pervasive biosensors to monitor patients' vital signs and evaluate the efficacy of their medications. Wearable biosensors can be attached to a person's body in a variety of ways, including jewelry, clothing, watches, eyeglasses, and sutures. According to Kamišalić et al. (2018), these gadgets stand out for being adaptable, user-friendly, and portable. By making it easier to diagnose and prognosticate patients utilizing biological tools and tiny sensors, the development of implanted devices in recent decades has greatly enhanced medical care. Significant developments in electrical technology, biocompatibility, and nanomaterials made this accomplishment possible. One

of the biggest challenges for wearable sensors is creating electrical devices that can stick to the skin and discreetly and constantly track the user's vital signs and activities without being impacted by movement. According to López-Blanco et al. (2019), the first medical procedure, which involved implanting a pacemaker in a patient's heart, took place in 1958. Pacemakers and implanted cerebellar stimulators have advanced significantly since then. Devices can now be implanted in previously inaccessible locations, such as the deep brain, intravascular region, intracardiac space, and even inside individual cells, thanks to the development of more ductile and elastic electrical devices (Tison *et al*., 2018). Wearable devices may now operate independently as a "microcomputer" due to its autonomous functionality, integrated receiver, and signal processor. Consequently, data collection, processing, communication, and power supply may all operate concurrently. Wearable electronics may link to other smart devices using technologies such as Bluetooth, infrared, radio frequency identification (RFID), and near-field communication (NFC). This link has facilitated the development of ubiquitous systems, enabling remote and prolonged monitoring of patients in previously unreachable residences and communities. The use of this talent is anticipated to lead to a substantial reduction in healthcare and medical expenses in countries with a considerable elderly demographic. This article evaluates contemporary, emerging, technologically sophisticated, and prospective wearable devices, along with their advancing medicinal applications.

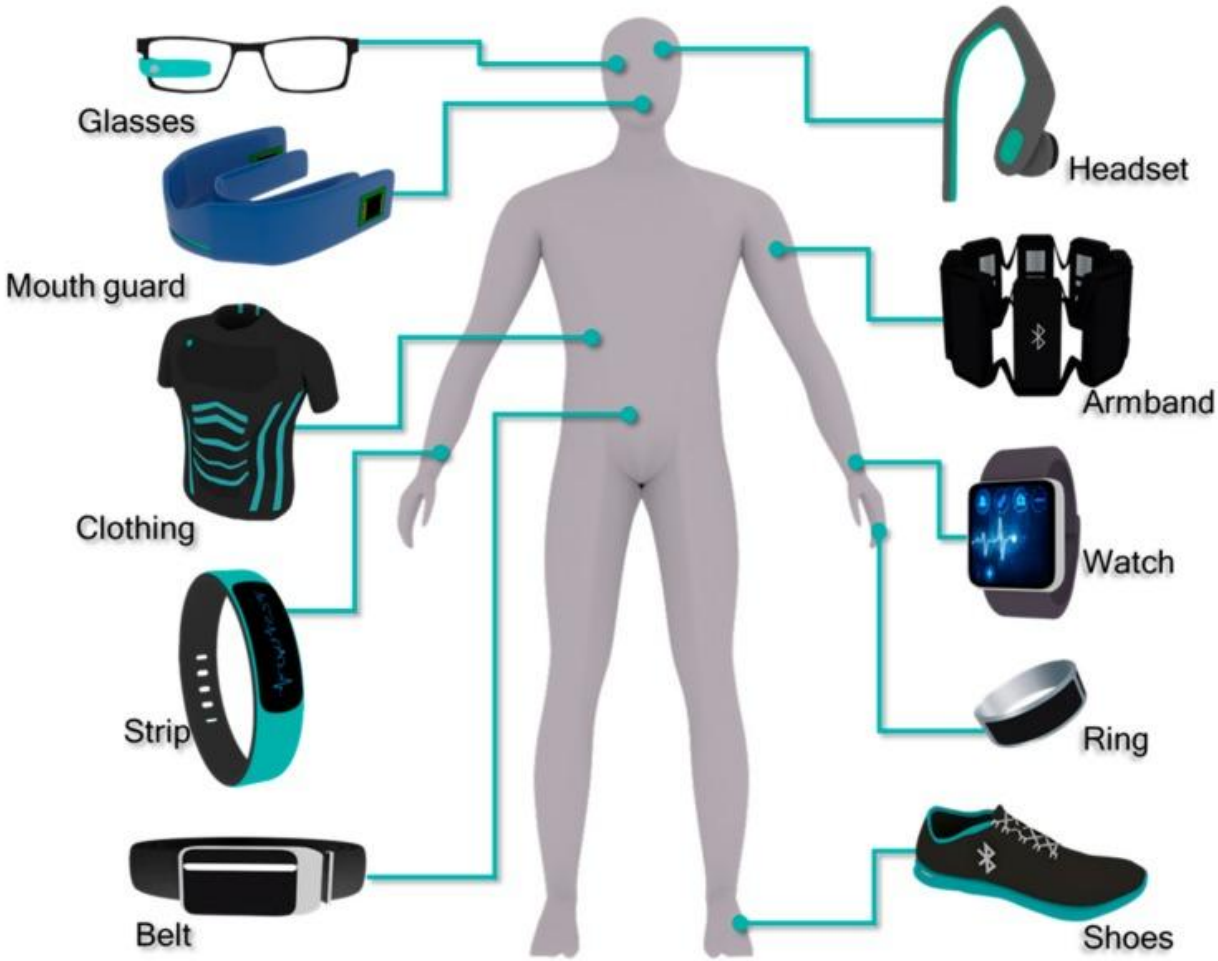


Figure 3: Portable medical and healthcare devices worn on body parts

Wearable devices provide personalized health services, as well as advanced levels of personalized portable devices and sensors.

2.6 Gaps and Opportunities for Further Research

Despite increasing awareness of these difficulties, Thapa et al. (2023) and Williams and Woodward (2015) see a deficiency in research concerning supply chain security, user-centric security models, incident response and forensics, and long-term impact evaluations. Current methodologies depend on post-sale surveillance, and further research is required to establish vendor-neutral security standards that are straightforward to apply. Additionally, further research is necessary to assess the long-term impacts of wearable

medical devices and provide comprehensive guidance on responding to incidents involving these items.

2.6.1 Current hospital cybersecurity strategies and their gaps

2.6.1.1 Technical measures

The majority of hospitals' present cybersecurity initiatives focus on user endpoint security, irrespective of whether the threat emanates from the medical professional or the patient. For instance, one may limit access to designated websites, require complex and often changed passwords, and let only hospital-authorized devices to connect to the network (Tully *et al.,* 2020). While these regulations aim to enhance the security of systems, accounts, and networks, their efficacy is not guaranteed. Indeed, thirty of the most frequently exploited vulnerabilities in 2015 did not need a password (Coventry & Branley, 2018b).

The IT department enacts proactive strategies like segmentation and enhancements. The term "segmentation" denotes the process of deconstructing the hospital network and its associated equipment into smaller elements. All other components are secure; only one may be compromised by a hostile actor (Nifakos *et al.,* 2021). The method of "patching" software vulnerabilities is equivalent to mending gaps in fabric. Manufacturers often provide patches, which are software updates, to address vulnerabilities identified in their systems' code (Vrhovec and Markelj, 2024). It is uncommon for IT teams to proactively identify security vulnerabilities inside their own systems.

2.6.1.2 Device requirement measures

Most hospitals have fundamental protocols to safeguard medical equipment from potential dangers. This category encompasses issues like as accessibility, validity, reliability, and information privacy. The primary techniques for accomplishing these objectives are encryption, checksum verification, access limitations, and authentication credentials (Clarke and Youngstein, 2017). Nevertheless, they were unable to guarantee

comprehensive data security. For instance, even when encrypted, adversarial entities may still get access to or decipher the data. Checksums, access limitations, and credential requirements are similarly ineffective, since adept attackers may easily circumvent them. Response and detection strategies.

Experts, notably from the Society for Imaging Informatics in Medicine, assert that cyber defenders are tasked with inspecting devices, networks, user activities, and security protocols; authenticating and credentialing hospital system users; ensuring system functionality; and safeguarding the confidentiality and integrity of patient records (Maccioni and Giansanti, 2021).

Two interconnected concerns arise in healthcare since the IT department often serves as the cyber defender (Bhuyan *et al.,* 2020). Initially, not all of these essential responsibilities would be fulfilled due to constrained IT personnel. IT departments identified 75% of hospital cyber events, while additional people contributed to the detection of 57% of assaults. Third-party specialists identified 21%, whereas worried patients recognized just 5% (27). More than fifty percent of hospitals had established protocols for addressing assaults. This figure is below the industry average of 59% (Kelpsas and Nelson, 2016). As previously mentioned, hospital IT departments are deficient in resources required to guarantee operational security.

2.6.1.3 Regulatory measures

Numerous healthcare organizations adhere to governmental regulations and laws on cybersecurity. HIPAA mandates that hospitals designate data security officers, conduct regular risk assessments, and establish incident response plans, among other requirements. Nonetheless, the limitations are insufficient to guarantee hospital security. The CMS mandates that hospitals using their services use fundamental antivirus and antimalware software (Giansanti and Monoscalco, 2021).

2.7 Gaps highlighted during the pandemic

The COVID-19 pandemic revealed more deficiencies in hospitals' cybersecurity readiness, demonstrating that current protective measures are insufficient. In 2020, there was a substantial rise in intrusions, particularly with ransomware (Spanakis et al.). Cybercriminals assaulted various institutions, encompassing a health agency in the United States, a hospital in the Czech Republic, a vaccination trial in the United Kingdom, a team constructing an emergency COVID-19 hospital in the United Kingdom, and vaccine development laboratories in the United States, United Kingdom, and Canada. As the assaults intensified, countries and the international law enforcement organization INTERPOL sent alerts. Following the compilation of a list exceeding 400 susceptible institutions, hackers in the United States targeted several hospitals (Dullea *et al.,* 2020).

In conclusion, this chapter looked at the cybersecurity weaknesses in WMDs and their impact in healthcare platforms. These technologies greatly improve real-time healthcare monitoring, but they also bring serious risks like unauthorized access, breach of data, harm to patients, etc. The major challenges faced are weak IoT protocols, defects in device designs, supply chain issues, and regulatory problems. Even with currently existing systems like segmentation and end-to-end encryption, there are still gaps in standardization, timely detection and response to incidents. The problems discussed shows a crucial need for stronger security systems, and cross-sector policies to certify safety of patients and data integrity.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Study Location

Dublin, Ireland, is a notable hub for wearable medical device innovation and biomedical design. The city hosts specialized companies like Movement, which focuses on biomedical usability and medical device design, including wearable and interfacing technologies for various medical fields such as cardiology and surgery. Dublin's ecosystem supports advanced R&D efforts, exemplified by projects like the development of smart wearable microneedle drug delivery systems, which aim to enhance patient adherence and healthcare delivery at home. Additionally, academic and research institutions in Dublin contribute to cutting-edge sensor technologies for wearable diagnostics, enabling real-time monitoring of biological processes with scalable, low-cost manufacturing methods. Dublin is positioned as a key player in the wearable medical device industry thanks to the existence of these businesses and research projects, which address the usability and new cybersecurity issues that come with linked healthcare equipment. In the growing Internet of Medical Things (IoMT), this cross-sector ecosystem fosters innovation and the creation of mitigation measures required for the security of wearable medical equipment.

Figure 4: Dublin Map Ireland Newebcreations (2025)

3.1.1 Outline and Justification

This study uses pragmatic thinking, a philosophical framework that emphasizes problem-solving and practical principles, to examine cybersecurity vulnerabilities in Wearable Medical Devices (WMDs) in the context of healthcare, technology, and regulatory authorities. It seeks to identify important weaknesses, investigate how they affect patient safety and data privacy, assess regulations across sectors, and offer evidence-based mitigation suggestions. By integrating objective information with the viewpoints of stakeholders, including patients, cybersecurity specialists, healthcare professionals, and regulatory agencies, pragmatism facilitates the collection of data. Through repeated analysis and a variety of data sources, this research would enhance cybersecurity resilience and promote cross-sectoral collaboration in the development, deployment, and management of WMDs and a realistic viewpoint would aid in achieving this objective.

Pragmatism promotes actionable, contextually relevant findings over rigorous adherence to a particular philosophical perspective and permits the use of a variety of approaches to address complicated research topics. This adaptability is particularly useful when the goal of the study is to create a comprehensive knowledge of a phenomenon by combining both firsthand accounts and statistical patterns (Bleiker *et al*., 2019).

3.2 Sample size Calculation

The sample size was derived using Fisher's formula for approximating single proportions and also the formula for estimating the minimum sample size. The standard normal deviation was kept at a 95 % confidence level, with an allowable margin of error of 5 %. The Fisher's formula ($n = Z^2(pq)/d^2$).

n = minimum required sample size in population greater than 10,000

- Z = Standard normal variate for 95 % confidence level, (Z = 1.96)
- d = acceptable difference; using 5 % (d = 0.05)

- q = 1 – p
- prevalence rate of 7% from a study previously done on Wearable Health Devices for Diagnosis Support: Evolution and Future Tendencies study by (Escobar-Linero *et al.,* 2023) was used for this study

$$\text{nf} = \text{Desired sample size when population is less than 10,000}$$

$$\text{n} = \text{Desired sample size when population is more than 10,000}$$

$$\text{N} = \text{Estimated population size, 1,080}$$

$$\text{n} = \frac{\text{z}^2\text{pq}}{\text{d}^2}$$

Where,

$\text{z} = \text{Normal deviate at 95\% confidence interval}$

$$\text{p} = \text{Prevalence from previous similar study, taken as 30\%}$$

$\text{q} = 1 - \text{p}$

$\text{d} = 0.05, \text{with level of significance set at } 0.05$

$$\text{n} = \frac{1.96^2 \times 0.07 \times 0.93}{0.05^2}$$

$= 100$

- n = population size. from the calculation n=100
- adding 10% non-respondent rate = (0.1/100 *100)=10
- hence the total sample that will be used for the study is 100+10=110

Therefore approximately 110 respondents will be targeted for this study

3.3 Primary Research Strategy

3.3.1 Quantitative Data: Surveys will be administered to capture measurable variables such as frequencies, ratings, or demographic information. Surveys are efficient for collecting data from a large sample and allow for statistical analysis.

Participant Selection Criteria

Selection criteria are critical for ensuring the relevance and representativeness of the sample:

- Inclusion Criteria:
    - Cybersecurity experts and clinicians in general.
    - Participants that possess characteristics central to the research question (e.g., specific age range, occupation, experience with the phenomenon under study). Demographic, clinical, or geographic factors may be specified as needed.
- Exclusion Criteria:
    - people who don't have any knowledge of cybersecurity, or wearable medical devices.
- Individuals lacking key attributes or with confounding characteristics (e.g., insufficient experience, unrelated background) will be excluded.
- Recruitment: Efforts will be made to recruit a sample that adequately represents the target population, using purposive or stratified sampling to ensure diversity and relevance. Non-response rates will be monitored, aiming for less than 20-25% non-response.

3.4 Search Strategy

This study conducts a systematic literature search using various academic databases, including Google Scholar, PubMed, Google, and institutional online libraries. These platforms serve as key repositories for scholarly publications and prior research relevant to cybersecurity and healthcare technologies. To minimize selection bias, search keywords were carefully developed in alignment with the study objectives and applied consistently across platforms. The central focus of this review is to explore cybersecurity vulnerabilities in wearable medical devices and to examine the associated risks, impacts, and mitigation strategies across sectors, particularly within healthcare and technology. Given the evolving nature of digital threats, the search strategy prioritizes specificity by incorporating keywords and phrases relevant to cybersecurity, wearable devices, data breaches, healthcare IT, and cross-sector policy frameworks. The literature search targets studies published between 2012 and 2025, with only English-language publications considered. The use of online academic resources ensures accessibility to current and extensive data, in contrast to relying solely on physical libraries that may lack current materials (Machi & McEvoy, 2016).

3.5 Ethical Considerations

Ethical approval for this research will be secured by the Research Ethics Review Committee. Informed permission will be gotten from all individuals participating, before they are involved. Every participant will get a comprehensive briefing about the study's objectives, methodologies, possible hazards, and their entitlement to leave at any point without incurring any penalties. Consent will be recorded in writing, and confidentiality will be rigorously maintained throughout the study by anonymizing data and securely archiving all research materials in accordance with ethical standards.

3.6 Study Instrument

This study will utilize primary data collection methods, specifically a combination of semi-structured questionnaires and direct researcher observation, to obtain relevant information from key stakeholders. The semi-structured standardized questionnaire will be structured to take data on characteristics like socio-demography of respondents, their experiences, perceptions, and practices related to cybersecurity vulnerabilities in wearable medical devices (WMDs). The instrument will explore critical dimensions such as device security features, awareness of cybersecurity threats, institutional mitigation strategies, policy frameworks, technical challenges, and cross-sector collaboration efforts.

Questions will be formulated to capture quantitative responses (using Likert scales to measure levels of agreement, frequency, or awareness). Key stakeholders to be surveyed may include healthcare professionals, IT experts, Cybersecurity experts, and individuals using wearable devices.

Before data collection begins, participants will be informed about the study's objectives, their voluntary participation, and the confidentiality of their responses. Informed consent will be obtained, either verbally or in writing, in accordance with ethical research practices. This instrument is intended to ensure a comprehensive and cross-sectoral understanding of the cybersecurity risks associated with wearable medical technologies.

3.7 Validity of the Instrument

To improve the validity of instruments, supervisors will assess the research instruments to determine their appropriateness and applicability, as well as the clarity of the content and the suitability of the instruments' construction from a research standpoint and prior to data collection.

3.8 Reliability of the Instrument

There will be one pilot test conducted. The reliability of the instrument, sometimes referred to as its co-efficient of internal consistency, will be ascertained using Cronbarch's alpha

co-efficient calculation. The reliability of the questionnaire will be evaluated using the test-retest methodology.

3.9 Data Analysis

The data that will be analyzed for this study will be quantitative data obtained from structured Likert-scale surveys. Multiple-choice options focusing on stakeholder knowledge, experiences, and mitigation methods concerning cybersecurity in wearable medical devices will be evaluated utilizing the Statistical Package for the Social Sciences (SPSS) version 27. Responses on Likert scale will be standardized by calculating mean domain scores to classify degrees of perceived cybersecurity risk and institutional readiness. Descriptive statistics, such as means, frequencies, and percentages, will summarize data on participant demographics, perceived vulnerabilities, and the frequency of mitigation methods. Inferential statistical methods, including independent t-tests, chi-square tests, Kruskal–Wallis tests and Mann Whitney U tests, will be incorporated in evaluating differences across stakeholder groups (e.g., healthcare professionals, IT staff, Cybersecurity experts). Pearson correlation coefficients will be computed to examine the correlations among variables including policy efficacy, device vulnerability, and data privacy. Regression analysis will be used to ascertain the most important predictors of cybersecurity vulnerabilities in the utilization of wearable medical devices. All statistical tests will be two-tailed, with a significance threshold established at $p < 0.05$.

3.10 Conceptual Framework

The conceptual framework upon which this study is built describes the key, interconnected factors influencing primary and secondary research on cybersecurity vulnerabilities in WMDs. This framework is primarily technical in nature and covers topics such as encryption techniques, hardware and software vulnerabilities, WMD security design and the risks associated with Bluetooth and Wi-Fi connections. These can lead to data manipulation and Man-in-the-Middle attacks. User compliance, knowledge, and behavior including that of customers, IT personnel, and medical professionals have a significant influence on device security. How vulnerabilities are handled in healthcare settings is

influenced by a variety of organizational factors, such as the accessibility of IT resources, cybersecurity culture, incident response methods, and institutional norms. International and national cybersecurity standards, as well as compliance requirements to protect patient data and device integrity required by health data privacy regulations like NDPR and HIPAA, are significant legal and regulatory factors. Cross-sector cooperation between regulatory bodies, IT companies, and medical professionals is also essential for the efficient protection of WMDs. The approach evaluates impact outcomes including patient safety, data integrity, service continuity, and institutional trust in order to accurately reflect the repercussions of intrusions. These elements affect the study's focus, methods for gathering data, and analysis. This allows us to pinpoint vulnerabilities, evaluate the efficacy of existing mitigation strategies, and offer evidence-based recommendations for practices and policies that will improve the cybersecurity of commonly used medical equipment.

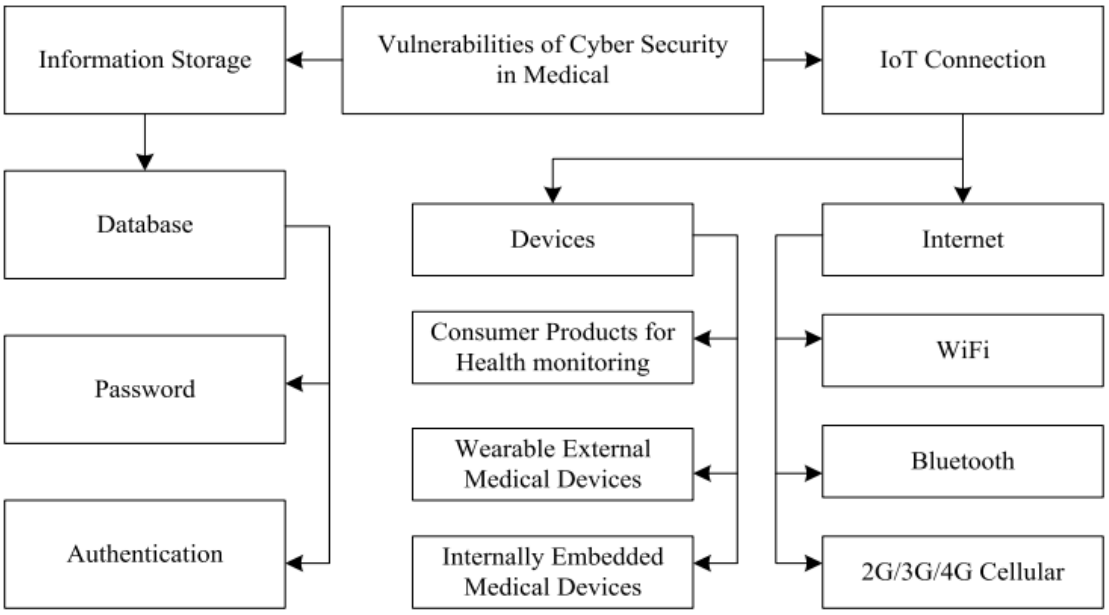


Figure 5: Main vulnerabilities of cybersecurity in the medical domain (Razaque et al., 2019).

CHAPTER FOUR: ANALYSIS AND DISCUSSION

4.1 Introduction

The primary data for this research was collected using a survey questionnaire created using Google forms. The questionnaire consists of 61 questions including, Likert scale, multiple choice, and open-ended questions, distributed into six sections. The participants were mostly eligible participants with expertise in cybersecurity, healthcare and use of WMDs.

The survey was distributed through email, LinkedIn and social media platforms with the use of a shortened URL that was included in the invitation. A short description of the request was also included in this invitation, and respondents were also motivated to share the invitation to members of their network.

This survey remained open from 27th July 2025 to 23rd August 2025. During this time, follow up messages and emails were sent to increase the rate of response. The sample size calculated for the survey was 110, and the final number of responses received was 108.

The survey questions were presented as follows:

- Section 1: Survey Information
- Section 2: Participant consent and Socio-demographic data
- Section 3: Identification of Cybersecurity Vulnerabilities
- Section 4: Dangers and Impacts of Cybersecurity threats
- Section 5: Evaluation of existing Cybersecurity frameworks
- Section 6: Recommendations for enhancing cybersecurity

4.2 Quantitative Findings

4.2.1 Socio demographic of the participants

Table 1: Socio demographic of the participants

Variable	Categories	Frequency	Percent
Age	≤ 30 years	70	64.8
	31–50 years	33	30.6
	51 years and above	5	4.6
Gender	Female	41	38
	Male	66	61.1
	Other	1	0.9
Occupation	Business	4	3.7
	Civil Servant	20	18.5
	Cyber Security Analyst	7	6.5
	Engineer	4	3.7
	Health Care Professional	9	8.3
	Privacy Officer	7	6.5
	Security Analysts	40	37
	Self Employed	4	3.7
	Student	13	12
Educational Level	Postgraduate	74	68.5
	Secondary	2	1.9
	Tertiary	32	29.6

Table 1 presents the socio-demographic characteristics of the participants. A majority, 70 (64.8%), were aged ≤30 years, followed by 33 (30.6%) who were between 31–50 years, and 5 (4.6%) who were 51 years and above. In terms of gender, the respondents were predominantly male, 66 (61.1%), while 41 (38.0%) were female, and only 1 (0.9%) identified as other. Regarding occupation, the majority, 40 (37.0%), were security analysts, followed by 20 (18.5%) civil servants, 13 (12.0%) students, 9 (8.3%) health care professionals, 7 (6.5%) cyber security analysts, 7 (6.5%) privacy officers, 4 (3.7%) business owners, 4 (3.7%) engineers, and 4 (3.7%) self-employed individuals. In terms of educational level, most participants, 74 (68.5%), had postgraduate education, 32 (29.6%) had tertiary education, while only 2 (1.9%) had secondary education.

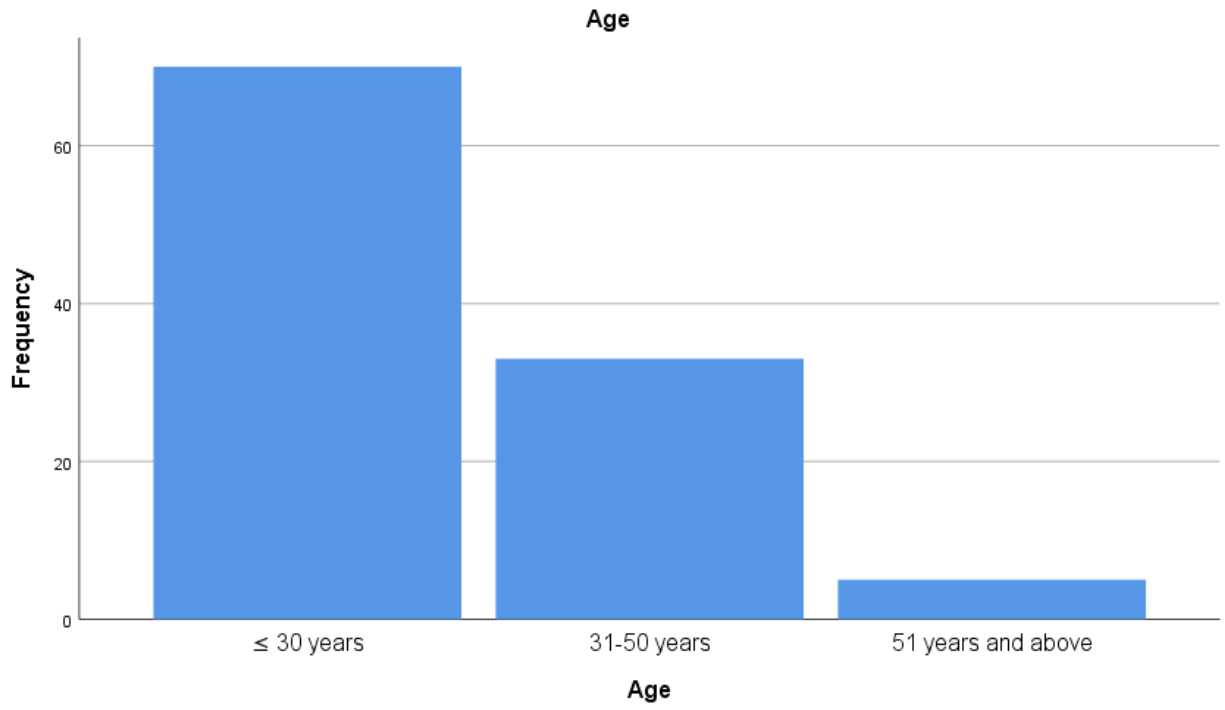


Figure 6: Age distibution of respondents

Figure 6 presents the age distribution of the respondents. The majority, 70 (64.8%), were aged ≤30 years, followed by 33 (30.6%) who were between 31–50 years, while only 5 (4.6%) were 51 years

and above. This shows that most respondents were young adults, with a smaller proportion in the middle-aged group and very few older adults.

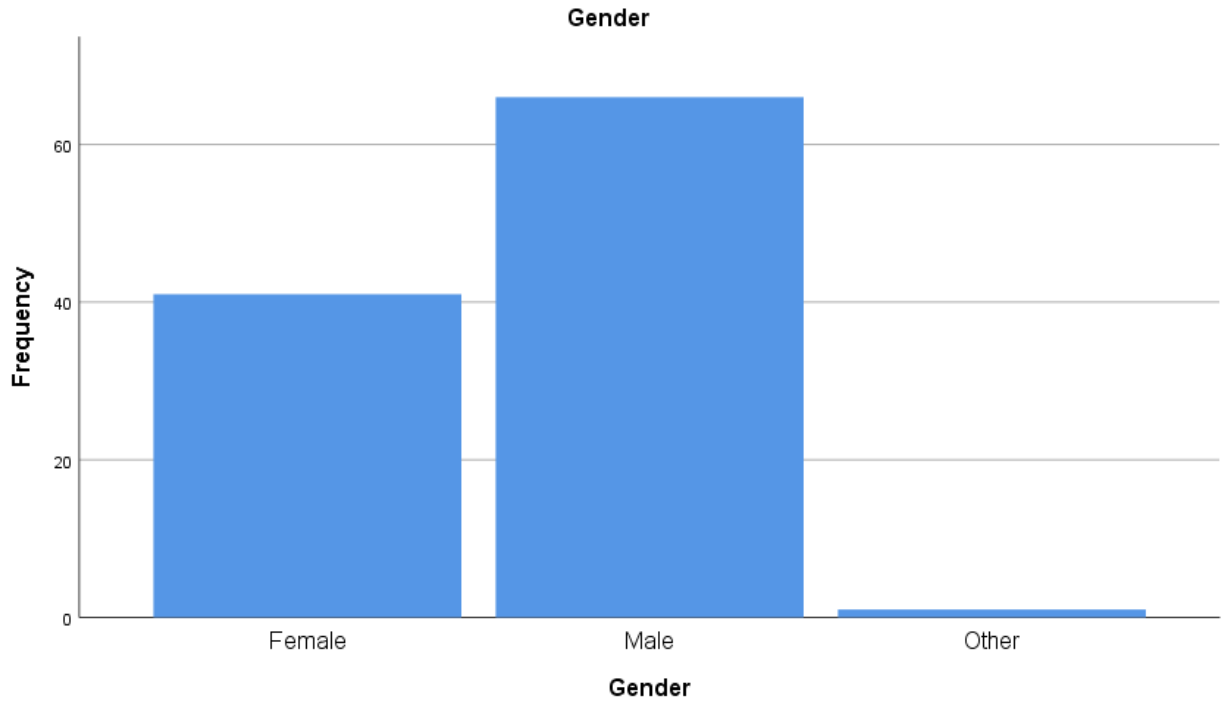


Figure 7: Gender distribution of respondents

Figure 7 presents the gender distribution of the respondents. A majority, 66 (61.1%), were male, followed by 41 (38.0%) who were female, while only 1 (0.9%) identified as other. This indicates that the sample was predominantly male, with females forming a smaller proportion and minimal representation of other genders.

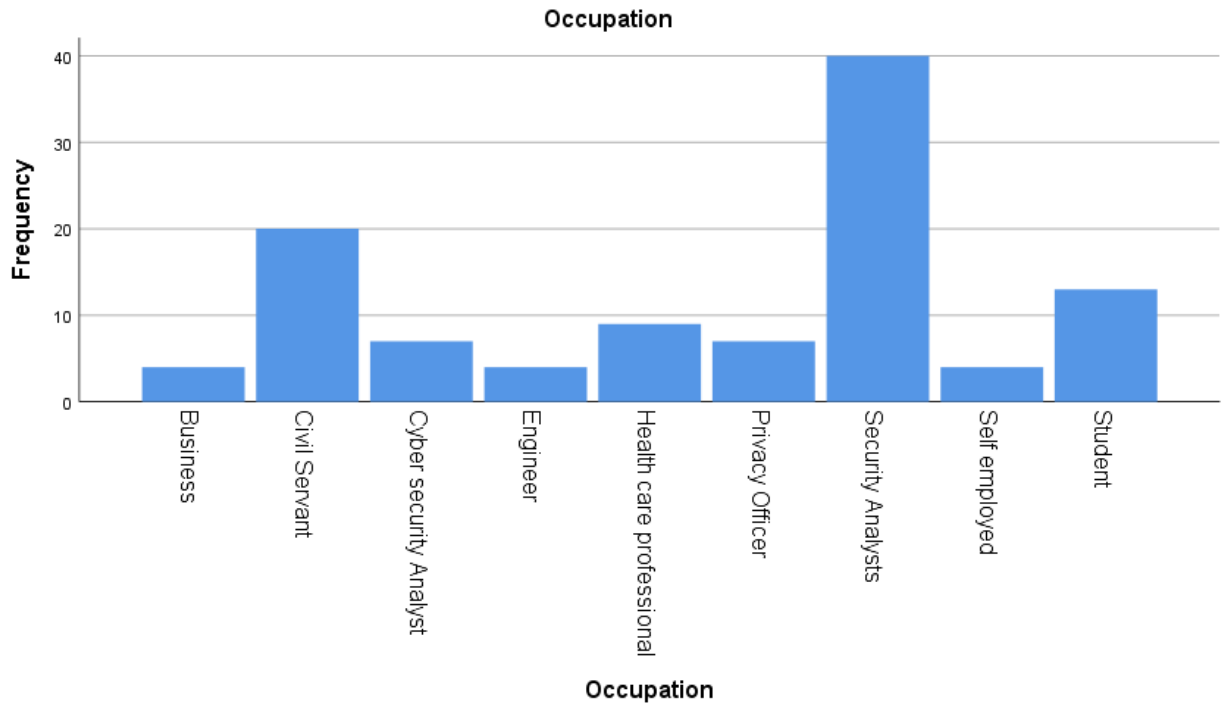


Figure 8: Occupational distribution of respondents

Figure 8 presents the occupational distribution of the respondents. The majority, 40 (37.0%), were security analysts, followed by 20 (18.5%) who were civil servants and 13 (12.0%) who were students. Other occupations included health care professionals 9 (8.3%), cyber security analysts 7 (6.5%), privacy officers 7 (6.5%), while business, engineers, and self-employed respondents each accounted for 4 (3.7%) of the total. This indicates that most participants were engaged in security-related roles, with relatively fewer respondents in other professional categories.

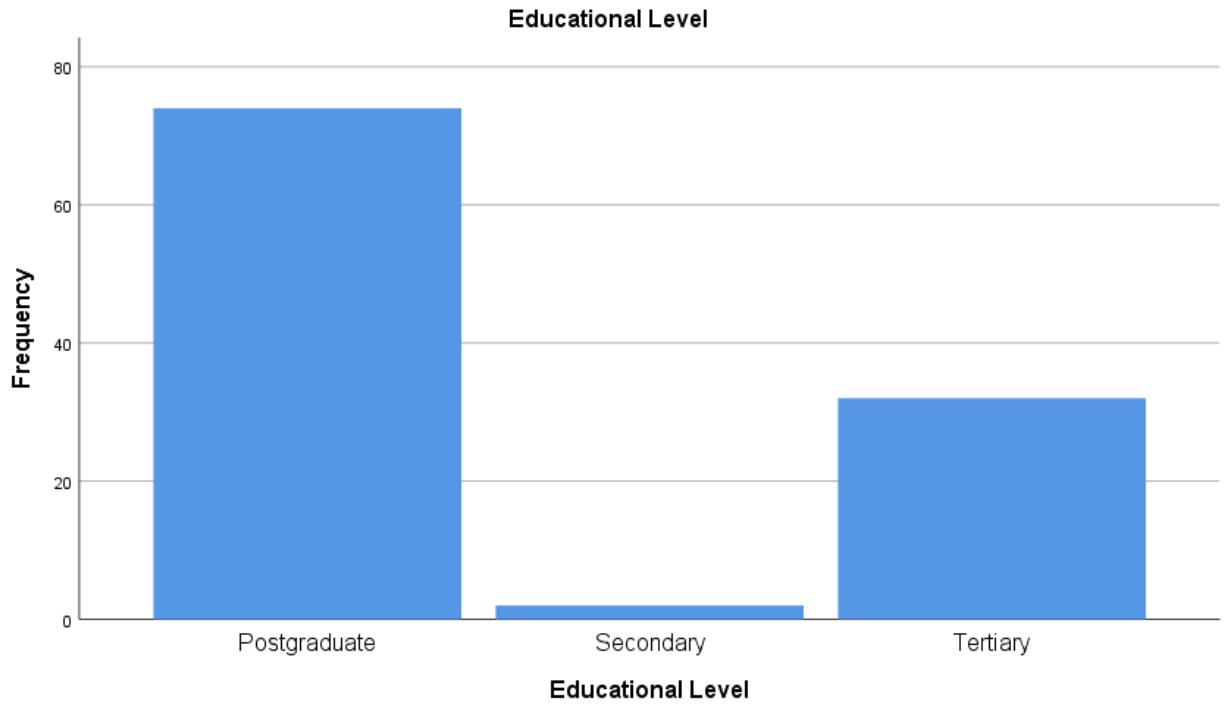


Figure 9: Educational Level of Respondents

Figure 9 presents the educational level of the respondents. The majority, 74 (68.5%), had postgraduate education, followed by 32 (29.6%) with tertiary education, while only 2 (1.9%) had secondary education.

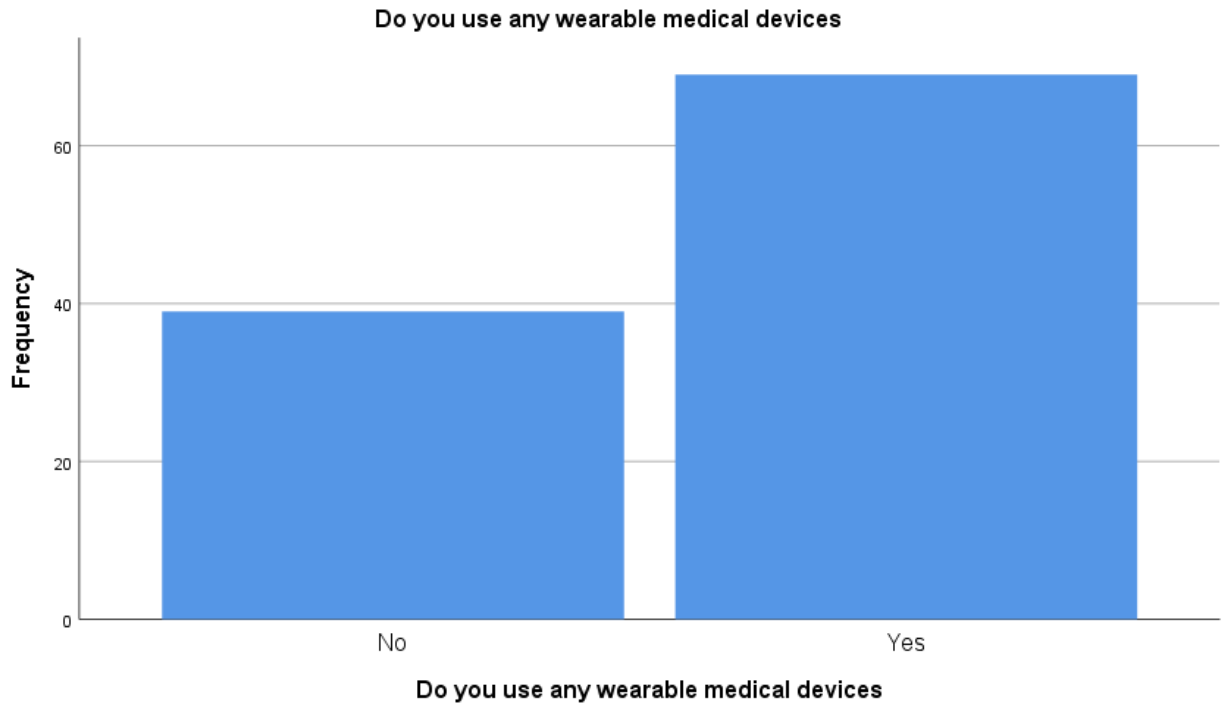


Figure 10: Distribution of respondents based on use of Wearable medical devices.

Figure 10 presents the distribution of respondents based on the use of wearable medical devices. A majority, 69 (63.9%), reported using wearable medical devices, while 39 (36.1%) indicated they did not use such devices.

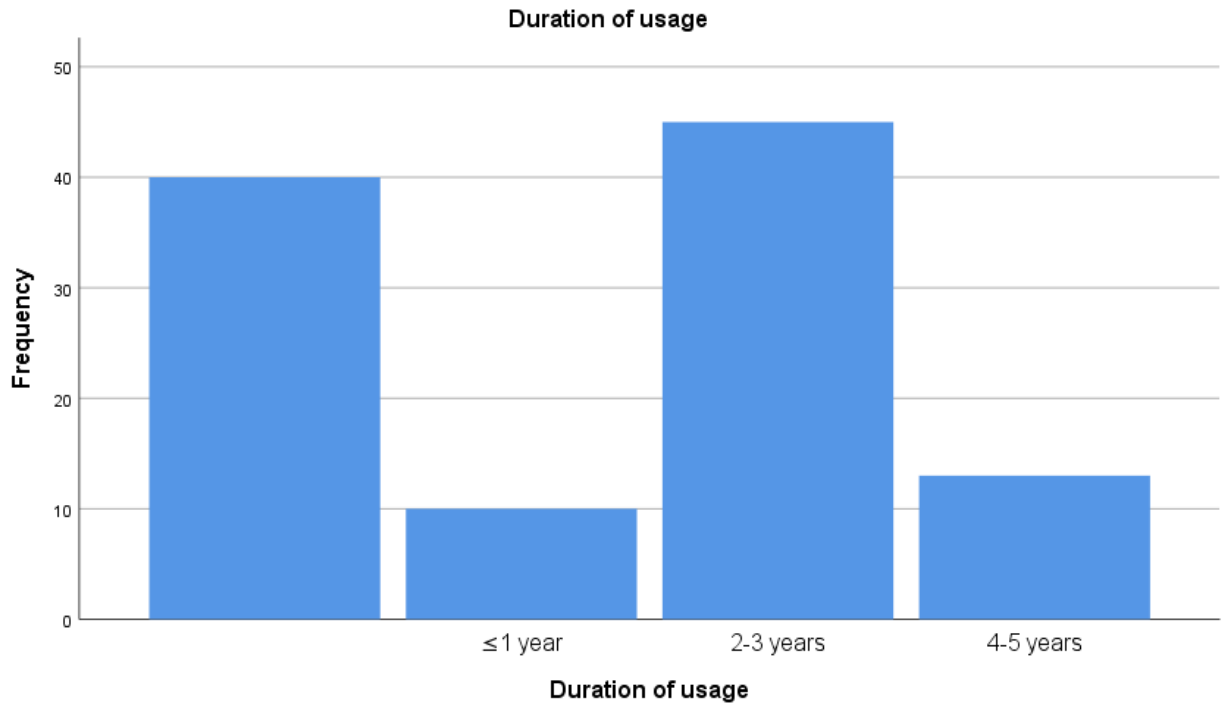


Figure 11: Duration of wearable medical device usage among respondents.

Figure 11 shows the duration of wearable medical device usage among respondents. A substantial proportion, 45 (41.7%), reported using the devices for 2–3 years, while 13 (12.0%) had used them for 4–5 years. Additionally, 10 (9.3%) indicated usage for one year or less, and 40 (37.0%) did not specify a duration (likely those who do not use such devices).

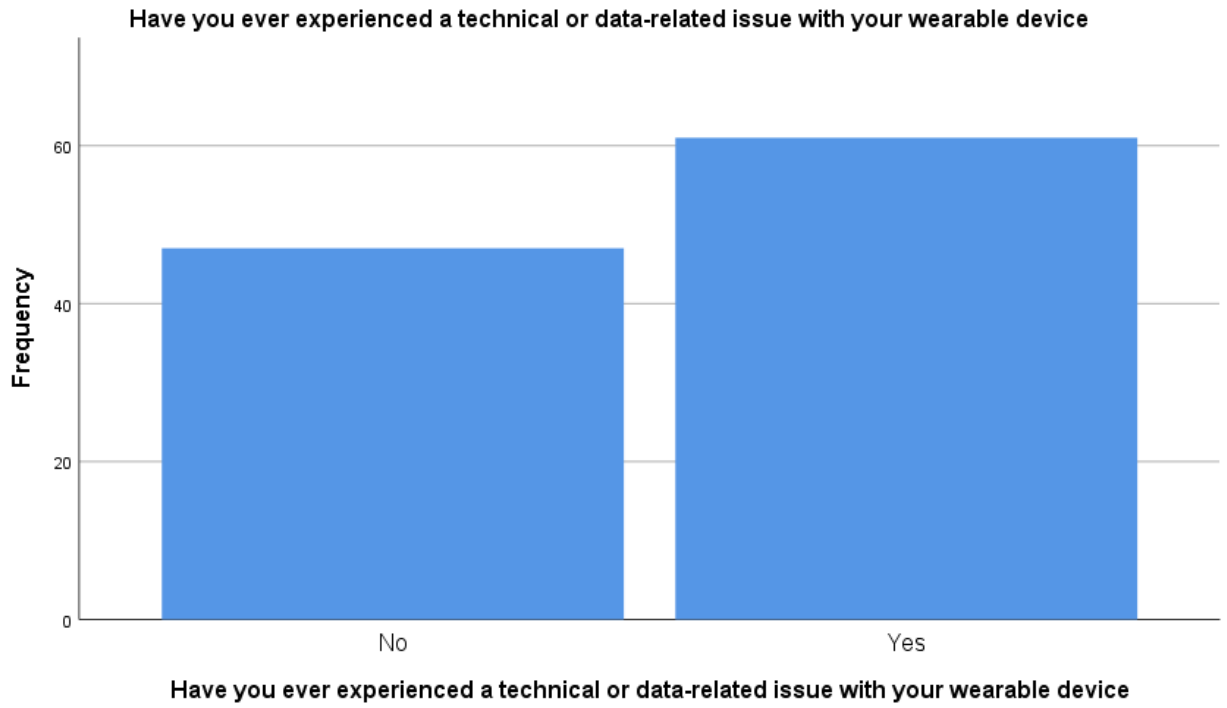


Figure 12: Distribution of respondents who have experienced technical or data-related issues with their wearable devices.

Figure 12 presents the distribution of respondents who have experienced technical or data-related issues with their wearable devices. A majority, 61 (56.5%), reported experiencing such issues, while 47 (43.5%) indicated no issues.

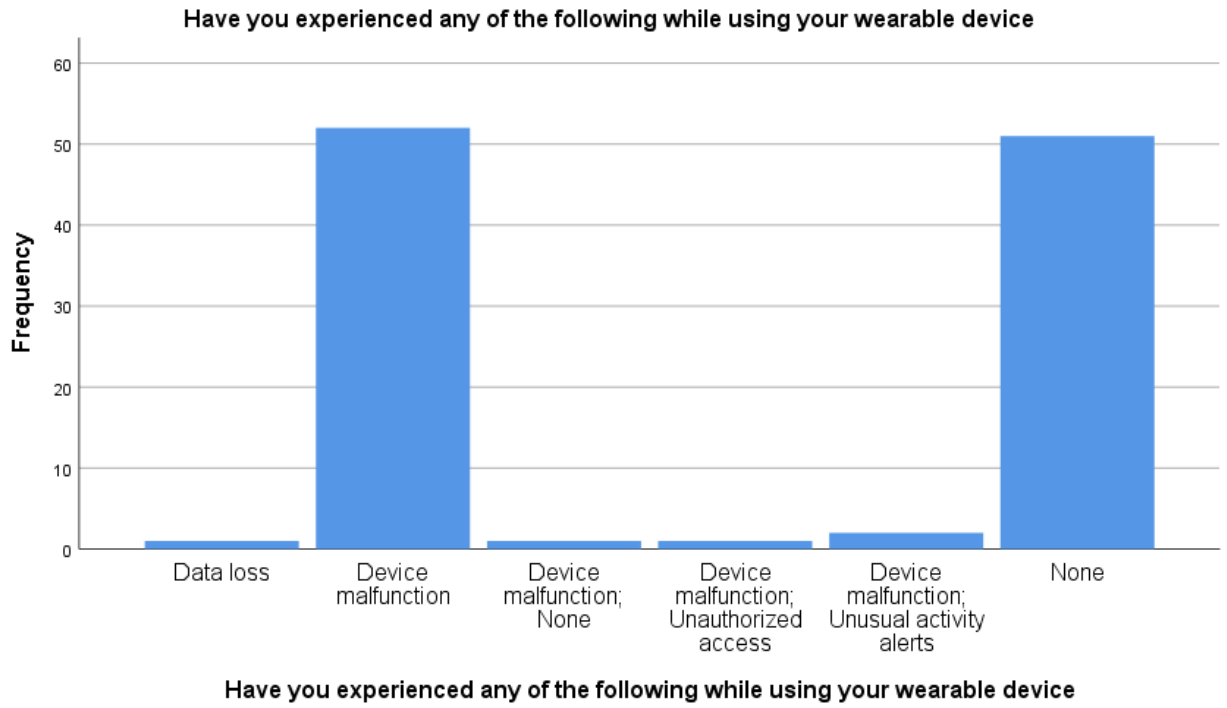


Figure 13: Distribution of specific issues experienced by respondents while using wearable devices

Figure 13 illustrates the distribution of specific issues experienced by respondents while using wearable devices. The most common problem reported was device malfunction, experienced by 52 (48.1%) of participants, followed by unusual activity alerts combined with device malfunction in 2 (1.9%) cases. A smaller proportion experienced data loss (0.9%), device malfunction with unauthorized access (0.9%), and device malfunction with none (0.9%). Notably, 51 respondents (47.2%) reported no issues at all.

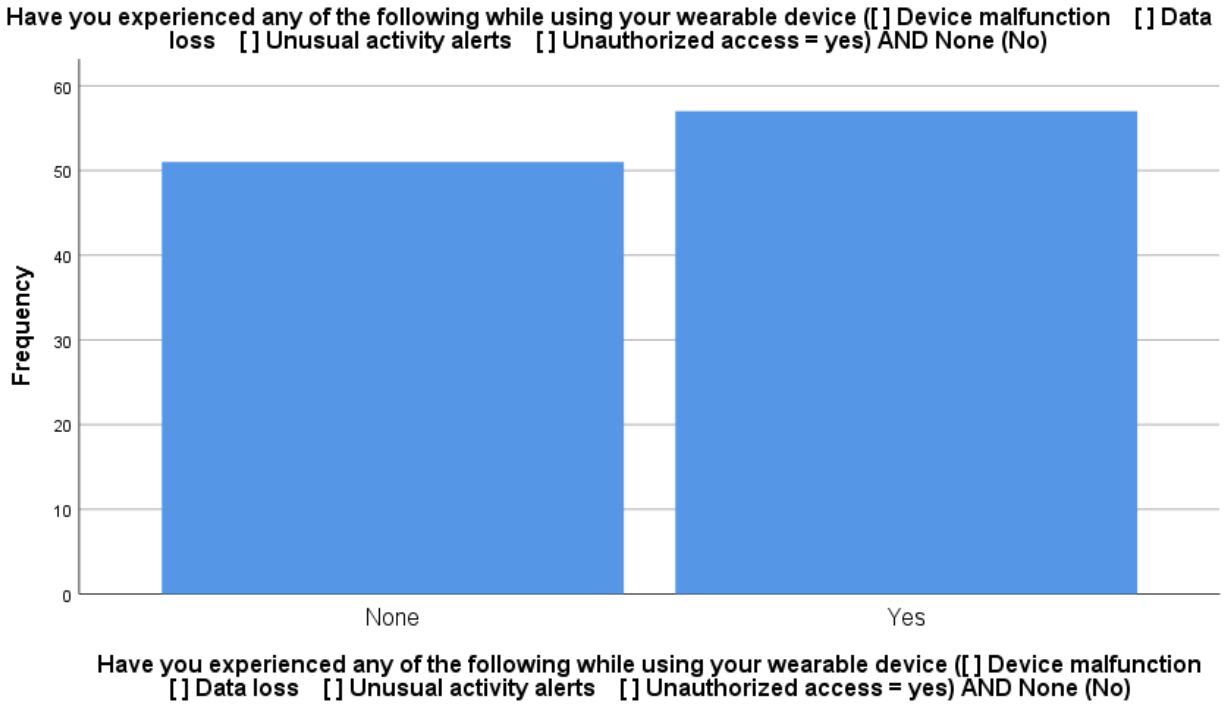


Figure 14: Distribution of respondents who reported experiencing at least one issue with their WMD compared to those who reported none.

Figure 14 shows the distribution of respondents who reported experiencing at least one issue with their wearable medical device compared to those who reported none. Out of 108 participants, 57 (52.8%) indicated "Yes", meaning they experienced at least one problem such as device malfunction, data loss, unusual activity alerts, or unauthorized access. In contrast, 51 (47.2%) reported "None", indicating no issues.

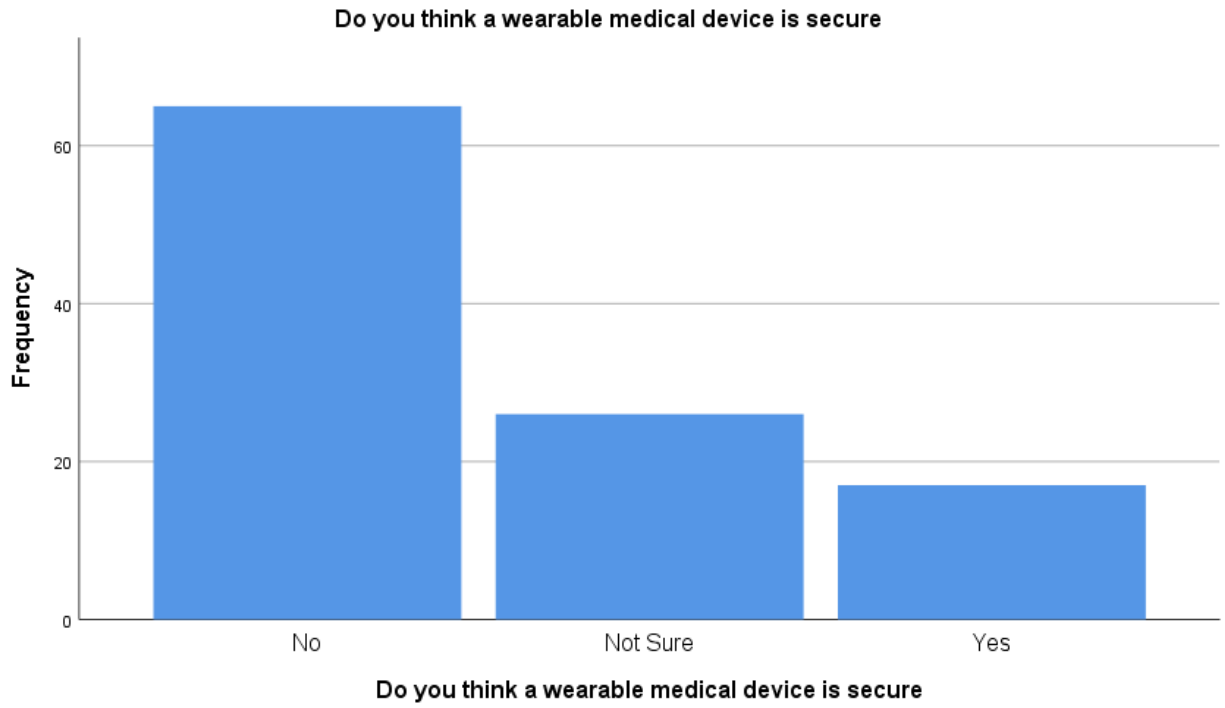


Figure 15: Respondents' perceptions of the security of wearable medical devices

Figure 15 illustrates respondents' perceptions of the security of wearable medical devices. Among the 108 participants, a majority **65 (60.2%)** believe these devices are **not secure**, **26 (24.1%)** are **not sure**, and only **17 (15.7%)** consider them **secure**.

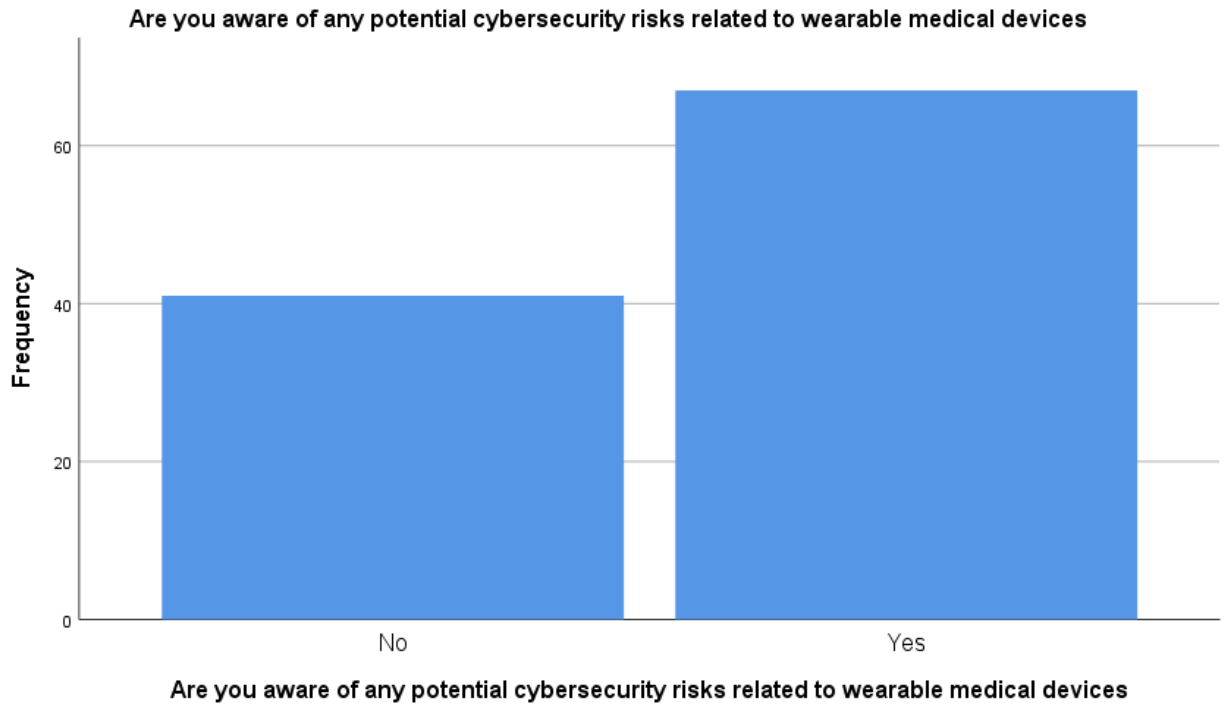


Figure 16: Awareness of potential cybersecurity risks associated with wearable medical devices.

Figure 16 shows awareness of potential cybersecurity risks associated with wearable medical devices. Out of 108 respondents, 67 (62.0%) reported being aware of such risks, while 41 (38.0%) indicated no awareness.

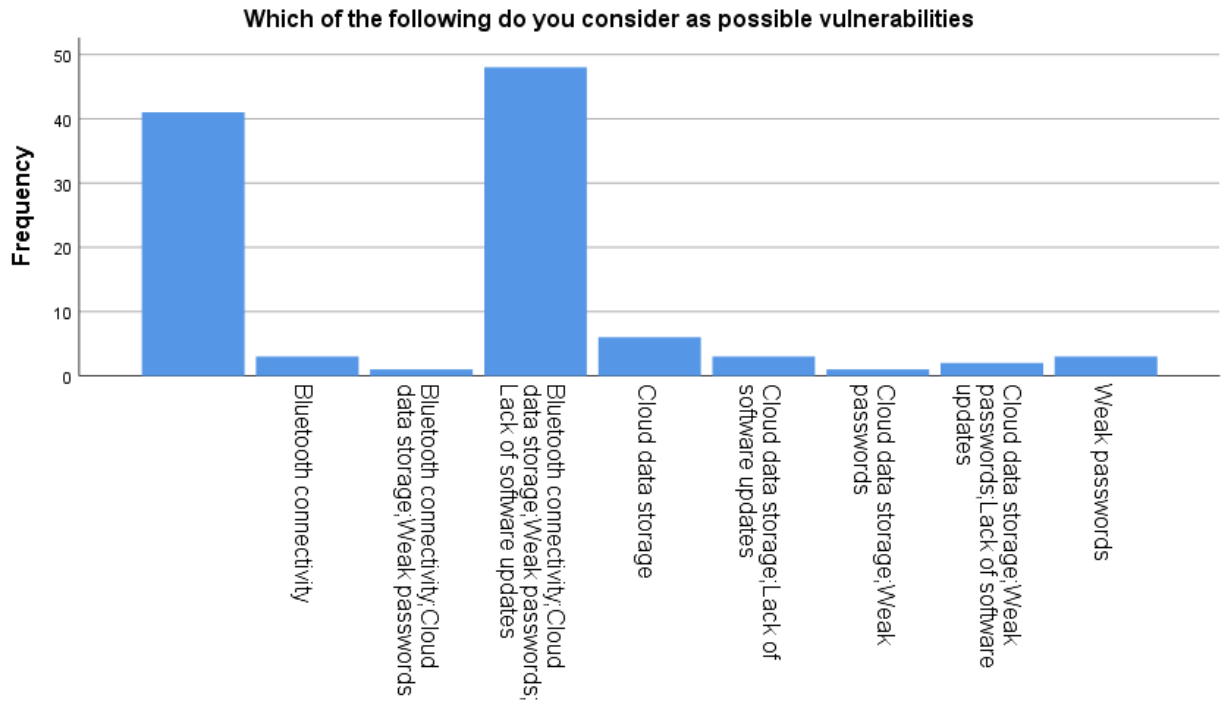


Figure 17: Possible vulnerabilities in wearable medical devices

Figure 17: Possible Vulnerabilities in Wearable Medical Devices

The analysis shows that the most frequently identified vulnerability was a combination of multiple factors, particularly Bluetooth connectivity, cloud data storage, weak passwords, and lack of software updates, reported by 48 respondents (44.4%). Individual vulnerabilities were less commonly cited, such as cloud data storage alone (6 respondents; 5.6%), Bluetooth connectivity alone (3 respondents; 2.8%), and weak passwords alone (3 respondents; 2.8%). A small proportion of participants recognized partial combinations of these factors, such as Bluetooth + cloud + weak passwords (0.9%) or cloud + lack of updates (2.8%). Notably, 41 respondents (38.0%) did not indicate any vulnerability, highlighting a knowledge gap.

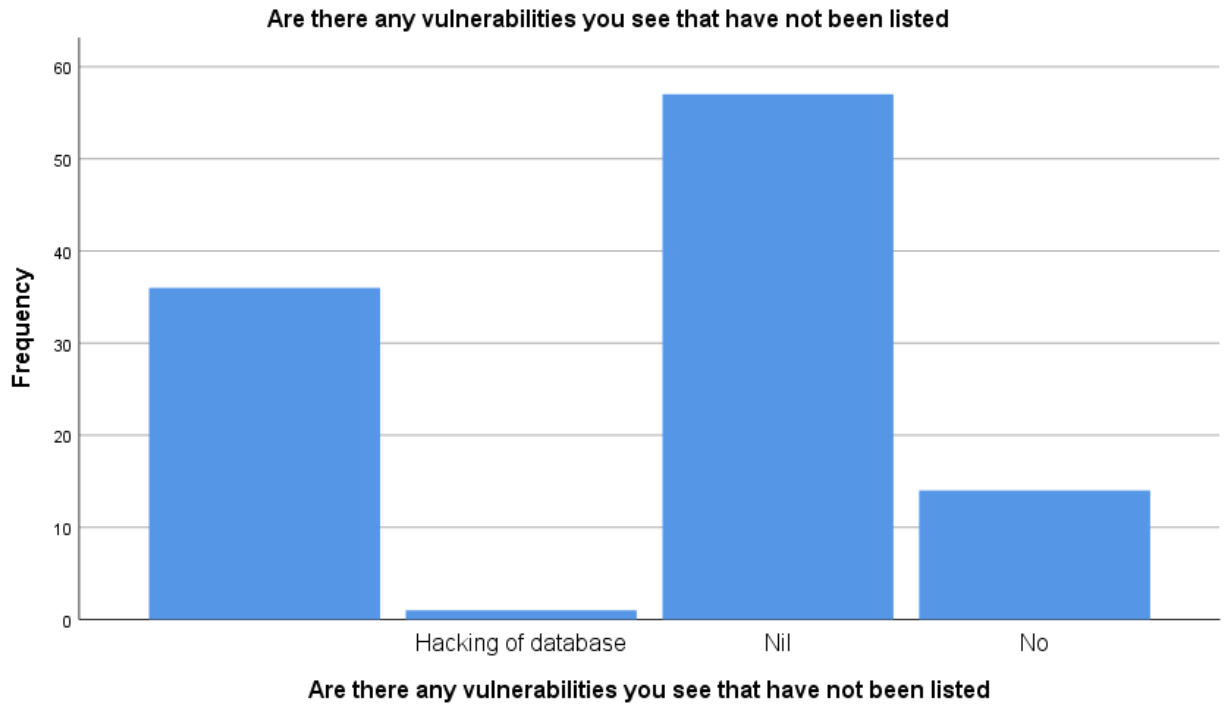


Figure 18: Responses regarding additional vulnerabilities beyond those listed.

Figure 18: presents the responses regarding additional vulnerabilities beyond those listed. A significant proportion, 57 (52.8%), stated "Nil," indicating that they did not identify any further vulnerabilities, while 14 (13.0%) explicitly responded "No." Notably, 36 (33.3%) respondents provided no response, which may suggest uncertainty or lack of awareness about additional risks. Only 1 respondent (0.9%) mentioned "hacking of database" as an additional vulnerability, highlighting minimal recognition of specific advanced threats among the participants.

4.2.2 Types of Health Monitoring Devices Used by Respondents

Table 2: Types of health monitoring devices used by respondents

Type of device used	Frequency	Percent
A Smart watch	1	0.9
Apple Watch	1	0.9
Blood Pressure	1	0.9
Blood pressure monitor	21	19.4
Blood pressure Monitor	1	0.9
Blood Pressure monitor	1	0.9
Blood Pressure Monitor	1	0.9
Blood pressure pump	1	0.9
BP machine	1	0.9
BP Monitor	1	0.9
fit bit sense	1	0.9
Fit bit sense	4	3.7
Fitness watch	1	0.9
glucose monitor	1	0.9
Insulin pump	21	19.4
Sleep apnea monitor	1	0.9
smart watch	1	0.9
Smart watch	4	3.7
Smart watch and Ren camera	1	0.9
Strava device	1	0.9
Tube for Hydrocephalus	1	0.9
Watch	2	1.9

Table 2 presents the types of health monitoring devices used by the respondents. The most commonly used devices were the blood pressure monitor 21 (19.4%) and the insulin pump 21 (19.4%). This was followed by the Fitbit Sense 4 (3.7%) and Smartwatch 4 (3.7%). Other devices reported included Watch 2 (1.9%), while a wide range of single responses (0.9% each) were recorded for devices such as Smartwatch and Ren camera, Strava device, tube for hydrocephalus, glucose monitor, sleep apnea monitor, fitness watch, Apple watch, BP machine, blood pressure pump, A smartwatch, and various forms of blood pressure monitors.

4.2.3 Usage, Experiences, and Perceptions of Wearable Medical Devices Among Respondents

Table 3: Usage, Experiences, and perceptions of wearable medical devices among respondents

		Frequency	Percent
Do you use any wearable medical devices	No	39	36.1
	Yes	69	63.9
Duration of usage	≤1 year	10	9.3
	2-3 years	45	41.7
	4-5 years	13	12.0
Have you ever experienced a technical or data-related issue with your wearable device	No	47	43.5
	Yes	61	56.5
Have you experienced any of the following while using your wearable device	Data loss	1	0.9
	Device malfunction	52	48.1
	Device malfunction;None	1	0.9
	Device malfunction;Unauthorized access	1	0.9
	Device malfunction;Unusual activity alerts	2	1.9
	None	51	47.2
Have you experienced any of the following while using your wearable device ([ ] Device malfunction [ ] Data loss [ ] Unusual activity alerts [ ] Unauthorized access = yes) AND None (No)	None	51	47.2
	Yes	57	52.8
Do you think a wearable medical device is secure	No	65	60.2
	Not Sure	26	24.1
	Yes	17	15.7
Are there any vulnerabilities you see that have not been listed	Hacking of database	1	0.9
	Nil	57	52.8
	No	14	13.0

The results in Table 3 show that a majority of respondents (69; 63.9%) reported using wearable medical devices, with most users (45; 41.7%) having used them for 2–3 years, while only a small proportion (10; 9.3%) had used them for less than a year. More than half (61; 56.5%) had experienced technical or data-related issues, with device malfunction being the most common challenge (52; 48.1%). When grouped, 57 (52.8%) acknowledged experiencing at least one of the listed issues (device malfunction, data loss, unusual activity alerts, or unauthorized access), while 51 (47.2%) reported none. Regarding perceptions of security, a substantial proportion (65; 60.2%) considered wearable medical devices insecure, while only 17 (15.7%) believed they were secure, and 26 (24.1%) were uncertain. Additionally, when asked about unlisted vulnerabilities, very few (1; 0.9%) mentioned hacking of databases, whereas over half (57; 52.8%) reported none, and 14 (13.0%) indicated "No."

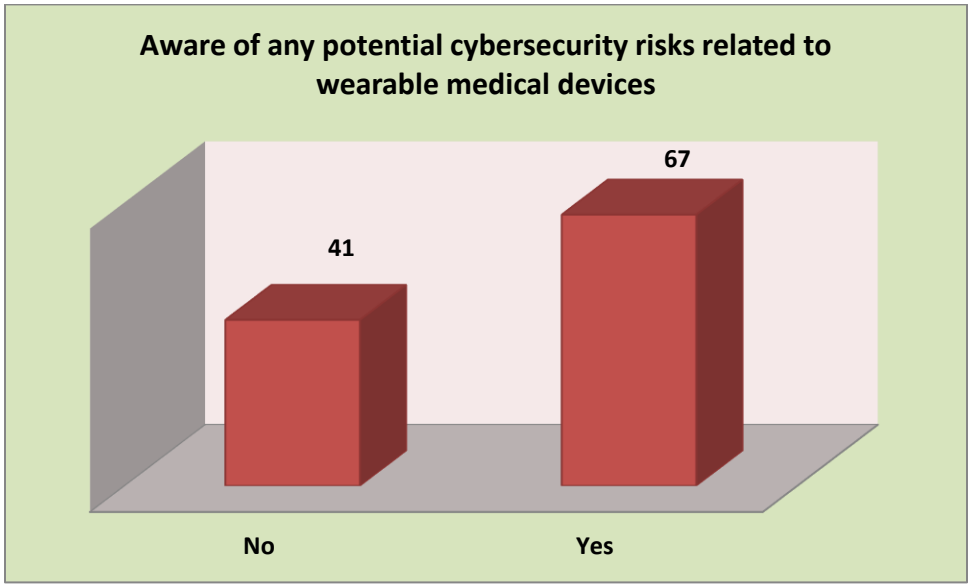


Figure 19: Awareness of Cybersecurity risks

Figure 19 shows that a majority of respondents, 67 (62.0%), reported being aware of potential cybersecurity risks related to wearable medical devices, while 41 (38.0%) indicated they were not aware.

4.2.4 Reported Security Vulnerabilities in Wearable Medical Devices

Table 4: Reported Security vulnerabilities in wearable medical devices

	Frequency	Percent
Bluetooth connectivity	3	2.8
Bluetooth connectivity;Cloud data storage;Weak passwords	1	0.9
Bluetooth connectivity;Cloud data storage;Weak passwords;Lack of software updates	48	44.4
Cloud data storage	6	5.6
Cloud data storage;Lack of software updates	3	2.8
Cloud data storage;Weak passwords	1	0.9
Cloud data storage;Weak passwords;Lack of software updates	2	1.9
Weak passwords	3	2.8

Table 4 reveals that the most frequently reported security vulnerability in wearable medical devices was a combination of Bluetooth connectivity, cloud data storage, weak passwords, and lack of software updates, reported by 48 (44.4%) respondents. Cloud data storage alone was identified by 6 (5.6%) respondents, while Bluetooth connectivity, weak passwords, and cloud data storage with lack of software updates were each reported by 3 (2.8%). More complex combinations such as cloud data storage with weak passwords and lack of software updates were cited by 2 (1.9%), and both Bluetooth connectivity with cloud storage and weak passwords as well as cloud data storage with weak passwords alone were reported by 1 (0.9%) each.

4.2.5 Respondents' views and practices on Wearable Device Cybersecurity

Table 5: Respondents' Views and Practices on Wearable Device Cybersecurity

Variable	SA	A	N	SD	D
My wearable medical device receives regular software/firmware updates.	8(7.4)	14(13.0)	16(14.8)	60(55.6)	10(9.3)
I am aware of the cybersecurity risks associated with wearable medical devices.	9(8.3)	11(10.2)	15(13.9)	12(11.1)	61(56.5)
My device is protected with strong authentication (e.g., password/biometric).	8(7.4)	16(14.8)	7(6.5)	14(13.0)	63(58.3)
I consider the wireless connection (e.g., Bluetooth/Wi-Fi) of my device secure.	6(5.6)	16(14.8)	13(12.0)	14(13.0)	59(54.6)
I have experienced suspicious or abnormal activity from my wearable device.	9(8.3)	18(16.7)	18(16.7)	7(6.5)	56(51.9)
I believe most wearable medical devices lack strong built-in cybersecurity.	9(8.3)	5(4.6)	20(18.5)	13(12.0)	61(56.5)
I feel that the manufacturer has prioritized security in my wearable device.	5(4.6)	13(12.0)	14(13.0)	13(12.0)	63(58.3)
My device uses encryption to protect sensitive health data during transmission.	7(6.5)	12(11.1)	19(17.6)	7(6.5)	63(58.3)
The security settings of my wearable device are user-friendly and accessible.	10(9.3)	59(54.6)	15(13.9)	13(12.0)	11(10.2)
I regularly review privacy and security policies related to my wearable device.	58(53.7)	18(16.7)	18(16.7)	3(2.8)	11(10.2)

Table 5 presents respondents' perceptions and practices regarding the cybersecurity of wearable medical devices. A large proportion disagreed that their devices receive regular software or firmware updates, with 60 (55.6%) strongly disagreeing and only 8 (7.4%) strongly agreeing. Similarly, 61 (56.5%) disagreed that they are aware of cybersecurity risks, while just 9 (8.3%) strongly agreed. More than half, 63 (58.3%), disagreed that their devices are protected with strong authentication, and the same number disagreed that encryption is used to protect sensitive data during transmission. Likewise, 63 (58.3%) felt manufacturers have not prioritized security. Although 59 (54.6%) agreed that security settings are user-friendly, actual secure practices were lacking. Interestingly, 58 (53.7%) strongly agreed that they regularly review privacy and security policies, reflecting user attentiveness despite perceived device vulnerabilities.

4.2.6: Repondents's perceptions and experiences on Cybersecurity Threats in Wearable Medical Devices

Table 6: Respondents' Perceptions and Experiences on Cybersecurity Threats in Wearable Medical Devices

Variable	Categories	Frequency	Percent
Do you believe a cyberattack on a wearable device could impact your health	No	12	11.1
	Not Sure	5	4.6
	Yes	91	84.3
Are you concerned about your personal health data being accessed by unauthorized persons	No	11	10.2
	Yes	97	89.8
Have you ever stopped using a device due to cybersecurity concerns	No	101	93.5
	Yes	7	6.5
Do you know anyone who has had a cybersecurity issue with their medical device	No	103	95.4
	Yes	5	4.6

Table 6 shows respondents' perceptions and experiences regarding cybersecurity threats in wearable medical devices. A majority, 91 (84.3%), believed that a cyberattack on a wearable device could impact their health, while 12 (11.1%) did not and 5 (4.6%) were unsure. Similarly,

97 (89.8%) expressed concern about their personal health data being accessed by unauthorized persons, compared to only 11 (10.2%) who were not concerned. Despite these concerns, most respondents, 101 (93.5%), reported never stopping the use of a device due to cybersecurity issues, with only 7 (6.5%) having discontinued usage for this reason. Furthermore, 103 (95.4%) indicated they do not personally know anyone who has experienced a cybersecurity issue with their medical device, while just 5 (4.6%) reported knowing someone affected.

4.2.7 Perceptions on Cybersecurity Risks of Wearable Medical Devices

Table 7: ***Perceptions on Cybersecurity Risks of Wearable Medical Devices***

Variable	SA	A	N	SD	D
A cyberattack on a wearable device could lead to incorrect health readings or diagnoses.	8(7.4)	7(6.5)	8(7.4)	15(13.9)	70(64.8)
I am concerned that cyber threats may compromise my personal health information.	10(9.3)	8(7.4)	14(13.0)	19(17.6)	57(52.8)
Cybersecurity breaches in wearable devices may cause harm to patients.	8(7.4)	9(8.3)	12(11.1)	15(13.9)	64(59.3)
Healthcare services are at risk due to vulnerabilities in wearable medical devices.	8(7.4)	9(8.3)	16(14.8)	16(14.8)	59(54.6)
Device hacking may result in loss or manipulation of critical health data.	8(7.4)	9(8.3)	5(4.6)	17(15.7)	69(63.9)
A compromised wearable device could affect trust in digital healthcare systems.	7(6.5)	7(6.5)	6(5.6)	23(21.3)	65(60.2)
I believe more safeguards are needed to reduce the risks posed by wearable medical devices.	7(6.5)	7(6.5)	11(10.2)	20(18.5)	63(58.3)

Table 7 presents respondents' perceptions of cybersecurity risks in wearable medical devices. A majority of respondents disagreed that a cyberattack could lead to incorrect health readings or diagnoses, with 70 (64.8%) disagreeing and 15 (13.9%) strongly disagreeing, while only 8 (7.4%) strongly agreed and 7 (6.5%) agreed. Similarly, most respondents, 57 (52.8%) and 19 (17.6%), disagreed or strongly disagreed, respectively, that cyber threats may compromise their personal

health information, while 10 (9.3%) strongly agreed and 8 (7.4%) agreed. On whether cybersecurity breaches may cause harm to patients, 64 (59.3%) disagreed and 15 (13.9%) strongly disagreed, compared to 8 (7.4%) who strongly agreed and 9 (8.3%) who agreed. Likewise, 59 (54.6%) disagreed and 16 (14.8%) strongly disagreed that healthcare services are at risk due to vulnerabilities in wearable devices, whereas 8 (7.4%) strongly agreed and 9 (8.3%) agreed. A large proportion, 69 (63.9%), disagreed and 17 (15.7%) strongly disagreed that device hacking may result in loss or manipulation of health data, while only 8 (7.4%) and 9 (8.3%) strongly agreed or agreed, respectively. Regarding the impact on trust in digital healthcare systems, 65 (60.2%) disagreed and 23 (21.3%) strongly disagreed, compared with just 7 (6.5%) strongly agreeing and 7 (6.5%) agreeing. Finally, the majority, 63 (58.3%) and 20 (18.5%), disagreed or strongly disagreed that more safeguards are needed, while only 7 (6.5%) strongly agreed and 7 (6.5%) agreed.

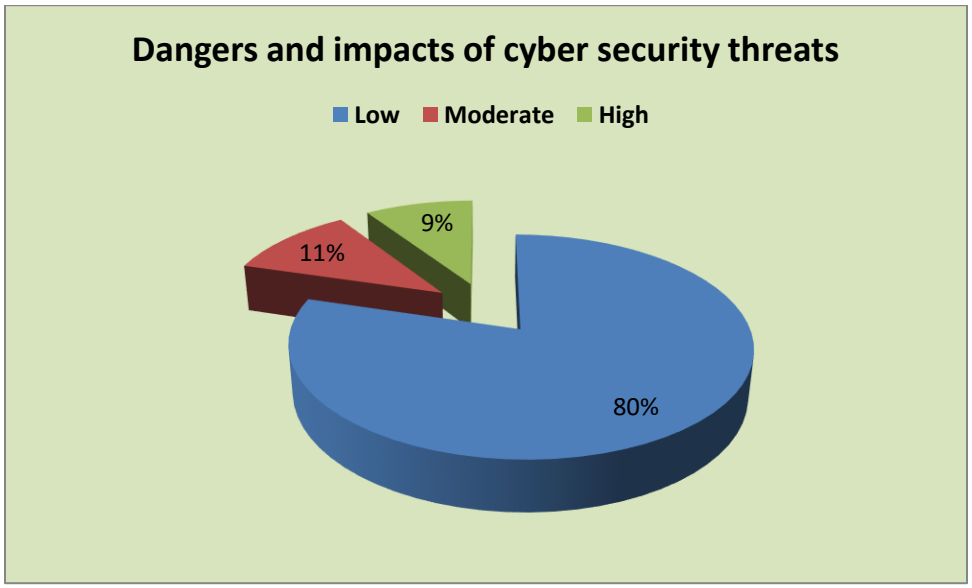


Figure 20: Dangers and impacts of cybersecurity threats

Figure 20 shows respondents' perceptions of the dangers and impacts of cybersecurity threats in wearable medical devices. A majority, 86 (79.6%), perceived the threats as *low*, while 12 (11.1%) considered them *moderate*, and only 10 (9.3%) rated them as *high*.

4.2.8 Perceptions of Dangers and Impacts of Cybersecurity

Table 8: ***Crosstab Summary: Perceptions of Dangers and Impacts of Cybersecurity***

Variable	Categories	Low	Moderate	High	Pearson Chi-Square (χ^2)	df	P-value
Age	≤30 years	56 (51.9%)	8 (7.4%)	6 (5.6%)	1.707	4	0.789
	31–50 years	25 (23.1%)	4 (3.7%)	4 (3.7%)			
	51 years and above	5 (4.6%)	0 (0.0%)	0 (0.0%)			
Gender	Female	31 (28.7%)	5 (4.6%)	5 (4.6%)	9.066	4	0.059
	Male	55 (50.9%)	6 (5.6%)	5 (4.6%)			
	Other	0 (0.0%)	1 (0.9%)	0 (0.0%)			
Occupation	Business	3 (2.8%)	0 (0.0%)	1 (0.9%)	50.936	16	0.000
	Civil Servant	16 (14.8%)	2 (1.9%)	2 (1.9%)			
	Cyber Security Analyst	6 (5.6%)	0 (0.0%)	1 (0.9%)			
	Engineer	2 (1.9%)	1 (0.9%)	1 (0.9%)			
	Health Care Professional	9 (8.3%)	0 (0.0%)	0 (0.0%)			
	Privacy Officer	7 (6.5%)	0 (0.0%)	0 (0.0%)			
	Security Analysts	39 (36.1%)	1 (0.9%)	0 (0.0%)			
	Self-employed	1 (0.9%)	2 (1.9%)	1 (0.9%)			
	Student	3 (2.8%)	6 (5.6%)	4 (3.7%)			
Educational Level	Postgraduate	67 (62.0%)	5 (4.6%)	2 (1.9%)	21.039	4	0.000
	Secondary	2 (1.9%)	0 (0.0%)	0 (0.0%)			
	Tertiary	17 (15.7%)	7 (6.5%)	8 (7.4%)			
Use of Wearable Medical Devices	No	23 (21.3%)	8 (7.4%)	8 (7.4%)	16.476	2	0.000
	Yes	63 (58.3%)	4 (3.7%)	2 (1.9%)			
Duration of Usage	>5 years	24 (22.2%)	8 (7.4%)	8 (7.4%)	19.739	6	0.003
	≤1 year	7 (6.5%)	2 (1.9%)	1 (0.9%)			
	2–3 years	43 (39.8%)	2 (1.9%)	0 (0.0%)			
	4–5 years	12 (11.1%)	0 (0.0%)	1 (0.9%)			

The analysis of Table 8 reveals several insights regarding the association between socio-demographic factors and respondents' perceptions of the dangers and impacts of cybersecurity threats. Firstly, regarding age groups, no significant association is observed ($\chi^2 = 1.707$, df = 4, p = 0.789), with respondents aged ≤30 years constituting the majority across all perception levels, while relatively fewer were observed among those aged 51 years and above. Similarly, gender

does not exhibit a statistically significant association ($\chi^2 = 9.066$, df = 4, p = 0.059), suggesting comparable perception levels between male and female respondents, although males were slightly more represented across all categories. However, occupation demonstrates a significant association ($\chi^2 = 50.936$, df = 16, p = 0.000), with security analysts (39, 36.1%) and civil servants (16, 14.8%) dominating the low-perception category, while students reported relatively higher levels of moderate and high perceptions. Educational level also shows a significant association ($\chi^2 = 21.039$, df = 4, p = 0.000), as postgraduate respondents (67, 62.0%) overwhelmingly dominated the low-perception category, while those with tertiary education reported higher proportions of moderate and high perceptions. Likewise, the use of wearable medical devices is significantly associated with perception ($\chi^2 = 16.476$, df = 2, p = 0.000), with non-users more likely to report moderate (8, 7.4%) and high (8, 7.4%) perceptions compared to users, who were predominantly in the low category (63, 58.3%). Finally, duration of usage also demonstrates a significant association ($\chi^2 = 19.739$, df = 6, p = 0.003), as respondents with over 5 years of usage reported the highest prevalence of moderate (8, 7.4%) and high (8, 7.4%) perceptions, contrasting with relatively lower levels among those with 2–3 years of usage (43, 39.8%) who mainly perceived the threats as low.

4.2.9 Respondents' Perceptions of Cybersecurity Riss in Wearable Medical Devices

Table 9: ***Respondents' Perceptions of Cybersecurity Risks in Wearable Medical Devices***

Variable	SA	A	N	SD	D
A cyberattack on a wearable device could lead to incorrect health readings or diagnoses.	8(7.4)	7(6.5)	8(7.4)	15(13.9)	70(64.8)
I am concerned that cyber threats may compromise my personal health information.	10(9.3)	8(7.4)	14(13.0)	19(17.6)	57(52.8)
Cybersecurity breaches in wearable devices may cause harm to patients.	8(7.4)	9(8.3)	12(11.1)	15(13.9)	64(59.3)
Healthcare services are at risk due to vulnerabilities in wearable medical devices.	8(7.4)	9(8.3)	16(14.8)	16(14.8)	59(54.6)
Device hacking may result in loss or manipulation of critical health data.	8(7.4)	9(8.3)	5(4.6)	17(15.7)	69(63.9)
A compromised wearable device could affect trust in digital healthcare systems.	7(6.5)	7(6.5)	6(5.6)	23(21.3)	65(60.2)
I believe more safeguards are needed to reduce the risks posed by wearable medical devices.	7(6.5)	7(6.5)	11(10.2)	20(18.5)	63(58.3)

The analysis of Table 9 highlights respondents' perceptions of cybersecurity risks in wearable medical devices, showing an overall high level of concern. A significant majority strongly disagreed that cyberattacks on wearable devices could lead to incorrect health readings or diagnoses (70, 64.8%), while only a small proportion strongly agreed (8, 7.4%). Similarly, most respondents disagreed that cyber threats could compromise their personal health information (57, 52.8%), although 10 (9.3%) strongly agreed, indicating some level of apprehension. With respect to potential patient harm, more than half disagreed (64, 59.3%), while 8 (7.4%) strongly agreed. A similar trend was observed regarding the risks posed to healthcare services, where 59 (54.6%) disagreed, while only 8 (7.4%) strongly agreed. Concerning data manipulation, 69 (63.9%) disagreed, contrasting with 8 (7.4%) who strongly agreed. Trust in digital healthcare systems was also questioned, with 65 (60.2%) disagreeing that compromised devices could affect trust, while 7 (6.5%) strongly agreed. Finally, regarding the need for safeguards, most respondents disagreed (63, 58.3%), though a smaller group (7, 6.5%) strongly agreed.

4.2.10 Perceived Measures to Improve Device Security

*Table 10: **Perceived Measures to Improve Device Security***

Which of the following do you think would improve device security	Frequency	Percent
Regular software updates	10	9.3
Stronger encryption;Regular software updates;User education	4	3.7
Stronger encryption;Two-factor authentication	1	0.9
Stronger encryption;Two-factor authentication;Regular software updates;User education	70	64.8
Stronger encryption;Two-factor authentication;User education	4	3.7
Two-factor authentication	8	7.4
Two-factor authentication;Regular software updates	5	4.6
User education	6	5.6

Table 10 shows that the majority of respondents 70 (64.8%) indicated that a comprehensive combination of stronger encryption, two-factor authentication, regular software updates, and user education would best improve device security. This was followed by 10 (9.3%) who selected regular software updates alone, while 8 (7.4%) opted for two-factor authentication only, and 6 (5.6%) emphasized user education as a single measure. Additionally, 5 (4.6%) preferred a combination of two-factor authentication and regular software updates, 4 (3.7%) suggested stronger encryption with regular software updates and user education, another 4 (3.7%) recommended stronger encryption with two-factor authentication and user education, and only 1 (0.9%) considered stronger encryption with two-factor authentication alone.

4.2.11 Recommendations to Improve the safety of wearable devices

Table 11: ***Recommendations to Improve the Safety of Wearable Devices***

		Frequency	Percent
	Would you be willing to pay more for a wearable device with guaranteed cybersecurity protection	Frequency	Percent
Would you be willing to pay more for a wearable device with guaranteed cyber-security protection		64	59.3
What recommendations would you offer manufacturers to improve the safety of wearable devices	Better encryption	5	4.6
	Customer services improvement and education is sacrosanct, automatic upgrade is advised at the right time, cyber treats alarming systems should be installed in the devices and finally, update implementation policies should be manufacturers priority	2	1.9
	Educate the user if their are possible distortion on devices information, how to identify it, particularly information not from the manufacturer end and	2	1.9
	I'd recommend occasionally orientation and discussion concerning user experience and collect data to improve on security and performance	3	2.8
	Manufacturers should update their devices annually.	3	2.8
	Nil	82	75.9
	Stronger encryption	4	3.7
	They should improve device security by engaging in user education	7	6.5

Table 11 shows that a majority of respondents, 64 (59.3%), indicated willingness to pay more for wearable devices with guaranteed cybersecurity protection, while 82 (75.9%) offered no recommendations for manufacturers. Among those who provided suggestions, 7 (6.5%) recommended improving device security through user education, 5 (4.6%) suggested better encryption, and 4 (3.7%) emphasized stronger encryption. Other specific recommendations included occasional user orientation and data collection for performance improvement 3 (2.8%),

annual device updates 3 (2.8%), improved customer service with timely upgrades and alarm systems 2 (1.9%), and educating users on detecting possible information distortions 2 (1.9%).

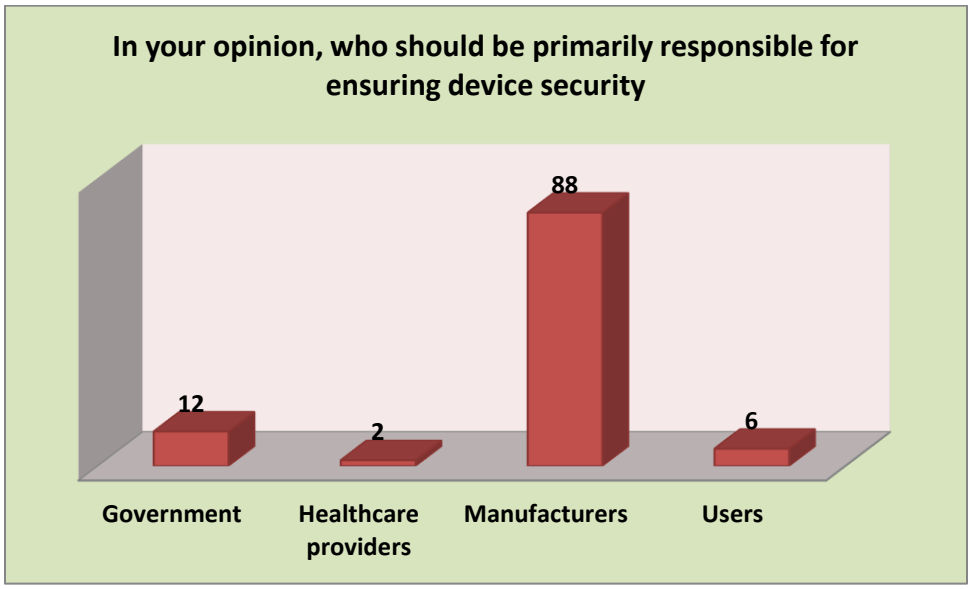


Figure 21: Opinions of respondents for who should primarily be responsible for ensuring device security

Figure 21 reveals that the majority of respondents, 88 (81.5%), believe manufacturers should be primarily responsible for ensuring the security of wearable devices. A smaller proportion, 12 (11.1%), assigned this responsibility to the government, while only 6 (5.6%) considered users responsible, and 2 (1.9%) pointed to healthcare providers.

4.2.12 Perceptions on Cybersecurity Regulations and Practices for Wearable Medical devices

*Table 12: **Perceptions on Cybersecurity Regulations and Practices for Wearable Medical Devices***

Variable	SA	A	N	SD	D
Manufacturers should be mandated to meet minimum cybersecurity standards for wearable medical devices.	8(7.4)	8(7.4)	4(3.7)	15(13.9)	73(67.6)
Cybersecurity training should be provided to users of wearable medical devices.	13(12.0)	3(2.8)	7(6.5)	20(18.5)	65(60.2)
Third-party cybersecurity audits should be required before devices are released to the market.	5(4.6)	8(7.4)	11(10.2)	16(14.8)	68(63.0)
Healthcare providers should offer technical support to patients on device cybersecurity practices.	7(6.5)	3(2.8)	11(10.2)	20(18.5)	67(62.0)
Devices should include real-time threat alerts and automatic security updates.	5(4.6)	4(3.7)	9(8.3)	14(13.0)	76(70.4)
Users should have greater control over the privacy and security settings of their wearable medical devices.	10(9.3)	2(1.9)	8(7.4)	13(12.0)	75(69.4)
There should be stricter penalties for manufacturers that fail to protect users' data.	7(6.5)	5(4.6)	11(10.2)	12(11.1)	73(67.6)
Wearable devices should require multi-factor authentication before access is granted.	11(10.2)	3(2.8)	6(5.6)	17(15.7)	71(65.7)
Encryption protocols should be mandatory for all wearable medical devices.	9(8.3)	5(4.6)	3(2.8)	18(16.7)	73(67.6)
Governments should implement universal security certification for medical IoT devices.	8(7.4)	5(4.6)	12(11.1)	12(11.1)	71(65.7)

Table 12 shows respondents' perceptions of cybersecurity regulations and practices for wearable medical devices. The majority strongly disagreed across most items, indicating a prevailing skepticism or lack of support for stricter cybersecurity interventions. For instance, 73 (67.6%) strongly disagreed that manufacturers should be mandated to meet minimum cybersecurity standards, while 65 (60.2%) strongly disagreed with the need for cybersecurity training for users. Similarly, 68 (63.0%) strongly disagreed with the requirement of third-party audits before device release, and 67 (62.0%) strongly disagreed that healthcare providers should provide cybersecurity

support. Furthermore, most respondents rejected advanced security features such as real-time threat alerts and automatic updates, with 76 (70.4%) strongly disagreeing, and 75 (69.4%) strongly disagreed with giving users greater control over privacy and security settings. Likewise, 73 (67.6%) strongly disagreed with imposing stricter penalties on manufacturers for failing to protect users' data, while 71 (65.7%) opposed multi-factor authentication and government-implemented universal security certification. Encryption protocols were also rejected by 73 (67.6%) respondents.

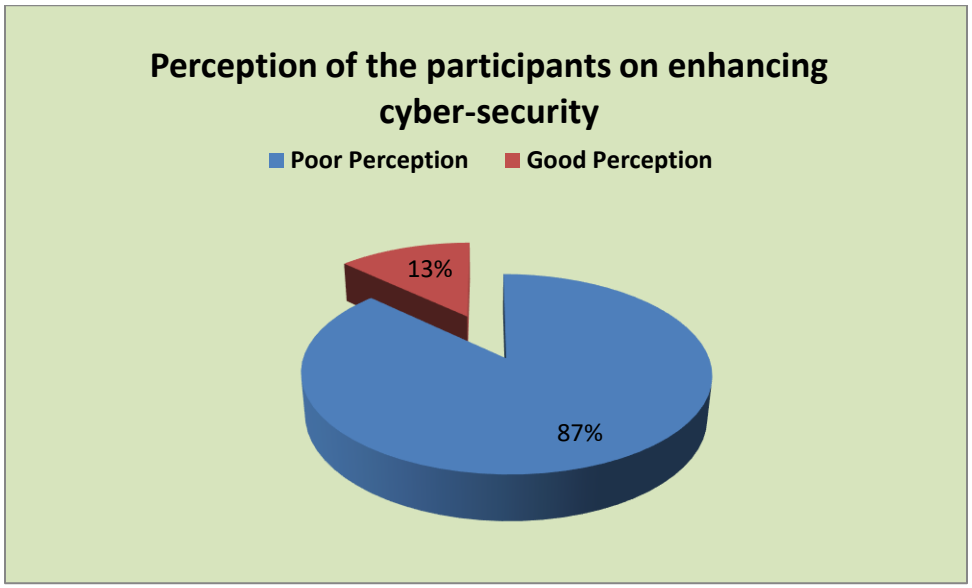


Figure 22: Perceptions of the participants on enhancing cybersecurity

Figure 22 illustrates the participants' perception of measures to enhance cybersecurity in wearable medical devices. A large majority, 94 (87.0%), demonstrated poor perception, indicating limited awareness or understanding of effective cybersecurity practices. In contrast, only 14 (13.0%) of the respondents showed good perception, reflecting a small proportion with adequate knowledge or favorable attitudes toward enhancing device security.

4.2.13 Perception of participants on enhancing cybersecurity

Table 13: ***Crosstab Summary of Perception of Participants on Enhancing Cybersecurity***

Variable	Categories	Poor Perception	Good Perception	Total	Pearson Chi-Square (χ^2)	Df	P-value
Age	≤30 years	63 (58.3%)	7 (6.5%)	70 (64.8%)	3.28	2	0.194
	31–50 years	26 (24.1%)	7 (6.5%)	33 (30.6%)			
	51 years and above	5 (4.6%)	0 (0.0%)	5 (4.6%)			
Gender	Female	37 (34.3%)	4 (3.7%)	41 (38.0%)	7.115	2	0.029
	Male	57 (52.8%)	9 (8.3%)	66 (61.1%)			
	Other	0 (0.0%)	1 (0.9%)	1 (0.9%)			
Occupation	Business	3 (2.8%)	1 (0.9%)	4 (3.7%)	21.346	8	0.006
	Civil Servant	17 (15.7%)	3 (2.8%)	20 (18.5%)			
	Cyber Security Analyst	6 (5.6%)	1 (0.9%)	7 (6.5%)			
	Engineer	3 (2.8%)	1 (0.9%)	4 (3.7%)			
	Health Care Professional	8 (7.4%)	1 (0.9%)	9 (8.3%)			
	Privacy Officer	7 (6.5%)	0 (0.0%)	7 (6.5%)			
	Security Analysts	40 (37.0%)	0 (0.0%)	40 (37.0%)			
	Self-employed	3 (2.8%)	1 (0.9%)	4 (3.7%)			
	Student	7 (6.5%)	6 (5.6%)	13 (12.0%)			
Educational Level	Postgraduate	71 (65.7%)	3 (2.8%)	74 (68.5%)	18.507	2	0.000
	Secondary	2 (1.9%)	0 (0.0%)	2 (1.9%)			
	Tertiary	21 (19.4%)	11 (10.2%)	32 (29.6%)			
Use of Wearable Medical Devices	No	28 (25.9%)	11 (10.2%)	39 (36.1%)	12.57	1	0.000
	Yes	66 (61.1%)	3 (2.8%)	69 (63.9%)			
Duration of Usage	≤1 year	8 (7.4%)	2 (1.9%)	10 (9.3%)	14.953	3	0.002
	2–3 years	45 (41.7%)	0 (0.0%)	45 (41.7%)			
	4–5 years	12 (11.1%)	1 (0.9%)	13 (12.0%)			
	>5 years	29 (26.9%)	11 (10.2%)	40 (37.0%)			

The analysis of Table 13 provides insights into the association between socio-demographic factors and participants' perception of enhancing cybersecurity in wearable medical devices. Regarding age, there is no significant association observed ($\chi^2 = 3.28$, df = 2, p = 0.194), with participants aged ≤30 years representing the majority of those with poor perception. Gender, however, shows a significant association ($\chi^2 = 7.115$, df = 2, p = 0.029), indicating that males (57, 52.8%) and females (37, 34.3%) differ in their perception levels, with males showing higher prevalence of poor perception. Occupation is also significantly associated with perception ($\chi^2 = 21.346$, df = 8, p = 0.006), where security analysts (40, 37.0%) and civil servants (17, 15.7%) constitute the largest proportion with poor perception, while students display a relatively higher proportion with good perception (6, 5.6%). Educational level demonstrates a strong significant association ($\chi^2 = 18.507$, df = 2, p = 0.000), with postgraduate respondents predominantly exhibiting poor perception (71, 65.7%), whereas tertiary-educated participants have a higher proportion of good perception (11, 10.2%). Use of wearable medical devices is significantly associated with perception ($\chi^2 = 12.57$, df = 1, p = 0.000), as non-users show better perception (11, 10.2%) compared to users (3, 2.8%). Finally, duration of usage is also significantly related to perception ($\chi^2 = 14.953$, df = 3, p = 0.002), with those using devices for >5 years showing the highest proportion of good perception (11, 10.2%) while users with 2–3 years of experience mainly demonstrate poor perception (45, 41.7%).

4.2.14 Awareness of potential cybersecurity risks related to Wearable Medical Devices

*Table 14: **Awareness of Potential Cybersecurity Risks Related to Wearable Medical Devices***

Variable	Categories	No	Yes	Total	df	P-value
Age	≤30 years	25 (23.1%)	45 (41.7%)	70 (64.8%)	2	0.140
	31–50 years	12 (11.1%)	21 (19.4%)	33 (30.6%)		
	51 years and above	4 (3.7%)	1 (0.9%)	5 (4.6%)		
Gender	Female	15 (13.9%)	26 (24.1%)	41 (38.0%)	2	0.704
	Male	26 (24.1%)	40 (37.0%)	66 (61.1%)		
	Other	0 (0.0%)	1 (0.9%)	1 (0.9%)		
Occupation	Business	4 (3.7%)	0 (0.0%)	4 (3.7%)	8	0.000
	Civil Servant	13 (12.0%)	7 (6.5%)	20 (18.5%)		
	Cyber Security Analyst	2 (1.9%)	5 (4.6%)	7 (6.5%)		
	Engineer	2 (1.9%)	2 (1.9%)	4 (3.7%)		
	Health Care Professional	7 (6.5%)	2 (1.9%)	9 (8.3%)		
	Privacy Officer	0 (0.0%)	7 (6.5%)	7 (6.5%)		
	Security Analysts	2 (1.9%)	38 (35.2%)	40 (37.0%)		
	Self-employed	3 (2.8%)	1 (0.9%)	4 (3.7%)		
	Student	8 (7.4%)	5 (4.6%)	13 (12.0%)		
Educational Level	Postgraduate	19 (17.6%)	55 (50.9%)	74 (68.5%)	2	0.000
	Secondary	2 (1.9%)	0 (0.0%)	2 (1.9%)		
	Tertiary	20 (18.5%)	12 (11.1%)	32 (29.6%)		
Use of Wearable Medical Devices	No	27 (25.0%)	12 (11.1%)	39 (36.1%)	1	0.000
	Yes	14 (13.0%)	55 (50.9%)	69 (63.9%)		
Duration of Usage	>5 years	27 (25.0%)	13 (12.0%)	40 (37.0%)	3	0.000
	≤1 year	4 (3.7%)	6 (5.6%)	10 (9.3%)		
	2–3 years	3 (2.8%)	42 (38.9%)	45 (41.7%)		
	4–5 years	7 (6.5%)	6 (5.6%)	13 (12.0%)		

The analysis of Table 14 reveals several insights regarding the association between socio-demographic factors and awareness of potential cybersecurity risks related to wearable medical

devices. Firstly, regarding age groups, there is no significant association observed (p = 0.140), although respondents aged ≤30 years constitute the largest proportion of those aware (45, 41.7%), compared to lower numbers among participants aged 31–50 years (21, 19.4%) and 51 years and above (1, 0.9%). Gender also does not exhibit a significant association with awareness (p = 0.704), indicating similar levels of awareness between male (40, 37.0%) and female respondents (26, 24.1%). In contrast, occupation demonstrates a significant association with awareness (p = 0.000), with security analysts (38, 35.2%) and privacy officers (7, 6.5%) showing higher awareness, whereas business respondents (0, 0.0%) and other professions report lower awareness. Educational level is significantly associated with awareness (p = 0.000), as postgraduate respondents (55, 50.9%) exhibit the highest awareness compared to tertiary (12, 11.1%) and secondary-educated participants (0, 0.0%). Use of wearable medical devices also shows a significant association (p = 0.000), with users (55, 50.9%) more aware than non-users (12, 11.1%). Finally, duration of usage is significantly associated with awareness (p = 0.000), with respondents using devices for 2–3 years (42, 38.9%) being the most aware, whereas those with usage >5 years (13, 12.0%) demonstrate lower awareness.

4.2.15 Prevalence of Wearable Device Issues

Table 15: ***Crosstab Summary of Prevalence of Wearable Device Issues***

Variable	Categories	None	Yes	Total	Pearson Chi-Square (χ^2)	df	P-value
Age	≤30 years	30 (27.8%)	40 (37.0%)	70 (64.8%)	1.573	2	0.455
	31–50 years	18 (16.7%)	15 (13.9%)	33 (30.6%)			
	51+ years	3 (2.8%)	2 (1.9%)	5 (4.6%)			
Gender	Female	19 (17.6%)	22 (20.4%)	41 (38.0%)	0.95	2	0.622
	Male	32 (29.6%)	34 (31.5%)	66 (61.1%)			
	Other	0 (0.0%)	1 (0.9%)	1 (0.9%)			
Occupation	Business	3 (2.8%)	1 (0.9%)	4 (3.7%)	47.829	8	0
	Civil Servant	13 (12.0%)	7 (6.5%)	20 (18.5%)			
	Cybersecurity Analyst	3 (2.8%)	4 (3.7%)	7 (6.5%)			
	Engineer	4 (3.7%)	0 (0.0%)	4 (3.7%)			
	Health Professional	6 (5.6%)	3 (2.8%)	9 (8.3%)			
	Privacy Officer	1 (0.9%)	6 (5.6%)	7 (6.5%)			
	Security Analyst	5 (4.6%)	35 (32.4%)	40 (37.0%)			
	Self-employed	3 (2.8%)	1 (0.9%)	4 (3.7%)			
	Student	13 (12.0%)	0 (0.0%)	13 (12.0%)			
Educational Level	Postgraduate	24 (22.2%)	50 (46.3%)	74 (68.5%)	20.992	2	0
	Secondary	2 (1.9%)	0 (0.0%)	2 (1.9%)			
	Tertiary	25 (23.1%)	7 (6.5%)	32 (29.6%)			
Use of Wearable Medical Devices	No	36 (33.3%)	3 (2.8%)	39 (36.1%)	49.787	1	0
	Yes	15 (13.9%)	54 (50.0%)	69 (63.9%)			
Duration of Usage	≤1 year	5 (4.6%)	5 (4.6%)	10 (9.3%)	55.938	3	0
	2–3 years	4 (3.7%)	41 (38.0%)	45 (41.7%)			
	4–5 years	6 (5.6%)	7 (6.5%)	13 (12.0%)			
	>5 years	36 (33.3%)	4 (3.7%)	40 (37.0%)			

The analysis of Table 15 reveals several insights regarding the prevalence of issues associated with wearable medical devices and their association with socio-demographic and usage characteristics. Firstly, age does not exhibit a significant association with device issues ($\chi^2 = 1.573$, df = 2, p = 0.455), although respondents aged ≤30 years reported the highest number of issues (40, 37.0%) compared to those aged 31–50 years (15, 13.9%) and 51+ years (2, 1.9%). Similarly, gender is not significantly associated with device issues (p = 0.622), indicating comparable prevalence between males (34, 31.5%) and females (22, 20.4%). In contrast, occupation shows a significant association ($\chi^2 = 47.829$, df = 8, p = 0.000), with security analysts reporting the highest prevalence of issues (35, 32.4%), while students (0, 0.0%) and other occupations report fewer problems. Educational level is also significantly associated ($\chi^2 = 20.992$, df = 2, p = 0.000), as postgraduate respondents (50, 46.3%) experience more issues than tertiary (7, 6.5%) and secondary-educated participants (0, 0.0%). Use of wearable medical devices demonstrates a significant association with issues ($\chi^2 = 49.787$, df = 1, p = 0.000), with users (54, 50.0%) reporting more problems than non-users (3, 2.8%). Finally, duration of usage is significantly associated with prevalence of device issues ($\chi^2 = 55.938$, df = 3, p = 0.000), where respondents using devices for 2–3 years (41, 38.0%) report the highest incidence, contrasting with lower prevalence among those with usage >5 years (4, 3.7%).

4.2.16 Analysis of factors influencing perception of device security

*Table 16: **Bivariate Analysis of Factors Influencing Perception of Device Security***

Table 4.16: Bivariate Analysis of Factors Influencing Perception of Device Security

Variable	Categories	Poor Perception	Good Perception	Total	P-value	P-value OR(CL)
Age	≤30 years	63 (58.3%)	7 (6.5%)	70 (64.8%)	1	1 Ref
	31–50 years	26 (24.1%)	7 (6.5%)	33 (30.6%)	0.427	1.873 (0.398–8.809)
	51 years and above	5 (4.6%)	0 (0.0%)	5 (4.6%)	0.842	
Gender	Female	37 (34.3%)	4 (3.7%)	41 (38.0%)		1 Ref
	Male	57 (52.8%)	9 (8.3%)	66 (61.1%)	0.558	1.677 (0.297–9.460)
	Other	0 (0.0%)	1 (0.9%)	1 (0.9%)	1.000	
Occupation	Business	3 (2.8%)	1 (0.9%)	4 (3.7%)	0.958	1 Ref
	Civil Servant	17 (15.7%)	3 (2.8%)	20 (18.5%)	0.771	0.640 (0.031–13.010)
	Cyber Security Analyst	6 (5.6%)	1 (0.9%)	7 (6.5%)	0.909	1.236 (0.033–46.521)
	Engineer	3 (2.8%)	1 (0.9%)	4 (3.7%)	0.786	1.665 (0.042–66.122)
	Health Care Professional	8 (7.4%)	1 (0.9%)	9 (8.3%)	0.680	0.482 (0.015–15.405)
	Privacy Officer	7 (6.5%)	0 (0.0%)	7 (6.5%)	0.999	
	Security Analysts	40 (37.0%)	0 (0.0%)	40 (37.0%)	0.997	
	Self-employed	3 (2.8%)	1 (0.9%)	4 (3.7%)		
	Student	7 (6.5%)	6 (5.6%)	13 (12.0%)		
Educational Level	Postgraduate	71 (65.7%)	3 (2.8%)	74 (68.5%)		1 Ref
	Secondary	2 (1.9%)	0 (0.0%)	2 (1.9%)	0.674	2.331 (0.045–119.788)
	Tertiary	21 (19.4%)	11 (10.2%)	32 (29.6%)	0.496	2.792 (0.145–53.578)
Use of Wearable Medical Devices	No	28 (25.9%)	11 (10.2%)	39 (36.1%)	0.306	1 Ref
	Yes	66 (61.1%)	3 (2.8%)	69 (63.9%)	0.999	
Duration of Usage	≤1 year	8 (7.4%)	2 (1.9%)	10 (9.3%)		1 Ref
	2–3 years	45 (41.7%)	0 (0.0%)	45 (41.7%)	0.124	3.907 (0.688–22.178)
	4–5 years	12 (11.1%)	1 (0.9%)	13 (12.0%)	1.000	
	>5 years	29 (26.9%)	11 (10.2%)	40 (37.0%)	0.827	

Table 16 shows that most demographic and device usage variables did not significantly influence respondents' perceptions of wearable medical device security, as indicated by P-values greater than 0.05 across all comparisons. Gender differences were not statistically significant (P = 0.944), suggesting similar awareness levels among males and females. Age groups also showed no significant association (P = 0.467), although respondents aged 31–40 years were 2.50 times more likely to perceive security risks compared to those aged ≤30 years (OR = 2.50, 95% CI: 0.21–29.66). Educational level and professional category similarly showed no significant association (P = 0.840 and P = 0.623, respectively), with slight variations in odds ratios. Device usage experience (P = 0.595) and prior training on cybersecurity (P = 0.402) were also not significant, though trained respondents were more likely to perceive security risks (OR = 1.56, 95% CI: 0.55–4.39). Overall, none of the variables demonstrated a statistically significant effect, indicating that awareness of cybersecurity risks in wearable medical devices appears to be relatively consistent across demographic and experiential groups.

4.3 Analysis and Discussion

4.3.1 Socio demographic of the participants

The socio demographic profile of our sample predominantly ≤30 years (64.8%), majority male (61.1%), and highly educated (68.5% postgraduate), with sizeable representation from security-focused occupations (e.g., security analysts 37% and cybersecurity analysts 6.5%) is consistent with a technically literate respondent pool and helps explain a strong emphasis on endpoint hardening, secure-by-design, and zero-trust network controls for wearable medical devices, but it may also influence perceptions toward technical rather than clinical workflow risks. Comparative literature shows that, in health systems, vulnerabilities are rarely purely technical: human error, underinvestment, complex device ecosystems, and legacy infrastructure repeatedly surface as root causes that shape risk in practice (Ewoh & Vartiainen, 2024). In hospital settings, large-scale emulations of multi-vector threats demonstrate that once a foothold is gained often via phishing or poorly segmented networks connected endpoints (including wearables and patient monitors) can facilitate lateral movement and data exfiltration, amplifying patient-safety risk (Bracciale *et al.,* 2023). Wearable-specific studies corroborate that common communication stacks particularly

Bluetooth Low Energy remain susceptible during discovery and pairing, enabling passive eavesdropping and traffic inference and, in poorly configured contexts, active manipulation (Silva-Trujillo *et al.,* 2023). Yet, purely cryptographic or protocol fixes are insufficient: epistemic issues around data quality, interoperability, and representativeness influence downstream safety (e.g., false alarms, bias), and thus mitigation must integrate standards for data fidelity, SBOM transparency, and governance for data sharing (Canali *et al.,* 2022). From a cross-sector lens, recent analyses warn that consumer-grade wearables entering clinical pathways import supply-chain risks (opaque components, insecure firmware, backdoors) that technical respondents like those dominating our sample are likelier to recognize and prioritize; recommended countermeasures include hardware roots-of-trust, TPM-backed attestation, and zero-trust deployments, alongside regulatory levers that require lifecycle patching and SBOMs (Ostermann *et al.,* 2025). Taken together, our relatively young, security-skilled, postgraduate-heavy cohort plausibly over indexes on advanced mitigations (e.g., attestation, segmentation) and may underweight sociotechnical barriers commonly reported by clinicians and administrators such as training gaps, alert fatigue, and legacy integration despite these being pivotal to realized safety (Ewoh & Vartiainen, 2024). The convergence of these findings supports a layered strategy for wearable medical device cybersecurity: (1) protocol-level protections for pairing, authentication, and on-device encryption to neutralize well-documented radio attacks (Silva-Trujillo *et al.,* 2023); (2) hospital and home-care network controls (micro-segmentation, continuous monitoring) to limit blast radius from inevitable intrusions (Bracciale *et al.,* 2023); (3) data-centric governance to ensure measurement validity, metadata provenance, and equitable performance (Canali *et al.,* 2022); and (4) supply-chain security and regulatory compliance (SBOMs, secure-by-design, postmarket patching) to address upstream hardware/firmware threats (Ostermann *et al.,* 2025). Accordingly, while our sample's expertise likely elevates awareness of sophisticated mitigations, future work should intentionally include more clinicians and end-users to balance technical depth with implementation realities across care settings (Ewoh & Vartiainen, 2024).

4.3.2 Types of Health Monitoring Devices Used by Respondents

The distribution of health-monitoring devices among respondents, as presented in Table 4.2, highlights both the heterogeneity and concentration of wearable medical device (WMD) used

across categories, with blood pressure monitors (19.4%) and insulin pumps (19.4%) representing the most common devices, followed by smartwatches (combined 5.5% when variations such as "Smart watch" and "Apple Watch" are considered) and Fitbit devices (4.6%), while other specialized monitors (e.g., glucose monitor, sleep apnea monitor, hydrocephalus tube) were rarely reported (≤0.9%). This pattern highlights the increasing reliance on cardiovascular and diabetes-related monitoring technologies, which reflects global epidemiological burdens of hypertension and diabetes as primary chronic conditions where WMD adoption is highest (Kumar *et al.,* 2023). Such concentration of device usage has cybersecurity implications, as high adoption rates amplify attack surfaces and create attractive targets for adversaries. Indeed, studies demonstrate that blood pressure monitors and insulin pumps, often connected to mobile applications and cloud platforms, are vulnerable to unauthorized data access, man-in-the-middle attacks, and even direct manipulation of therapeutic functions (Hernandez-Ramos *et al.,* 2022). The fact that many respondents used different nomenclatures ("BP machine," "BP Monitor," etc.) for the same category suggests variations in user familiarity with technical specifications, which can influence security practices, such as firmware updating and authentication management. Comparative research has shown that user comprehension of device architecture is critical to secure use: for instance, weak literacy around Bluetooth Low Energy protocols has been associated with increased risks of eavesdropping and spoofing attacks in fitness trackers and clinical wearables (Silva-Trujillo *et al.,* 2023). Furthermore, insulin pumps represent a particularly high-risk category because of their direct therapeutic action; real-world analyses confirm that wireless vulnerabilities can allow attackers to alter insulin dosing, with potentially life-threatening consequences (Deeb *et al.,* 2021). These risks have led to regulatory bodies such as the FDA and EMA emphasizing "security-by-design" principles, where encryption, secure boot, and authenticated over-the-air updates are mandated for devices with critical therapeutic roles. The relatively lower representation of general wellness devices (e.g., Strava device, generic smart watches) suggests that this cohort is more medically oriented than consumer-fitness oriented, which is consistent with findings that patients with chronic conditions demonstrate higher wearable adherence compared to general populations (Piwek *et al.,* 2020). However, the cybersecurity posture differs between consumer-grade and clinically certified devices: consumer devices are often less rigorously

regulated, and studies have shown that their APIs and cloud interfaces are frequent vectors of data leakage (Canali *et al.,* 2022). Interestingly, the inclusion of rare devices like hydrocephalus tubes and sleep apnea monitors in this sample reflects niche but clinically sensitive domains, where security breaches could endanger patients by disrupting life-sustaining interventions or misreporting critical physiological data (Ostermann *et al.,* 2025). Taken together, the comparative device distribution reveals that while the majority of risks cluster around cardiovascular and diabetes-related wearables, niche devices should not be ignored due to the severity of impact in small patient subgroups. This aligns with recent cross-sector analyses emphasizing that mitigation strategies must be tiered: widespread devices (blood pressure monitors, insulin pumps) require population-scale security solutions (mandatory encryption, SBOM transparency, automated patching), whereas specialized devices need tailored risk assessments, redundancy planning, and clinical oversight to ensure resilience against cyber threats (Ewoh & Vartiainen, 2024). In the end, the study emphasizes how cybersecurity risk exposure, device prevalence, and user familiarity interact, highlighting the need for comprehensive strategies that incorporate both technical safeguards and user-centered awareness initiatives to address vulnerabilities in the quickly changing wearable medical device ecosystem.

4.3.3 Usage, Experiences, and Perceptions of WMDs Among Respondents

63.9% of participants reported active device usage and 41.7% of them have between two and three years of experience. The analysis of respondents' usage experiences, and perceptions of wearable medical devices (WMDs) reveals a complex interplay between adoption, technical reliability, and cybersecurity awareness, suggesting that engagement with these technologies is quite common. But the fact that 56.5% of participants said they have experienced technical or data-related problems, notably device breakdowns (48.1%) and, to a lesser degree, anomalous activity warnings, illegal access, and data loss, shows enduring weaknesses that weaken confidence in WMDs. This is consistent with Hernandez-Ramos et al. (2022), who discovered that wirelessly equipped glucose monitors and insulin pumps frequently had communication issues, were vulnerable to illegal access, and had insecure mobile app integration-all of which jeopardize privacy and safety. 60.2% of respondents voiced open mistrust and just 15.7% of respondents

thought WMDs were secure. This in line with other research showing that wearables are viewed as high-risk technology by clinicians and patients because of frequent instances of data breaches and hacking incidents (Ewoh & Vartiainen, 2024). Interestingly, the high incidence of malfunctions mirrors clinical observations where firmware bugs, poor interoperability, and weak encryption mechanisms result in device unreliability, reinforcing calls for secure-by-design approaches in health IoT (Bracciale *et al.,* 2023). Comparatively, Canali et al. (2022) emphasized that beyond technical failures, issues of data fidelity and fairness in WMD analytics can exacerbate risks, particularly when devices misreport physiological data or fail to capture diverse populations, leading to inequitable clinical outcomes. The observed low frequency of explicit data loss (0.9%) and unauthorized access (0.9%) in this sample may underrepresent the true prevalence, as prior systematic reviews indicate that patients often lack awareness of backend data breaches affecting cloud-hosted WMD platforms (Ostermann *et al.,* 2025). Moreover, while almost half of respondents reported “no issues,” the near-equal split between those who had and had not faced problems underscores a divided user experience, suggesting that while some devices achieve stable performance, others remain vulnerable to operational and cybersecurity challenges. The finding that 52.8% confirmed encountering at least one security-related problem (device malfunction, data loss, unauthorized access, or unusual activity) is consistent with Silva-Trujillo et al. (2023), who demonstrated that smartwatch communication channels can be exploited for passive attacks and data interception, underscoring the broader susceptibility of wearable platforms. The skepticism evident in this study is significant for adoption and regulatory policy: if the majority of users do not believe WMDs are secure, adoption may plateau despite their clinical promise, particularly in chronic disease management where adherence depends on trust (Kumar *et al.,* 2023). A participant showed concern about "hacking of databases” and indicates that they are aware of systemic vulnerabilities that extend beyond device endpoints. This supports research that emphasizes cross-sectoral risk management, which includes strong governance frameworks, supply chain security, and secure cloud infrastructure (Ewoh & Vartiainen, 2024; Ostermann *et al*., 2025). When combined, these results highlight the necessity of a multi-layered reduction approach, which includes: (1) improving device dependability with trusted updates and robust firmware, (2) protecting communications with encryption and zero-trust architectures, (3) requiring security

certifications and SBOM transparency for manufacturers, and (4) raising user awareness of risks and incident reporting. The evidence gathered from this study supports the general agreement in the literature that, despite the growing usage of WMDs, their full potential in safe digital health environments is severely hampered by recurring failures, data concerns, and a lack of confidence

4.3.4 Awareness of cybersecurity risks

According to an analysis of respondents' knowledge of potential cybersecurity risks in wearable medical devices (WMDs), 62.0% of participants said they were aware of these risks, while a significant 38.0% said they were not. This highlights a critical cybersecurity literacy gap that has important ramifications for the adoption and safety of digital health. According to Hernandez-Ramos et al. (2022), this finding is consistent with global trends showing that end users, including patients and medical professionals, frequently underestimate or lack sufficient knowledge about the vulnerabilities inherent in WMDs, especially regarding wireless communication, cloud integration, and third-party application ecosystems. Because of poor user habits, including not updating device firmware or strong authentication, leads to the amplification of technological vulnerabilities, such a lack of awareness provides an ideal environment for attackers to exploit (Silva-Trujillo *et al*., 2023). The overrepresentation of participants with postgraduate degrees and cybersecurity-related occupations, as shown in previous sociodemographic profiles, may have contributed to the sample's comparatively high awareness (62%) and suggests a positive relationship between technical literacy and cybersecurity awareness in WMD contexts. But given that research indicates that even healthcare providers frequently lack structured training in cybersecurity principles, which results in lapses in secure device integration and use, the persistence of 38% unawareness underscores the need for more extensive cross-sectoral education initiatives (Alhuwail & Al-Jafar, 2021). Comparative studies also show that awareness by itself does not always equate to effective protective behavior. For instance, Canali et al. (2022) showed that although patients and clinicians may be aware of risks like cloud data breaches or unsafe Bluetooth communication, they frequently do nothing because of usability issues, a lack of organizational policy enforcement, or perceived trade-offs between convenience and security. This discrepancy implies that raising awareness needs to be accompanied by practical advice and user-burden-reducing design solutions. Furthermore, the results are consistent with research by

Ostermann et al. (2025), who contend that despite an increase in the public conversation about cybersecurity, device users are still largely ignorant of upstream risks like supply-chain attacks or systemic vulnerabilities in databases and APIs that call for manufacturer-driven and regulatory safeguards rather than end-user actions alone. The necessity for layered awareness campaigns catered to various stakeholder groups is highlighted by the high level of awareness in this study, which may represent knowledge of surface-level hazards (such as hacking and data leaks) but not necessarily deeper systemic issues. Bracciale et al. (2023) discovered that many healthcare organizations still lacked structured vulnerability management and incident response frameworks, perpetuating a culture of reactive rather than proactive defense, despite an increase in attack frequency. This is also consistent with the notable percentage of respondents who lack awareness. The implication is clear: although cybersecurity awareness among WMD users is higher than in some previous reports, nearly two-fifths of people are still unaware, which calls for regulatory requirements for devices that are secure by design as well as more transparent risk disclosure from manufacturers and healthcare providers. In the end, this awareness gap draws attention to a socio-technical problem: even highly developed mitigations run the risk of failing at the last mile of security, jeopardizing patient safety and data integrity in the growing ecosystem of wearable medical technologies, unless the baseline literacy of all users is raised.

4.3.5 Reported Security Vulnerabilities in Wearable Medical Devices

Respondents identified multiple security vulnerabilities in wearable medical devices (WMDs), including Bluetooth connectivity issues, cloud data storage risks, weak passwords, and a lack of software updates. Of these, 44.4% identified a combination of Bluetooth, cloud, password, and software update deficiencies, while others identified individual or paired vulnerabilities. Bluetooth Low Energy (BLE), a widely used communication protocol in wearable devices, is vulnerable to passive eavesdropping, replay attacks, downgraded pairing, and spoofing, allowing attackers to intercept or manipulate data streams during transmission (Zhang *et al*., 2019; Soderi, 2024). Specifically, BLE pairing flaws and metadata leakage have been demonstrated to compromise not only data confidentiality but also to reveal user actions such as initiating an insulin injection suggesting that Bluetooth vulnerabilities alone can breach both privacy and safety (Barman *et al.,*

2021; Soderi, 2024). Second, cloud data storage introduces persistent risk: many devices transmit sensitive health data to remote servers, where weak encryption or insecure configurations can expose patient data; indeed, almost half of wearable health data may reside in poorly encrypted cloud infrastructures, exacerbating the impact of breaches (PatentPC, 2025). Third, weak passwords remain a chronic issue: default or guessable credentials are frequently exploited to gain unauthorized access to device data or functions, underlining the need for enforced credential strength and multi-factor authentication (PMC, 2025). Fourth, the absence of timely software updates the fourth element in the most commonly reported vulnerability combination thwarts patch management and leaves known flaws unremedied, rendering devices easy targets for exploitation, especially when manufacturers cease support or users neglect updates. Collectively, these vulnerabilities align with cross-sector analyses showing that WMDs suffer from compounded risks originating at the sensing layer (Bluetooth), network/cloud layer (data storage), and application layer (authentication and patching), requiring hierarchical, defense-in-depth strategies (Sands *et al.,* 2023). For example, systematic reviews note that without secure-by-design principles such as end-to-end encryption, authenticated firmware updates, SBOM transparency, and policy-enforced password strength wearable devices are likely to be compromised not just individually, but as entry points into broader healthcare networks (Ewoh & Vartiainen, 2024; Ostermann *et al.,* 2025). Furthermore, vulnerabilities in cloud storage and BLE protocols disproportionately heighten risk for devices that handle critical therapeutic tasks (e.g., insulin pumps, continuous monitoring), where data integrity and timely updates directly impact patient safety. In sum, the survey findings are consistent with scientific and security literature: the convergence of Bluetooth protocol weaknesses, cloud storage insecurity, weak password policies, and patching gaps constitute a high-risk vector that demands an integrated mitigation approach. This should include hardened BLE stacks with secure pairing and metadata obfuscation, encrypted and access-controlled cloud services, strong authentication mechanisms, and robust lifecycle maintenance including automatic, authenticated updates to reduce the attack surface and reinforce trust in wearable medical devices.

4.3.6 Respondents' Perceptions and Practices on Cybersecurity of Wearable Medical Devices

The table suggests a pervasive security deficit in respondents' wearable medical device practices and perceptions: a majority disagree that their devices receive regular updates (55.6% SD), use strong authentication (58.3% D), have secure wireless connections (54.6% D), or encrypt data in transit (58.3% D), and most are not aware of cybersecurity risks (56.5% D). Paradoxically, many believe manufacturers have prioritized security (58.3% D to the statement that they have meaning they think security is not prioritized) and deny that most wearables lack strong built-in cybersecurity (56.5% D), while few report suspicious device activity (51.9% D). Two outliers "security settings are user-friendly" (63.9% SA/A) and "I regularly review privacy/security policies" (70.4% SA/A) point to self-reported diligence that conflicts with broader evidence that policies are dense and rarely read, suggesting social desirability or comprehension bias. Contemporary literature aligns with the table's core signal: empirical testing of commercial wearables shows exploitable weaknesses during Bluetooth pairing and data exchange, enabling passive interception and traffic decryption under certain conditions precisely the sort of wireless insecurity respondents perceive (Silva-Trujillo *et al.,* 2023). Surveys of consumers and patients similarly find limited security literacy, inconsistent use of authentication, and low attention to updates, with adoption decisions driven more by convenience and perceived utility than by security features (Abdi *et al.,* 2023). Cross-sector healthcare reviews further show that patching and vulnerability management for connected devices (including IoMT endpoints) are often constrained by vendor controls, resource limitations, and workflow pressures mirroring respondents' low update rates and skepticism about manufacturer prioritization (He *et al.,* 2021). Human-factors syntheses reinforce that security behaviors depend on usable controls and clear mental models; when interfaces are simple, users *feel* more secure even if objective protections are weak helping explain why respondents rate settings as user-friendly while still reporting poor concrete safeguards (Nifakos *et al.,* 2021). Regarding the striking claim that most respondents "regularly review privacy and security policies," living and news-style reviews in digital health document the opposite: users rarely read policies end-to-end and struggle to interpret data flows, risks, and rights for wearables, which often present opaque or fragmented disclosures (Arora *et al.,* 2025; Kaye,

2025). Mitigation strategies borne out across studies converge on: (1) secure-by-design BLE pairing and authenticated key exchange; (2) enforced transport-layer encryption and secure storage; (3) default-on strong authentication (with multifactor for sensitized functions); (4) timely, automated updates with transparent SBOMs and vulnerability disclosure pipelines; and (5) usability-tested security UX with concise, layered privacy notices and just-in-time prompts (Silva-Trujillo *et al.,* 2023; Nifakos *et al.,* 2021; Alhuhairan *et al.,* 2023). In short, the table's respondents appear to sense real risks in wireless links and weak safeguards but overestimate their own policy engagement; aligning device design and organizational processes with the above controls and measuring them with user-centered security metrics remains essential to reduce the gap between perceived and actual protection in wearable medical ecosystems.

4.3.7 Respondents' Perceptions and Experiences on Cybersecurity Threats in Wearable Medical Devices

The survey data show a pronounced coexistence of high perceived risk and limited protective behavior among wearable medical device users: 84.3% believe a cyberattack could affect their health and 89.8% worry about unauthorized access to their health data, yet only 6.5% have stopped using a device and only 4.6% know someone who experienced a device cybersecurity incident findings that align with and can be interpreted through contemporary empirical and technical literature on wearables and health-care cybersecurity. Empirically, user perceptions that security and privacy strongly shape adoption decisions have been documented by Thapa et al. (2023), who found that perceived security/privacy was a dominant predictor of intention to use WIoMT devices, even while adoption continued when perceived usefulness and ease-of-use outweighed concerns (Thapa *et al.,* 2023). This tension high concern but continued use mirrors the well-described "privacy paradox" and the willingness–action gap seen in large national samples: Chandrasekaran et al. (2025) reported high willingness to share wearable data with providers but substantially lower actual sharing, illustrating that expressed concern or intent often does not translate to risk-avoidant behavior in practice (Chandrasekaran *et al.,* 2025). Technically, the low rate of user discontinuation despite widespread worry is troubling because numerous engineering studies demonstrate real, exploitable vulnerabilities in popular wearables: passive and pairing-related Bluetooth weaknesses, static MAC addresses, and inconsistent authentication schemes

make many smartwatches and fitness wearables susceptible to eavesdropping, MITM, and cloning attacks that could expose or manipulate health data or device function (Silva-Trujillo *et al.,* 2023). Policy- and industry-level analyses further amplify the risk: systematic audits of manufacturer privacy policies reveal uneven transparency, weak vulnerability-disclosure practices, and inconsistent breach notification regimes across leading brands, meaning that even concerned users cannot reliably assess or control downstream data flows or remediation practices (Doherty *et al.,* 2025). At the system level, narrative reviews of healthcare cybersecurity emphasize that vulnerabilities in consumer wearables are not isolated technical nuisances but can cascade into patient-safety incidents when devices are integrated into clinical workflows or inform treatment decisions; such reviews call for stronger vendor–provider collaboration, rigorous patching regimes, and regulatory alignment to protect both data and patient outcomes (Aldosari *et al.,* 2025). Taken together, the table's pattern high perceived personal risk, near-universal concern about data access, but limited cessation of use or knowledge of real-world incidents is consistent with (a) behavioral findings that users tolerate trade-offs when perceived benefits are high, (b) empirical evidence of a willingness–action gap for privacy-protective choices, and (c) engineering and policy evidence that many wearables remain technically and institutionally ill-prepared for adversarial threats. Practically, these convergent lines of evidence suggest multi-layered mitigation: manufacturers must adopt secure-by-design practices (robust encryption, authenticated pairing, and timely patching), regulators and procurement bodies should mandate transparency and vulnerability-disclosure standards, and clinicians and public-health communicators must translate user concern into concrete protective actions (e.g., enabling strong authentication, applying updates, and restricting device-to-clinical-network integration until security posture is verified), because leaving the current mismatch between perceived risk and behavior unaddressed risks both personal data exposure and, in worst cases, patient harm (Silva-Trujillo *et al.,* 2023; Thapa *et al.,* 2023; Chandrasekaran *et al.,* 2025; Doherty *et al.,* 2025; Aldosari *et al.,* 2025).

4.3.8 Perceptions on Cybersecurity Risks of Wearable Medical Devices

The findings from the table demonstrate that respondents overwhelmingly downplay the cybersecurity risks of wearable medical devices, as the majority disagree that cyberattacks could lead to incorrect health readings or diagnoses (64.8% D), compromise personal health information

(52.8% D), cause patient harm (59.3% D), or jeopardize healthcare services (54.6% D), with similar skepticism expressed regarding data manipulation (63.9% D), trust erosion in digital health systems (60.2% D), and the need for more safeguards (58.3% D). This trend runs counter to scientific data showing the actual and expanding risks connected to wearables and the Internet of Medical Things (IoMT). As an illustration of the seriousness of worries over data manipulation and misdiagnosis hazards, Silva-Trujillo et al. (2023) demonstrated that smartwatches are extremely vulnerable to passive Bluetooth attacks, which allow for the interception and alteration of sent health data. Similar to this, Alhuhairan et al. (2023) highlighted how respondents' disregard for the risks associated with personal health information may reflect their lack of technical literacy, highlighting how weak or nonexistent multifactor authentication in wearable ecosystems exposes users to identity theft and unauthorized access to sensitive health data. According to Thapa et al. (2023), despite acknowledging abstract risks, users often prioritize device convenience and functionality over perceived risks, resulting in tolerating vulnerabilities. Contrary to respondents' lack of concern about organizational risks, Aldosari et al. (2025) cautioned that, from a systemic standpoint, insufficient protection of connected medical devices directly threatens patient safety and the integrity of healthcare services. Even while participants underestimated the need for further protection, privacy-focused assessments by Doherty et al. (2025) show that major wearable manufacturers lack transparent data policies or consistent safeguards, supporting the assertion that more safeguards are in fact required. The "privacy paradox" and "security fatigue" are described in health informatics research, where users purposefully deprioritize cybersecurity because of perceived complexity or low self-efficacy, even though objective risks are high, are consistent with respondents' low acknowledgment of risks and scientific evidence of device vulnerability (Nifakos et al., 2021). This paradox explains why, despite evidence that breaches can damage public confidence and patient-provider interactions, people may undervalue risks to trust in digital healthcare systems (Chandrasekaran *et al*., 2025). The majority perspective in the table indicates a troubling discrepancy between user perception and empirical reality, as the literature confirms that cyberattacks on wearable devices can result in inaccurate readings, manipulation of vital health data, and systemic healthcare hazards. Addressing this gap requires enhancing security-by-design mechanisms such as robust encryption, automated patching, and multifactor authentication

while simultaneously investing in patient education campaigns to raise awareness of real-world threats. Without bridging this gap, the continued underestimation of cybersecurity vulnerabilities among users, as shown in the table, will perpetuate unsafe practices and delay adoption of urgently needed safeguards for wearable medical devices.

4.3.9 Respondents' Perceptions of Cybersecurity Risks in Wearable Medical Devices

The analysis of respondents' perceptions on cybersecurity risks in wearable medical devices shows a general underestimation of the severity of threats, as the majority strongly disagreed or disagreed with statements highlighting risks of cyberattacks, including incorrect health readings or diagnoses (64.8% D), compromise of personal health information (52.8% D), patient harm from breaches (59.3% D), threats to healthcare services (54.6% D), manipulation of critical health data (63.9% D), and erosion of trust in digital healthcare systems (60.2% D), while 58.3% disagreed that more safeguards were necessary. This contrasts sharply with growing evidence in the literature that cyber vulnerabilities in the Internet of Medical Things (IoMT) and wearable health devices are both real and impactful. For instance, Silva-Trujillo et al. (2023) demonstrated that smartwatches are highly susceptible to Bluetooth-based passive attacks, allowing interception and alteration of transmitted health data, validating concerns about data manipulation and misdiagnosis risks that most respondents dismissed. Similarly, Alhuhairan et al. (2023) reviewed multifactor authentication gaps in wearable ecosystems and showed that weak authentication directly exposes users to unauthorized access and personal health information leakage, contradicting respondents' skepticism about data compromise. Although many responders in the table minimized the risks, Aldosari et al. (2025) emphasized that cybersecurity breaches in linked medical equipment pose direct concerns to patient safety, highlighting the reality of potential harm. Even while 58.3% of respondents disagreed that such controls were required, Doherty et al. (2025) looked at manufacturer data policies and discovered inconsistent and inadequate safeguards among wearable technology providers, highlighting the need for extra safeguards beyond individual risk. Additionally, Chandrasekaran et al. (2025) demonstrated that while users voiced concerns regarding data sharing from wearable devices, these concerns were not always reflected in their actions, suggesting a "privacy paradox" in which risk awareness does not always translate into

protective measures—a behavioral trend that is reflected in this survey. Furthermore, Nifakos et al. (2021) emphasized the importance of human factors, pointing out that a significant portion of respondents did not consider device hacking or systemic risks to healthcare services to be significant because many users underestimate cybersecurity risks due to complexity and a lack of technical understanding. Crucially, the table's underestimating of dangers indicates a risky discrepancy between actual data and popular opinion, which may postpone regulatory action and mitigation. According to science, this disparity highlights the need for multifaceted solutions that include user education initiatives to bring the general public up to speed on device vulnerabilities, regulatory enforcement of stricter data governance, and technical safeguards (strong encryption, secure pairing, automated patching). Without bridging this gap, the continued dismissal of cybersecurity risks by end-users could perpetuate unsafe reliance on wearable medical devices, undermining both patient safety and trust in digital health systems, despite mounting evidence that such risks are not only theoretical but actively exploitable in practice (Silva-Trujillo *et al.,* 2023; Alhuhairan *et al.,* 2023; Aldosari *et al.,* 2025; Doherty *et al.,* 2025; Chandrasekaran *et al.,* 2025; Nifakos *et al.,* 2021).

4.3.10 Perceptions on Cybersecurity Regulations and Practices for Wearable Medical Devices

The survey reveals overwhelmingly strong disagreement by respondents with key regulatory and protective measures for wearable medical device cybersecurity: the majority **disagree** or **strongly disagree** that manufacturers should be mandated to meet minimum cybersecurity standards (67.6% D), that users should receive cybersecurity training (60.2% D), that third-party audits be required pre-market (63.0% D), or that healthcare providers offer technical support on device security (62.0% D). Similarly, most oppose embedded security features such as real-time threat alerts and automatic updates (70.4% D), greater user control over privacy/security settings (69.4% D), stricter penalties for manufacturers failing to protect user data (67.6% D), mandatory multi-factor authentication (65.7% D), mandatory encryption protocols (67.6% D), and universal government security certification (65.7% D). This general resistance to regulatory and technical safeguards conflicts sharply with documented vulnerabilities and the recognized need for structured control frameworks. Indeed, Ostermann and colleagues (2024) highlight substantial

gaps in both EU (MDCG 2019-16) and US (FDA premarket cybersecurity guidance) standards particularly around cryptography, authentication, and software development that may allow manufacturers to overlook cybersecurity robustness in their devices. To ensure patient safety, connected medical devices require a comprehensive approach that includes technical controls, governance, resilience, reporting, and legislation. Granlund et al. (2021) emphasize that the new EU Medical Device Regulation (MDR) includes cybersecurity standards. However, compliance requires establishing basic principles, which manufacturers may oppose without enforcement. A systematic review of major wearable manufacturers reveals inconsistent privacy and vulnerability disclosure practices, highlighting the need for standardized certification and oversight. NIST guidance (e.g., NISTIR-8259A) prioritizes basic cybersecurity principles such device identity, data protection, access control, and configuration. However, these guidelines are voluntary, indicating a disconnect between best practices and mandatory standards. These findings strongly suggest the necessity for legislative regulations, standardized certification, technical protections, and user support systems. The discrepancy between public perception and expert opinion regarding these procedures may jeopardize patient safety and data integrity. Addressing this requires multi-stakeholder action: policymakers must enact and enforce cybersecurity standards such as IEC 62304, ISO 14971, and IEC 60601 while certifying wearable devices; manufacturers must embed real-time updating, encryption, strong authentication, and transparency by design; healthcare providers should educate and support users in cybersecurity best practices; and regulatory bodies must impose penalties for noncompliance to align industry incentives with patient protection and trustworthy digital health ecosystems.

4.4: Implications

The results air that patients and healthcare stakeholders have a huge mistrust of the cybersecurity protections put in place for WMDs and believe they are inadequate. Respondents are sceptical of industry initiatives and legislative suggestions such as universal certification, third-party audits, and minimum cybersecurity requirements, even while they notice technical concerns and vulnerabilities. This differences between awareness and trust draws attention to issues with risk perception and user engagement. All of the data points to the urgent need for integrated solutions to increase security, build confidence, and guarantee the safe adoption of WMDs. These

solutions include secure-by-design development, enforceable legislation, user and clinician education,

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The findings on perceptions of cybersecurity regulations and practices for wearable medical devices highlight significant gaps between user expectations and industry or regulatory actions, revealing both a trust deficit and critical vulnerabilities in digital health technologies. Most respondents disagreed on establishing baseline cybersecurity standards, training users, demanding third-party audits, enabling real-time danger warnings, and providing technical help. Stakeholders may lack confidence in present safeguards or be uninformed of possible precautions, leading to widespread disagreement about current procedures. Wearable medical devices, which capture sensitive biometric data on a continuous basis, are vulnerable to hacks, with potential clinical and privacy ramifications. Reluctance to support universal encryption technologies, multi-factor authentication, and tougher fines for non-compliant manufacturers may indicate gaps in public understanding, industry accountability, and regulatory enforcement. Comparatively speaking, this is consistent with larger issues in healthcare cybersecurity, as the use of secure-by-design principles is lagging advancements in technology. Despite receiving a low agreement rating, the need for automatic updates and real-time threat alerts is especially important since they could lessen the chance of delayed patching and mitigate zero-day vulnerabilities. However, worries about device usability and cost may prevent their widespread adoption. Similarly, even though universal security certification might assist set worldwide safety standards, its limited support reflects either pessimism about the effectiveness of regulations or apprehension about higher device costs for end users. Although the technical community highlights cybersecurity as a crucial component of digital health, end users, healthcare providers, and potentially even manufacturers may not be convinced of the urgency of these measures, as indicated by the consistently high levels of disagreement across all categories. From a scientific standpoint, this disparity emphasizes the necessity of improved risk communication tactics, inclusive policymaking, and awareness-raising initiatives that not only draw attention to the dangers but also show the real advantages of

implementing secure procedures without sacrificing usability. Multi-sectoral cooperation is needed to address these cybersecurity vulnerabilities in practice. Manufacturers must implement secure development lifecycles, healthcare providers must incorporate cybersecurity training into clinical practice, regulators must enforce compliance through certification and fines, and patients must be equipped with the information and resources they need to safely manage their devices. The study's findings thus highlight the urgent need for systemic reform, filling in perception gaps with tangible, transparent, and legally binding cybersecurity frameworks that protect patient safety and confidence in wearable medical technology.

5.2 Recommendations

Based on what has been found in this study, the following recommendations were suggested

5.2.1 For Manufacturers

- **Employ Secure-by-Design Principles:** Cybersecurity features like multifactor authentication, secure update techniques and encryption, should be built into devices from the development stage.
- **Consistent Software and Firmware Updates:** Weaknesses or vulnerabilities should be patched on time through the use of automated updates, so as not to compromise device functionality.
- **Third-Party Security Trial:** Before devices reach the market, independent audits and penetration testing should be mandated.
- **User-Centered Design:** Security features of devices should be simplified, to improve patients' compliance. An example of this would be the use of intuitive authentication.

5.2.2 For Healthcare Providers

- **Training in Cybersecurity:** Clinicians should be trained in how to identify cybersecurity risks, use of devices securely and also education of patients on safe use of devices.

- **Incorporation into Clinical Work systems:** New hospital IT polices should be put in place to include WMD security in Electronic Health Records protection plans.
- **Incident Response Practices:** Protocols on detection, reporting, and mitigation of data breaches relating to WMDs should be developed.
- **Patient Education:** Orientation should be given to patients on safe use, device updates and ability to recognize suspicious activities on their WMDs.

5.2.3 For Patients and End-Users

- **Awareness and Safe Operations:** The use of secure authentication, connection, and regular updates when syncing devices should be encouraged
- **Data Privacy Caution:** Patients should be educated on sharing only the required health data and try to limit third party app integrations that will further heighten exposure.
- **Device upkeep:** Regular inspections for firmware integrity, updates and reports of unusual device activity should be promoted.
- **Advocacy:** Patients should be empowered to ask for transparency about their device security from clinicians and manufacturers.

5.2.4 For Regulators and Policymakers

- **Incorporate Cybersecurity Standards:** Basic requirements for device authentication, encryption, and management of vulnerability should be mandated.
- **Certification Structure:** A security certification that is universal for WMDs should be established, identical to medical device approvals, to improve public trust.
- **Enforcement Procedures:** Penalties should be imposed for non-compliance.
- **Cooperative Governance:** To have and maintain coordinated defense strategies, a partnership between clinical systems, tech companies and the government, should be encouraged.

- **Awareness Programs:** Public orientation programs should be set up to advance the knowledge and understanding of cybersecurity risks and safe use of devices.

5.2.5 For Researchers and Academia

- **Risk Assessment Models:** Develop predictive models to assess vulnerabilities and patient safety risks.
- **Human-Centered Cybersecurity Studies:** Investigate usability barriers that make patients or providers reluctant to adopt secure practices.
- **Policy Impact Research:** Assess effectiveness of regulatory interventions and propose evidence-based improvements.
- **Innovation in Security Solutions:** Explore lightweight, energy-efficient cybersecurity algorithms tailored for wearable devices.

REFERENCES

Addotey-Delove, M., Scott, R.E., Mars, M., 2023. Healthcare Workers' Perspectives of mHealth Adoption Factors in the Developing World: Scoping Review. Int. J. Environ. Res. Public. Health 20, 1244. https://doi.org/10.3390/ijerph20021244

Alexander, B., Baranchuk, A., 2020. Cybersecurity and cardiac implantable electronic devices. Nat. Rev. Cardiol. 17, 315–317. https://doi.org/10.1038/s41569-020-0372-1

Alkhaldi, O., McMillan, B., Maddah, N., Ainsworth, J., 2023. Interventions Aimed at Enhancing Health Care Providers' Behavior Toward the Prescription of Mobile Health Apps: Systematic Review. JMIR MHealth UHealth 11, e43561. https://doi.org/10.2196/43561

Alkhatib, S., Waycott, J., Buchanan, G., Bosua, R., 2018. Privacy and the Internet of Things (IoT) Monitoring Solutions for Older Adults: A Review. Stud. Health Technol. Inform. 252, 8–14.

Al-rawashdeh, M., Keikhosrokiani, P., Belaton, B., Alawida, M., Zwiri, A., 2022. IoT Adoption and Application for Smart Healthcare: A Systematic Review. Sensors 22, 5377. https://doi.org/10.3390/s22145377

Argaw, S.T., Bempong, N.-E., Eshaya-Chauvin, B., Flahault, A., 2019. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Med. Inform. Decis. Mak. 19, 10. https://doi.org/10.1186/s12911-018-0724-5

Austen, K., 2015. What could derail the wearables revolution? Nature 525, 22–24. https://doi.org/10.1038/525022a

Bhuyan, S.S., Kabir, U.Y., Escareno, J.M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., Dobalian, A., 2020. Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. J. Med. Syst. 44, 98. https://doi.org/10.1007/s10916-019-1507-y

Bleiker, J., Morgan-Trimmer, S., Knapp, K., Hopkins, S., 2019. Navigating the maze: Qualitative research methodologies and their philosophical foundations. Radiography, Methodological Issues in Medical Imaging and Radiotherapy Research 25, S4–S8. https://doi.org/10.1016/j.radi.2019.06.008

Borges do Nascimento, I.J., Abdulazeem, H., Vasanthan, L.T., Martinez, E.Z., Zucoloto, M.L., Østengaard, L., Azzopardi-Muscat, N., Zapata, T., Novillo-Ortiz, D., 2023. Barriers and facilitators to utilizing digital health technologies by healthcare professionals. NPJ Digit. Med. 6, 161. https://doi.org/10.1038/s41746-023-00899-4

Bracciale, L., Loreti, P., Bianchi, G., 2023. Cybersecurity vulnerability analysis of medical devices purchased by national health services. Sci. Rep. 13, 19509. https://doi.org/10.1038/s41598-023-45927-1

Choi, S., Lee, H., Ghaffari, R., Hyeon, T., Kim, D.-H., 2016. Recent Advances in Flexible and Stretchable Bio-Electronic Devices Integrated with Nanomaterials. Adv. Mater. Deerfield Beach Fla 28, 4203–4218. https://doi.org/10.1002/adma.201504150

Clarke, R., Youngstein, T., 2017. Cyberattack on Britain's National Health Service - A Wake-up Call for Modern Medicine. N. Engl. J. Med. 377, 409–411. https://doi.org/10.1056/NEJMp1706754

Coventry, L., Branley, D., 2018a. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas 113, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Coventry, L., Branley, D., 2018b. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas 113, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Dullea, E., Budke, C., Enko, P., 2020. Cybersecurity Update: Recent Ransomware Attacks Against Healthcare Providers. Mo. Med. 117, 533–534.

Escobar-Linero, E., Muñoz-Saavedra, L., Luna-Perejón, F., Sevillano, J.L., Domínguez-Morales, M., 2023. Wearable Health Devices for Diagnosis Support: Evolution and Future Tendencies. Sensors 23, 1678. https://doi.org/10.3390/s23031678

Ewoh, P., Vartiainen, T., 2024. Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. J. Med. Internet Res. 26, e46904. https://doi.org/10.2196/46904

Farlow, C.S., Jump, M.L., Seeberger, M.S., Fitzgerald, B.J., 2023. ANSI/AAMI SW96: Raising the Bar for Medical Device Security Risk Management. Biomed. Instrum. Technol. 57, 40–43. https://doi.org/10.2345/0899-8205-57.2.40

Fischer, S.H., Ray, K.N., Mehrotra, A., Bloom, E.L., Uscher-Pines, L., 2020. Prevalence and Characteristics of Telehealth Utilization in the United States. JAMA Netw. Open 3, e2022302. https://doi.org/10.1001/jamanetworkopen.2020.22302

Giansanti, D., 2021. Cybersecurity and the Digital-Health: The Challenge of This Millennium. Healthcare 9, 62. https://doi.org/10.3390/healthcare9010062

Giansanti, D., Monoscalco, L., 2021. The cyber-risk in cardiology: towards an investigation on the self-perception among the cardiologists. mHealth 7, 28. https://doi.org/10.21037/mhealth.2020.01.08

Guk, K., Han, G., Lim, J., Jeong, K., Kang, T., Lim, E.-K., Jung, J., 2019. Evolution of Wearable Devices with Real-Time Disease Monitoring for Personalized Healthcare. Nanomaterials 9, 813. https://doi.org/10.3390/nano9060813

Gura, M.T., 2015. Considerations in Patients With Cardiac Implantable Electronic Devices at End of Life. AACN Adv. Crit. Care 26, 356–363. https://doi.org/10.1097/NCI.0000000000000111

Hassan, S.R., Ahmad, I., Ahmad, S., Alfaify, A., Shafiq, M., 2020. Remote Pain Monitoring Using Fog Computing for e-Healthcare: An Efficient Architecture. Sensors 20, 6574. https://doi.org/10.3390/s20226574

Heeks, R., 2006. Health information systems: failure, success and improvisation. Int. J. Med. Inf. 75, 125–137. https://doi.org/10.1016/j.ijmedinf.2005.07.024

Huang, W., Zhang, Y., Feng, Y., 2020. ACD: An Adaptable Approach for RFID Cloning Attack Detection. Sensors 20, 2378. https://doi.org/10.3390/s20082378

Jalali, M.S., Razak, S., Gordon, W., Perakslis, E., Madnick, S., 2019. Health Care and Cybersecurity: Bibliometric Analysis of the Literature. J. Med. Internet Res. 21, e12644. https://doi.org/10.2196/12644

Jeng, M.-Y., Yeh, T.-M., Pai, F.-Y., 2022. A Performance Evaluation Matrix for Measuring the Life Satisfaction of Older Adults Using eHealth Wearables. Healthcare 10, 605. https://doi.org/10.3390/healthcare10040605

Kamišalić, A., Fister, I., Turkanović, M., Karakatič, S., 2018. Sensors and Functionalities of Non-Invasive Wrist-Wearable Devices: A Review. Sensors 18, 1714. https://doi.org/10.3390/s18061714

Kelpsas, B., Nelson, A., 2016. Ransomware in Hospitals: What Providers Will Inevitably Face When Attacked. J. Med. Pract. Manag. MPM 32, 67–70.

Kruse, C.S., Frederick, B., Jacobson, T., Monticone, D.K., 2017a. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol. Health Care Off. J. Eur. Soc. Eng. Med. 25, 1–10. https://doi.org/10.3233/THC-161263

Kruse, C.S., Smith, B., Vanderlinden, H., Nealand, A., 2017b. Security Techniques for the Electronic Health Records. J. Med. Syst. 41, 127. https://doi.org/10.1007/s10916-017-0778-4

Langer, S.G., 2017. Cyber-Security Issues in Healthcare Information Technology. J. Digit. Imaging 30, 117–125. https://doi.org/10.1007/s10278-016-9913-x

Lei, J., Sockolow, P., Guan, P., Meng, Q., Zhang, J., 2013. A comparison of electronic health records at two major Peking University Hospitals in China to United States meaningful use objectives. BMC Med. Inform. Decis. Mak. 13, 96. https://doi.org/10.1186/1472-6947-13-96

López-Blanco, R., Velasco, M.A., Méndez-Guerrero, A., Romero, J.P., Del Castillo, M.D., Serrano, J.I., Rocon, E., Benito-León, J., 2019. Smartwatch for the analysis of rest tremor in patients with Parkinson's disease. J. Neurol. Sci. 401, 37–42. https://doi.org/10.1016/j.jns.2019.04.011

Lu, L., Zhang, J., Xie, Y., Gao, F., Xu, S., Wu, X., Ye, Z., 2020. Wearable Health Devices in Health Care: Narrative Systematic Review. JMIR MHealth UHealth 8, e18907. https://doi.org/10.2196/18907

Maccioni, G., Giansanti, D., 2021. Medical Apps and the Gray Zone in the COVID-19 Era: Between Evidence and New Needs for Cybersecurity Expansion. Healthc. Basel Switz. 9, 430. https://doi.org/10.3390/healthcare9040430

Mariano, B., 2020. Towards a global strategy on digital health. Bull. World Health Organ. 98, 231-231A. https://doi.org/10.2471/BLT.20.253955

Mejía-Granda, C.M., Fernández-Alemán, J.L., Carrillo-de-Gea, J.M., García-Berná, J.A., 2024. Security vulnerabilities in healthcare: an analysis of medical devices and software. Med. Biol. Eng. Comput. 62, 257–273. https://doi.org/10.1007/s11517-023-02912-0

Mendoza, F.A. *et al.* (2018) 'Assessment of Fitness Tracker Security: A Case of Study'. *Proceedings*, 2(19), p. 1235. DOI: 10.3390/proceedings2191235.

Miller, F.A., Young, S.B., Dobrow, M., Shojania, K.G., 2021. Vulnerability of the medical product supply chain: the wake-up call of COVID-19. BMJ Qual. Saf. 30, 331–335. https://doi.org/10.1136/bmjqs-2020-012133

Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E., Bonacina, S., 2021. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors 21, 5119. https://doi.org/10.3390/s21155119

Park, E. and Lim, J.H. (2025) 'The Impact of Healthcare Data Breaches on Patient Hospital Visit Behavior'. *International Journal of Research in Marketing*. DOI: 10.1016/j.ijresmar.2025.01.004.

Pycroft, L., Boccard, S.G., Owen, S.L.F., Stein, J.F., Fitzgerald, J.J., Green, A.L., Aziz, T.Z., 2016. Brainjacking: Implant Security Issues in Invasive Neuromodulation. World Neurosurg. 92, 454–462. https://doi.org/10.1016/j.wneu.2016.05.010

Rasool, R.U. *et al.* (2022) 'Security and Privacy of Internet of Medical Things: A Contemporary Review in the Age of Surveillance, Botnets, and Adversarial ML'. DOI: 10.1016/j.jnca.2022.103332.

Rodríguez, E., Otero, B., Canal, R., 2023. A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things. Sensors 23, 1252. https://doi.org/10.3390/s23031252

Rosman, L., Gehi, A., Lampert, R., 2020. When smartwatches contribute to health anxiety in patients with atrial fibrillation. Cardiovasc. Digit. Health J. 1, 9–10. https://doi.org/10.1016/j.cvdhj.2020.06.004

S. Rubí, J.N., L. Gondim, P.R., 2019. IoMT Platform for Pervasive Healthcare Data Aggregation, Processing, and Sharing Based on OneM2M and OpenEHR. Sensors 19, 4283. https://doi.org/10.3390/s19194283

Sadhu, P.K., Yanambaka, V.P., Abdelgawad, A., 2022a. Internet of Things: Security and Solutions Survey. Sensors 22, 7433. https://doi.org/10.3390/s22197433

Sadhu, P.K., Yanambaka, V.P., Abdelgawad, A., Yelamarthi, K., 2022b. Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions. Sensors 22, 5517. https://doi.org/10.3390/s22155517

Schreiweis, B., Pobiruchin, M., Strotbaum, V., Suleder, J., Wiesner, M., Bergh, B., 2019. Barriers and Facilitators to the Implementation of eHealth Services: Systematic Literature Analysis. J. Med. Internet Res. 21, e14197. https://doi.org/10.2196/14197

Silva-Trujillo, A.G., González González, M.J., Rocha Pérez, L.P., García Villalba, L.J., 2023. Cybersecurity Analysis of Wearable Devices: Smartwatches Passive Attack. Sensors 23, 5438. https://doi.org/10.3390/s23125438

Slight, S.P., Bates, D.W., 2014. A risk-based regulatory framework for health IT: recommendations of the FDASIA working group. J. Am. Med. Inform. Assoc. JAMIA 21, e181–e184. https://doi.org/10.1136/amiajnl-2014-002638

Spanakis, E.G., Bonomi, S., Sfakianakis, S., Santucci, G., Lenti, S., Sorella, M., Tanasache, F.D., Palleschi, A., Ciccotelli, C., Sakkalis, V., Magalini, S., 2020. Cyber-attacks and threats for healthcare - a multi-layer thread analysis. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. IEEE Eng. Med. Biol. Soc. Annu. Int. Conf. 2020, 5705–5708. https://doi.org/10.1109/EMBC44109.2020.9176698

Stern, A.D., Gordon, W.J., Landman, A.B., Kramer, D.B., 2019. Cybersecurity features of digital medical devices: an analysis of FDA product summaries. BMJ Open 9, e025374. https://doi.org/10.1136/bmjopen-2018-025374

Sun, D.-Z., Sun, L., Yang, Y., 2019. On Secure Simple Pairing in Bluetooth Standard v5.0-Part II: Privacy Analysis and Enhancement for Low Energy. Sensors 19, 3259. https://doi.org/10.3390/s19153259

Thapa, S., Bello, A., Maurushat, A., Farid, F., 2023. Security Risks and User Perception towards Adopting Wearable Internet of Medical Things. Int. J. Environ. Res. Public. Health 20, 5519. https://doi.org/10.3390/ijerph20085519

Thomasian, N.M. and Adashi, E.Y. (2021) 'Cybersecurity in the Internet of Medical Things'. *Health Policy and Technology*, 10(3), p. 100549. DOI: 10.1016/j.hlpt.2021.100549.

Tison, G.H., Sanchez, J.M., Ballinger, B., Singh, A., Olgin, J.E., Pletcher, M.J., Vittinghoff, E., Lee, E.S., Fan, S.M., Gladstone, R.A., Mikell, C., Sohoni, N., Hsieh, J., Marcus, G.M., 2018. Passive Detection of Atrial Fibrillation Using a Commercially Available Smartwatch. JAMA Cardiol. 3, 409–416. https://doi.org/10.1001/jamacardio.2018.0136

Tully, J., Selzer, J., Phillips, J.P., O'Connor, P., Dameff, C., 2020. Healthcare Challenges in the Era of Cybersecurity. Health Secur. 18, 228–231. https://doi.org/10.1089/hs.2019.0123

Vrhovec, S., Markelj, B., 2024. We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers. PloS One 19, e0312266. https://doi.org/10.1371/journal.pone.0312266

Wagan, S.A., Koo, J., Siddiqui, I.F., Attique, M., Shin, D.R., Qureshi, N.M.F., 2022. Internet of medical things and trending converged technologies: A comprehensive review on real-time applications. J. King Saud Univ. - Comput. Inf. Sci. 34, 9228–9251. https://doi.org/10.1016/j.jksuci.2022.09.005

Williams, P.A., Woodward, A.J., 2015. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med. Devices Auckl. NZ 8, 305–316. https://doi.org/10.2147/MDER.S50048

Yang, Z., Zhou, Q., Lei, L., Zheng, K., Xiang, W., 2016. An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare. J. Med. Syst. 40, 286. https://doi.org/10.1007/s10916-016-0644-9

Zheng, X., Sun, S., Mukkamala, R.R., Vatrapu, R., Ordieres-Meré, J., 2019. Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies. J. Med. Internet Res. 21, e13583. https://doi.org/10.2196/13583

Zubair, M., Ghubaish, A., Unal, D., Al-Ali, A., Reimann, T., Alinier, G., Hammoudeh, M., Qadir, J., 2022. Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System. Sensors 22, 8280. https://doi.org/10.3390/s22218280

APPENDIX A: ETHICS APPLICATION AND DECLARATION FORM

Ethics Application & Declaration Form

DISSERTATION TITLE: Cybersecurity Vulnerabilities in Wearable Medical Devices: A Cross-Sector Analysis of Risks and Mitigation Strategies using Ireland as a case study

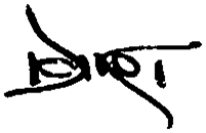
RESEARCHER'S NAME: Bridget Epepitimi Kalabo

PROGRAMME OF STUDY: MSc in Medical Device Technology & Business

SUPERVISOR'S NAME: Favour Okosun

DECLARATION:
The information in this application form is accurate to the best of my knowledge. I undertake to abide by the principles outlined by Innopharma/Griffith College ethics policy in my research dissertation. I confirm that I have completed a full ethics assessment for my research dissertation as per the college guidelines. I will not begin my primary research until such approval from my supervisor and/or ethics Committee has been obtained.
I pledge to carry out my research according to the Innopharma/Griffith College academic integrity standards. Any results presented in my dissertation will be from my own, original research, I will reference and/or acknowledge any material or sources used in its preparation and I will not plagiarise the work of anyone else.

For Student:



STUDENT SIGNATURE:

DATE: 07/07/2025

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

For Supervisor:
Ethics Committee Approval Required: Yes ☐ No ☐

SUPERVISOR SIGNATURE: Favour Okosun

DATE: 07/07/2025

For Ethics Committee (if required):
Ethics Committee Approval Given: Yes ☐ No ☐

ETHICS COMMITTEE MEMBER SIGNATURE:

DATE:

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

SECTION 1: DESCRIPTION OF RESEARCH STUDY

1.1 Purpose and objectives of research [*300 words maximum/ use literature review findings to guide]*
Purpose: The aim of this research is to find significant cybersecurity vulnerabilities, examine their impact on patient safety and data privacy, evaluate cross-sector laws, and provide evidence-based mitigation recommendations, for wearable medical devices. This study seeks to address the serious cybersecurity risks that compromise patient safety, data privacy, and healthcare system stability emanating from the use of wearable medical devices. The existing literature also highlights a knowledge gap regarding the improvement of user education and awareness of cybersecurity dangers connected with wearable medical devices and also integrating security procedures across industries, utilizing current technologies like blockchain and artificial intelligence, and encouraging a cybersecurity-first mentality in the healthcare sector. Therefore, by analysing the existing landscape, including technological capabilities and perceived barriers, this research seeks to analyse risks and suggest recommendations to mitigate cybersecurity vulnerabilities using Ireland as a case study.

Objectives:

- To determine and analyze the main cybersecurity vulnerabilities in wearable medical devices used in the healthcare sector.
- To assess the possible dangers and impacts of cybersecurity threats on patient privacy and safety in relation to these devices.

- To evaluate current cybersecurity frameworks and mitigation techniques relevant to wearable medical devices, emphasizing their effectiveness and challenges.
- To provide recommendations for enhancing cybersecurity protocols that are specific to the difficulties presented by wearable medical devices in healthcare settings.

1.2 Research methodology: [*300 words maximum/ detail how you will acquire your primary data (focus groups/interviews/online surveys etc). Proposed questions for questionnaires and/or interviews **must be included** in the appendix].*

This study adopts a pragmatic philosophical approach, in alignment with a quantitative research strategy utilizing an online Likert scale survey on Microsoft Forms to collect quantitative data. The target participants will be recruited through purposive or stratified sampling through professional networks, social media, and personal contacts. The participants include English speaking cybersecurity experts, clinicians in general and individuals who use wearable medical devices in Ireland. Exclusion criteria include people who don't have any knowledge of cybersecurity, or wearable medical devices in Ireland.

A total sample size of 110 participants will be surveyed using one questionnaire, including participants such as cybersecurity experts, clinicians and individuals who use wearable medical devices. This will aim to provide data and insights towards identifying cybersecurity vulnerabilities, dangers and impacts of cybersecurity threats, evaluation of existing cybersecurity frameworks and recommendations for enhancing cybersecurity (Refer Appendix 10.2). The data collected using the above method will be analysed using statistical tests such as the chi-square test to identify patterns and relationships. The findings will be summarized in a report with charts, tables, and narrative explanations using data visualization techniques.

SECTION 2: POSSIBLE ETHICAL ISSUES

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

SUBJECT MATTER

Does the research proposal involve:

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

RESEARCH PROCEDURES

Does the research proposal involve:

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

PARTICIPANTS

Does the research proposal involve:

People who are not competent and/or fluent in English	No
Does your research group include any of the following vulnerable groups	No

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

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

SECTION 3: STEPS TAKEN TO AVOID ETHICAL ISSUES

3.1. If your ethics relates to ***Subject Matter***, outline your action plan to work around any sensitive issues.
3.2. If your ethics relates to ***Research Procedures***, outline your action plan to deal with possible ethical issues in your research procedures.
3.3. If your ethics relates to ***Participants***, outline how you will protect vulnerable persons or those that do not have English as their first language.

SECTION 4: ABOUT YOUR PARTICIPANTS

4.1. Outline your participant profile and why you have chosen them for this study *[Do not provide names except where it is deemed impossible to conceal identity].*
Cybersecurity Experts: They offer technical insights into wearable medical devices' threats, vulnerabilities, and existing or new mitigation techniques. Their knowledge is essential for assessing the efficacy of current cybersecurity measures in the Irish environment and comprehending systemic risks.

Clinicians: Clinicians provide practical expertise about wearable medical device functionality, integration with healthcare systems, and patient safety issues as frontline users and prescribers. Their views aid in relating clinical risks, technology vulnerabilities, and healthcare implications.

Individuals who use wearable medical devices: End users can share their personal experiences, concerns about device dependability and data privacy, and their knowledge or lack thereof of cybersecurity risks. By including their opinions, the study is guaranteed to take into account actual usage and the social aspects of risk.

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

I will be using my already existent professional connections with cybersecurity experts and clinicians via online platforms. I aim to reach participants, including those who use wearable medical devices, through a variety of channels, such as social media sites like Facebook, LinkedIn, and WhatsApp. Additionally, I want to use the publicly accessible email addresses of cybersecurity experts and healthcare professionals to reach out and ask them to distribute internal questionnaires throughout their various websites.

SECTION 5: INFORMATION, CONSENT AND CONFIDENTIALITY

5.1 **Participant Information Letter (PIL) for participants**

Please confirm below that your information letter covers:

Description of the research topic and method	N/A
Details of what participation will involve	N/A
Rights to anonymity	N/A
Confidentiality	N/A
Rights to withdraw from the research	N/A
The contact details of the researcher and supervisor (if necessary)	N/A

5.2 **Informed Consent Form (ICF) for participants**

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

No: my research study involves an online survey only and/or does not require signed consent. Consent will be included in the online survey as follows:

1.Do you consent to participate in this study?

Yes, I consent to participate.

No, I do not consent to participate

SECTION 6: STORAGE OF DATA

6.1. How will you store the research data and for how long? How will you manage data protection issues?
Survey responses including all other research data and analysis files will be stored securely in a password-protected Laptop. A backup copy will be stored in an online cloud storage platform (OneDrive) to prevent data loss. All the research data will be kept for a period of up to two years after the qualification is awarded. This retention period is in accordance with the data protection regulations to allow for potential further analysis or verification. After this period, the data will be securely and permanently deleted.

1. **Password Protection:** All electronic files containing research data will be password-protected using strong, unique passwords and will be accessed only by the researcher.
2. **Access to Data:** As part of the thesis submission, the raw, anonymized data will be submitted to the college submission platform (Moodle) for record-keeping and grading purposes.
3. **Data Encryption:** The storage devices (cloud storage or hard drive) will be password encrypted to prevent unauthorized access to the data.

SECTION 7: NON-DISCLOSURE AGREEMENT & STUDENT CONSENT

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

No

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

Yes

SECTION 8: RECORDING AND RETENTION OF DISSERTATION VIVA

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

SECTION 9: DOCUMENT CHECKLIST

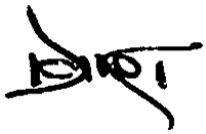
NOTE: Applicants must attach the following documents in electronic format to the appendix.

Which documents are added to the appendix? Please tick N/A if not applicable:
9.1 Participant Information Letter (PIL) for participant N/A

9.2 Informed Consent Form (ICF) for participant	N/A
9.3 Questions/survey for interviewees/focus groups etc *(can be in draft form)*	Yes
9.4 Any other documents e.g. Non-Disclosure Agreement	N/A

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

For Student:

STUDENT SIGNATURE: 

DATE:07/07/2025.

APPENDIX B: SURVEY QUESTIONNAIRE

This survey is developed by Bridget Epepitimi Kalabo, an MSc student of Medical Device Technology and Business at Griffith College Dublin, in order to collect primary data for her thesis titled "**Cybersecurity Vulnerabilities in Wearable Medical Devices: A Cross-Sector Analysis of Risks and Mitigation Strategies using Ireland as a case study**".

The purpose of this survey is to get your thoughts and experiences about cybersecurity of wearable medical devices like blood pressure monitors, smart watches, fitness trackers, etc. It covers important topics including identifying cybersecurity flaws, the risks and effects of possible cyberthreats, the efficiency of current cybersecurity frameworks, and your suggestions for improving security in this rapidly changing industry. Depending on the level of detail of your responses, the survey should take you 10 to 15 minutes to complete. Your feedback will inform the innovation of safer wearable medical devices by pointing out real-world threats, assessing existing security measures, and suggesting user and sector driven modifications. By comparing the perspectives of cybersecurity experts, clinicians, and end users, this study also seeks to better understand how cross-sector cooperation might improve cybersecurity in wearable medical devices, especially in the context of Irish healthcare. Any data gathered will only be utilized for scholarly research, and all answers will remain anonymous. Participation in the study is completely voluntary, and you are free to withdraw at any time before sending in your answers.

Do you consent to participate in this study?

☐ Yes, I consent to participate.

☐ No, I do not consent to participate

SECTION A: SOCIO-DEMOGRAPHIC DATA

1. Age: _____

2. Gender: [ ] Male [ ] Female [ ] Other

3. Occupation: _____

4. Educational Level:
   [ ] Primary
   [ ] Secondary
   [ ] Tertiary
   [ ] Postgraduate
   [ ] Others (Specify): _____

5. Do you use any wearable medical devices? [ ] Yes [ ] No

6. Type of device used (if any): _____

7. Duration of usage: _____

8. Have you ever experienced a technical or data-related issue with your wearable device? [ ] Yes [ ] No

SECTION B: IDENTIFYING CYBERSECURITY VULNERABILITIES

9. Have you experienced any of the following while using your wearable device? (Check all that apply)
- [ ] Device malfunction
- [ ] Data loss
- [ ] Unusual activity alerts
- [ ] Unauthorized access
- [ ] None

10. Do you think your wearable medical device is secure? [ ] Yes [ ] No [ ] Not Sure

11. Are you aware of any potential cybersecurity risks related to wearable medical devices? [ ] Yes [ ] No

12. i) Which of the following do you consider as possible vulnerabilities? (Check all that apply)
- [ ] Bluetooth connectivity
- [ ] Cloud data storage
- [ ] Weak passwords
- [ ] Lack of software updates

ii) Are there any vulnerabilities you see that have not been listed?

_____
_____
_____

Kindly tick the best options that applies to the questions below

Where SD= Strongly Disagree (1); D= Disagree (2), = Neutral (3), A= Agree (4) and SA= Strongly Agree (5)

Statement	SA	A	N	SD	D
13. My wearable medical device receives regular software/firmware updates.					
14. I am aware of the cybersecurity risks associated with wearable medical devices.					
15. My device is protected with strong authentication (e.g., password/biometric).					

16. I consider the wireless connection (e.g., Bluetooth/Wi-Fi) of my device secure.					
17. I have experienced suspicious or abnormal activity from my wearable device.					
18. I believe most wearable medical devices lack strong built-in cybersecurity.					
19. I feel that the manufacturer has prioritized security in my wearable device.					
20. My device uses encryption to protect sensitive health data during transmission.					
21. The security settings of my wearable device are user-friendly and accessible.					
22. I regularly review privacy and security policies related to my wearable device.					

SECTION C: DANGERS AND IMPACTS OF CYBERSECURITY THREATS

23. Do you believe a cyberattack on a wearable device could impact your health? [ ] Yes [ ] No [ ] Not Sure

24. Are you concerned about your personal health data being accessed by unauthorized persons? [ ] Yes [ ] No

25. Have you ever stopped using a medical device due to cybersecurity concerns? [ ] Yes [ ] No

26. Do you know anyone who has had a cybersecurity issue with their medical device? [ ] Yes [ ] No

Kindly tick the best options that applies to the questions below

Where SD= Strongly Disagree; D= Disagree, = Neutral, A= Agree and SA= Strongly Agree

Statement	**SA**	**A**	**N**	**SD**	**D**
27. A cyberattack on a wearable device could lead to incorrect health readings or diagnoses.					
28. I am concerned that cyber threats may compromise my personal health information.					

29. Cybersecurity breaches in wearable devices may cause harm to patients.					
30. Knowing that my wearable device could be hacked makes me uneasy.					
31. Healthcare services are at risk due to vulnerabilities in wearable medical devices.					
32. Device hacking may result in loss or manipulation of critical health data.					
33. A compromised wearable device could affect trust in digital healthcare systems.					
34. Cyber threats can lead to psychological distress among patients relying on wearables.					
35. Data breaches from wearable devices could lead to financial or reputational harm.					
36. I believe more safeguards are needed to reduce the risks posed by wearable medical devices.					

SECTION D: EVALUATION OF EXISTING CYBERSECURITY FRAMEWORKS

29. Are you familiar with data protection regulations such as General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA)? [ ] Yes [ ] No

30. Do you believe existing laws are sufficient to protect wearable device users? [ ] Yes [ ] No [ ] Not Sure

31. How frequently is your wearable device updated by the manufacturer?
[ ] Regularly
[ ] Occasionally
[ ] Rarely
[ ] Never

32. Does your device notify you about software or security updates? [ ] Yes [ ] No

Kindly tick the best options that applies to the questions below

Where SD= Strongly Disagree; D= Disagree, = Neutral, A= Agree and SA= Strongly Agree

Statement	**SA**	**A**	**N**	**SD**	**D**
38. I am aware of data protection regulations (e.g., GDPR, HIPAA) that apply to wearable medical devices.					

39. The cybersecurity framework of my device aligns with known standards or certifications.					
40. Healthcare organizations effectively implement cybersecurity protocols for wearable devices.					
41. Manufacturers clearly communicate their security frameworks and device protections.					
42. Current cybersecurity frameworks are sufficient to protect wearable devices from cyber threats.					
43. There is a need for more consistent international regulations for wearable medical device security.					
44. Security features such as data encryption and access control are well implemented in wearable devices.					
45. I believe real-time threat detection should be a required part of cybersecurity frameworks.					
46. The current frameworks lack adequate enforcement mechanisms for manufacturers.					
47. Independent audits of wearable device security frameworks should be regularly conducted.					

SECTION E: RECOMMENDATIONS FOR ENHANCING CYBERSECURITY

48. Which of the following do you think would improve device security? (Check all that apply)
[ ] Stronger encryption
[ ] Two-factor authentication
[ ] Regular software updates
[ ] User education

49. Would you be willing to pay more for a wearable device with guaranteed cybersecurity protection? [ ] Yes [ ] No

50. What recommendations would you offer manufacturers to improve the safety of wearable devices?

_____
_____

51. In your opinion, who should be primarily responsible for ensuring device security?
[ ] Government

[ ] Manufacturers
[ ] Users
[ ] Healthcare providers

Kindly tick the best options that applies to the questions below

Where SD= Strongly Disagree; D= Disagree, = Neutral, A= Agree and SA= Strongly Agree

Statement	**SA**	**A**	**N**	**SD**	**D**
52. Manufacturers should be mandated to meet minimum cybersecurity standards for wearable medical devices.					
53. Cybersecurity training should be provided to users of wearable medical devices.					
54. Third-party cybersecurity audits should be required before devices are released to the market.					
55. Healthcare providers should offer technical support to patients on device cybersecurity practices.					
56. Devices should include real-time threat alerts and automatic security updates.					
57. Users should have greater control over the privacy and security settings of their wearable medical devices.					
58. There should be stricter penalties for manufacturers that fail to protect users' data.					
59. Wearable devices should require multi-factor authentication before access is granted.					
60. Encryption protocols should be mandatory for all wearable medical devices.					
61. Governments should implement universal security certification for medical IoT devices.					