Grant Agreement No.: 101095542
Call: HORIZON- HLTH-2022-IND-13
Topic: HORIZON-HLTH-2022-IND-13-01
Type of action: HORIZON-RIA

CYLCOMED

Cyber-security toolbox
for connected medical devices

D3.3 Guidance improvement

Revision: v.1.0

Work package	WP 3
Task	Task 3.1
Due date	31/05/2024
Submission date	31/05/2024
Deliverable lead	FHUNJ
Version	01.0
Authors	Andrés Castillo (FUHNJ), Santiago Bollain (FUHNJ)
Reviewers	João Rodrigues (INOV)

Abstract	This report, which is the outcome of Task 3.1 in Work Package 3, analyzes the vulnerabilities related to cybersecurity threats faced by users of connected medical devices. It specifically addresses the vulnerabilities associated with the introduction of new technologies in the healthcare sector. The objective of this report is to provide recommendations for enhancing future editions of the Medical Device Coordination Group's cybersecurity guide for manufacturers, known as MDCG 2019-16. The guide aims to assist healthcare professionals in meeting the requirements of the Medical Devices Regulation and the In-Vitro Products Regulation. The focus of this report is to identify significant gaps and propose specific measures to strengthen the regulatory framework for the Internet of Medical Things (IoMT).

Keywords	Connected Medical Devices, In-Vitro Devices, Cybersecurity, MDCG, Guidance, Threats, Risks, Regulations

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	12.01.2024	First draft	Andrés Castillo, Santiago Bollaín
V0.2	30.04.2024	Ready for first review	Andrés Castillo, Santiago Bollaín
V0.3	14.05.2024	First Revision	João Rodrigues
V0.4	27.05.2024	Comments addressed	Andrés Castillo, Santiago Bollaín, Dusko Milosevic
V0.5	28.05.2024	Final Revision	João Rodrigues
V1.0	29.05.2024	Final Version	Andrés Castillo, Santiago Bollaín

Funded by Horizon Europe Framework Programme of the European Union

Disclaimer

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	R	
Dissemination Level		
PU	*Public, fully open, e.g. web*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagrams, algorithms, models, etc.

Funded by Horizon Europe Framework Programme of the European Union

Executive summary

This document outlines the criteria for expanding the existing baselines from both a technical and organizational viewpoint. It is a component of Task 3.1 within Work Package 3, which has carried out a thorough examination focused on end-users operational areas where Connected Medical Devices (CMD), In-Vitro Devices (IVD) and Software as a Medical Device (SaMD) are incorporated. This analysis encompasses all risk categories and associated vulnerabilities, as well as potential threats and attacks that could spread, in order to meticulously outline the necessary tools for effective mitigation.

The purpose of Medical Device Coordination Group guidance (MDCG 2019-16) is to support healthcare professionals in adhering to the requirements of the Medical Device Regulation and the In-Vitro Device Regulation. This report provides an initial assessment of MDCG 2019-16, highlighting significant gaps and suggesting a comprehensive list of suggestions to strengthen the regulatory framework for the Internet of Medical Things (IoMT).

This deliverable examines the major challenges associated with cybersecurity in the healthcare sector, specifically focusing on hospitals and telemedicine. These two settings heavily rely on interconnected medical devices, which necessitates their consideration in terms of threat and risk management. Additionally, this document briefly touches upon emerging technologies that are currently being developed and adopted in these environments, emphasizing their importance for future iterations of the guide.

The more precise recommendations for improving the guidance have been detailed within the scope of a number of ongoing projects (2023-2025) funded through the Horizon Europe call 'Enhancing the cybersecurity of connected medical devices': HORIZON-HLTH-2022-IND-13-01.

Funded by Horizon Europe Framework Programme of the European Union

Table of contents

Funded by Horizon Europe Framework Programme of the European Union

Abbreviations

AI[1]	Artificial Intelligence
AMD[1]	Active Medical Device
BGA[1]	Blood Gas Analyzer
CE	Clinical Evaluation
CIA	Confidentiality, Integrity and Availability
CMD[1]	Connected Medical Device
CPM[1]	Continuous Passive Motion
CSIRT	Computer Security Incident Response Team
CT[1]	Computed Tomography (scan)
ECG[1]	Electrocardiograph
ECMO[1]	Extracorporeal Membrane Oxygenation
EEG[1]	Electroencephalograph
EKG[1]	Electrocardiograph
EN	European Standard
ENISA	European Union Agency for Cybersecurity
FSCA	Field Safety Corrective actions
GDPR	General Data Protection Regulation
GSPR	General Safety and Performance Requirements
IAM[1]	Identity and Access Management
IDS[1]	Intrusion Detection Systems
IEC/TR	International Electrotechnical Commission - Technical Report
IMDRF	International Medical Device Regulators Forum
IoHT[1]	Internet of Health Things
IoMT[1]	Internet of Medical Things
IPS[1]	Intrusion Prevention Systems
ISMS	Information security management system
ISO/IEC	International Organisation for Standardisation/ International Electrotechnical Commission
ISV[1]	Independent Software Vendor
IT	Information Technology
IVDR	In Vitro Diagnostic Medical Devices Regulation; EU 2017/746
LASIK[1]	Laser-Assisted in Situ Keratomileusis
MD	Medical Device
MDCG	Medical Device Coordination Group
MDR	Medical Devices Regulation; EU 2017/745
MDS2	Manufacturers Disclosure Statement for Medical Device Security
MDSW	Medical Device Software
MIR	Manufacturer Incident Report
MRI[1]	Magnetic Resonance Imaging
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
OES	Operator of Essential Services

[1] *Abbreviations used in MDCG 2019-16 rev. 1*

Funded by Horizon Europe Framework Programme of the European Union

OTS	Off the Shelf software
PACS[1]	Picture Archiving and Communication System
PET[1]	Positron Emission Tomography
PLC[1]	Programmable Logic Controller
PSR	Periodic Summary Reports
PSUR	Periodic Safety Update Report
QMS	Quality Management System
RFP[1]	Request for proposal
SOTA	State of the Art

Funded by Horizon Europe Framework Programme of the European Union

1 Introduction

Information is the lifeblood of healthcare, as the World Economic Forum's report “Risk and Resilience: Understanding Systemic Cyber Risk” emphasizes. A significant quantity of sensitive and vital data, particularly credit card numbers, bank account information, social security numbers, and health data including diagnoses, insurance claims, and medical records, are gathered, stored, and processed by the healthcare industry.

Nevertheless, the healthcare industry has not made a commensurate investment in cybersecurity, leading to a deficiency of best practices to guarantee the confidentiality, integrity, and availability of vital and delicate personal and health-related data. This also holds for medical equipment. Security was not seen as a top priority until recently.

The analysis of cybersecurity baselines and potential improvements, security guidelines recommendations for various actors (clinicians, IT departments, manufacturers of medical devices), and suggestions to enhance the "MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices" are the main foci of this report.

1.1 Cybersecurity threats in the healthcare sector

Since cybersecurity helps shield private patient data from cybercriminals, helps guarantee patients’ data integrity for correct diagnosis and treatment, and helps guarantee the availability of IT equipment and overall hospital services, it is crucial for the healthcare industry. Because they store so much personal data—including financial, insurance, and medical records—healthcare organizations are a prime target for cyberattacks. A cyberattack on a healthcare facility may result in identity theft, patient privacy violations, and in certain situations, even fatalities.

Cyberattacks have the potential to severely impact healthcare organizations financially in addition to harming patients. For the healthcare sector, the consequences of a data breach can be catastrophic.

Furthermore, healthcare companies frequently take a while to implement new cybersecurity safeguards, which increases their susceptibility to intrusions. The intricacy of healthcare systems and the dearth of resources for putting new security measures in place are partially to blame for this.

In order to safeguard patient safety, avoid financial loss, and preserve patient privacy, cybersecurity is essential in the healthcare industry. Healthcare companies need to be proactive in protecting their data and systems from cyberattacks.

1.2 Evolution of medical devices and their interconnectivity

Healthcare providers are showing a growing inclination toward acquiring, preserving, and analyzing data produced by medical devices. In the health sector, there is a rising trend of medical device public tenders and Requests For Proposals (RFP) that demand communication protocol availability for medical devices. This access is sought to ensure the comprehensive capture of all the measured data. Numerous medical device manufacturers have already taken the initiative to provide their protocols, facilitating the seamless data capture process.

Funded by Horizon Europe Framework Programme of the European Union

1.3 Methodology

The methodology used for the analysis of the MDCG Guidance is rooted in doctrinal analysis for the interpretation of the rules at the EU level. In addition, it benefits from information security and risk management disciplines and incorporates them into legal research to assess the current legal rules and best practices available. For this reason, the overall methodology used in this research can be considered a socio-legal study. This type of study is distinguished by a lack of (formalised) methodology as well as a diversity of techniques and "ways of doing". One of these "means of doing" is unquestionably examining ideas and concepts from other disciplines to incorporate them into legal research and generate new legal ideas. This choice of methodology is justified because cybersecurity is considered an interdisciplinary course of study consisting of information security, law, policy, human factors, ethics, and risk management. The analysis of the MDCG Guidance has been based on secondary sources and best practices.

1.4 Structure of the document

The document is structured as follows:

- Section 2 is dedicated to security guidance suggestions for the different actors: clinicians, IT department, medical device manufacturers;
- Section 3 enumerates some cybersecurity issues associated with the implementation of the technologies of Healthcare 4.0;
- Section 4 describes the proposed improvements for the “MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices”;
- The final section is reserved for the conclusions.

Funded by Horizon Europe Framework Programme of the European Union

2 Cybersecurity Guidance in Healthcare

2.1 Introduction

Health 4.0 [1] has emerged as the prevailing concept in the healthcare sector, signifying the fusion of advanced technology and the healthcare industry. To grasp the essence of Health 4.0, it is essential to delve into the notion of Industry 4.0. This term denotes the fourth industrial revolution, characterized by the integration of digital, physical, and biological systems. Key technologies associated with Industry 4.0 encompass cloud computing, Big Data, the Internet of Things, wireless communication (including 5G), cryptography, augmented reality, and content-based image retrieval. Health 4.0 extends the principles of Industry 4.0 to the realm of healthcare, envisioning a future where intelligent machines and technologies play a pivotal role in enhancing healthcare services [2].

Health 4.0 signifies a revolutionary change in the healthcare industry, where technology plays a crucial role in improving patient outcomes and streamlining healthcare delivery [3][4]. At the core of this transformation is the Internet of Health Things (IoHT), which encompasses interconnected medical devices, wearables, and sensors that gather and exchange health data. Additionally, medical cyber-physical systems integrate physical devices with digital systems to enable real-time monitoring and decision-making. The concepts of Health Cloud [5] and Health Fog [6] utilize cloud and edge computing to enhance data processing and storage efficiency. The physical separation between IoT and the cloud poses a challenge in delivering services that meet specific demands, such as quick response time and less computationally intensive processing. In order to meet these demands, the implementation of a middleware technology, like Fog, becomes necessary. The Fog acts as an intermediary between the cloud and the IoT ecosystem. By embracing the concept of Health Fog, the convergence of cloud and IoT can be achieved, enabling the deployment of intelligent healthcare solutions [7][8].

The principles of Healthcare 4.0 and the "4P" model [9] complement each other. This model is based on four fundamental components:

- Personalized Medicine involves customizing medical treatments for individual patients based on their unique characteristics. It entails gathering detailed information about each patient through methods like genomics, proteomics, metabolomics, and transcriptomics. By analyzing this personalized data, healthcare professionals can make more accurate diagnoses and create targeted treatment plans.
- Predictive Medicine focuses on using personalized information to forecast an individual's risk of developing specific diseases. By examining genetic and other pertinent data, healthcare providers can estimate the probability of certain health conditions. Equipped with this knowledge, they can take proactive measures to prevent or lessen potential health issues.
- Preventive Medicine aims to decrease the occurrence of diseases by identifying risk factors and implementing strategies to avoid them. This includes lifestyle changes, therapeutic options, and other interventions. Instead of waiting for illness to strike, preventive medicine promotes early action to preserve health and prevent disease.
- Participatory Medicine underscores the collaboration between patients and healthcare providers. It acknowledges that patients play an active role in their health journey. In this model, patients are empowered to make informed decisions about their health, while healthcare professionals work alongside them. The objective is to eliminate excessive paternalism and cultivate a genuine partnership in healthcare.

Some experts even propose a fifth P: Precision Medicine, which elevates personalization by ensuring that treatments are not only tailored but also administered with utmost accuracy.

Funded by Horizon Europe Framework Programme of the European Union

Healthcare 4.0 introduces innovative technologies to the healthcare sector, with a strong emphasis on maintaining the security and privacy of data. Cloud-based electronic health records (EHRs) allow for convenient remote access to patient information, streamlining healthcare services. However, it is imperative to prioritize the security and privacy of sensitive medical data stored in the cloud.

The Healthcare 4.0 framework encompasses various layers for data management, including sensing, storage, sharing, and auditing. Safeguarding patient records from unauthorized access and cyber threats is critical. While traditional cryptography methods have been utilized for secure data storage, they may present challenges in terms of efficiency, user verification, and service verification.

Blockchain-based security solutions have emerged as a reliable option for ensuring robust security in medical data storage and sharing, with minimal computational burden. In IoT-cloud-based e-Health systems, security and privacy are key considerations. Effective solutions involve implementing secure consensus mechanisms, addressing privacy issues, and developing user-friendly interfaces for seamless integration. As the risk of patient data exploitation grows, cybersecurity collaboration between providers and healthcare facilities is essential to protect patient identities and prevent data breaches.

Certain cybersecurity issues that pertain to various stakeholders within the healthcare industry will be now explored.

2.2 Hospitals

Hospitals face various types of cyberattacks, such as ransomware attacks where hackers encrypt the hospital's data and demand a ransom for its release. In some cases, hospitals have had to pay a ransom to regain access to their data. Cybercriminals employ phishing attacks by sending deceptive emails or messages that appear to be from trusted sources like hospital staff or vendors. The aim is to trick the recipient into opening an attachment or clicking on a link that leads to malicious content [10].

Insider threats occur when an employee or contractor with access to confidential information intentionally or accidentally damages the hospital's systems or data [11].

Within the healthcare industry, the most common vulnerability is inadequate security measures. This can include incorrect system configurations, outdated software, and weak passwords.

Human error or internal individuals within the organization can also contribute to security breaches. This may involve staff members inadvertently disclosing private information or falling victim to phishing scams.

Phishing and social engineering are commonly utilized methods for initiating hacking and stealing data. This may involve hackers masquerading as trustworthy sources in an attempt to manipulate staff members into revealing confidential information.

With the increasing integration of medical devices, such as insulin pumps and pacemakers, into hospital networks, they become more vulnerable to cyberattacks. Cybercriminals exploit these devices to either pilfer data or cause harm to patients through medical device hijacking attacks. Additionally, they employ denial-of-service attacks to overwhelm the hospital's network with excessive traffic, resulting in system crashes and impeding access to critical systems [12].

To counter these threats, hospitals must implement robust cybersecurity measures. These measures encompass data encryption, network segmentation, and regular staff training.

Funded by Horizon Europe Framework Programme of the European Union

Furthermore, hospitals should establish a response plan to minimize damage and ensure a swift recovery in the event of a cyberattack [13][14].

Only a limited number of hospitals have incorporated cybersecurity training for users of connected medical devices. As an illustration, the MOOC Cybersecurity in Healthcare (Hospitals & Care Centres) was created as part of the SecureHospitals.eu initiative, which received funding from the European Commission's Horizon 2020 program. The primary objective of this online course is to enhance awareness and knowledge of cybersecurity within the healthcare industry, while also promoting the adoption of innovative cybersecurity solutions for medical purposes.

This freely accessible online course has been developed by the Erasmus University Rotterdam and aims to provide participants with a comprehensive understanding of the importance of digitalization and cybersecurity in the healthcare field. Students will have the opportunity to delve into the challenges and opportunities that arise from the digitalization and abundance of medical data in the healthcare sector. The Massive Open Online Course (MOOC) is entirely accessible online and is intended to be followed at your own pace. The primary topics that are covered by the course are:

- Cybersecurity in healthcare: technology, data, and human behaviour.
- Social aspects of cybersecurity: social engineering and social media.
- Data breaches, hackers, and malware in healthcare.
- Cyber hygiene: practices to improve cybersecurity.

2.3 Medical Device Manufacturers Instructions

As with many other aspects, the MDR and IVDR do not provide a definitive list of specific steps, which is a problem for many manufacturers, particularly their software developers.

A lot of software was never or is not being developed from the ground up with cybersecurity in mind, and certainly not in the context of a good risk management plan that considers all of the risks associated with its use in the environment in which it is used, the hardware on which it runs, the dependencies it has with other systems, and the relationship with other legislation that also governs software or IT processes, such as the General Data Protection Regulation (GDPR).

Software developers scrum and rush all over the place, often without a clear picture of where they want to go in terms of cybersecurity. Often, development teams will focus on delivering ‘something that works' rather than 'the software specified that meets the requirements specified', and they may even add security at the end. Also, post-market surveillance is rarely a top priority. Even though there is a clear regulatory framework for introducing medical devices to the market, manufacturers' cybersecurity cultures remain inconsistent. They fail to include cybersecurity in the MD design and development process because there are few guidelines or recommendations dedicated solely to IT cybersecurity of medical devices [15].

Manufacturers of medical devices typically offer not very detailed instructions and guidelines to ensure safe and effective use in terms of the existing cybersecurity threats. These instructions commonly include the following elements [16]:

- Device Identification and Intended Use: Manufacturers specify the device's intended purpose, patient population, and any limitations to help users understand when and how to use the device appropriately.
- Installation and Setup: Instructions cover how to properly install and set up the device, including physical placement, connecting components, and configuring settings.

Funded by Horizon Europe Framework Programme of the European Union

- Operating Procedures: Step-by-step instructions guide users through using the device, including turning it on, adjusting parameters, and performing necessary actions.
- Maintenance and Cleaning: Manufacturers outline routine maintenance tasks such as cleaning, calibration, and replacing consumables to ensure device longevity and accuracy.
- Troubleshooting: Instructions include troubleshooting steps for common issues so users can refer to them if the device malfunctions or displays errors.
- Safety Precautions: Manufacturers emphasize safety precautions to prevent harm to users, patients, or operators, including warnings about potential hazards and how to mitigate risks.
- Storage and Transport: Guidelines cover proper storage conditions (temperature, humidity, etc.) and safe transportation practices.
- Disposal and Recycling: Manufacturers provide information on environmentally responsible disposal of the device and its components.
- Software Updates and Upgrades: If applicable, instructions explain how to update or upgrade device software to maintain functionality and security.
- Contact Information: Manufacturers include contact details for technical support, customer service, and reporting adverse events.

2.4 Weaponization of Medical Devices

In this section, the potential threat of hackers weaponizing medical devices to harm patients in healthcare settings is examined. This is a key factor in the decision to classify hospitals as critical infrastructures by the European Commission. The main concern revolves around the consequences of a cyber attacker gaining access to a hospital network that manages the operations or settings of an active medical device (AMD) [10].

An active medical device is one that directly interacts with a patient to deliver medical care. Nowadays, many active medical devices are equipped with a computer for control and network communication. The simplest method for a hacker to manipulate an active medical device is to connect to the device's computer and issue commands directly. A majority of programmable logic controllers (PLC), protocol converters, or data acquisition servers lack basic authentication mechanisms and execute any correctly formatted command they receive without verification. In comparison to standard corporate IT networks found in financial or insurance companies, a healthcare facility's computer network is significantly more susceptible to cyber threats.

Researchers have identified numerous instances of medical device compromise, encompassing X-ray machines, PACS, and BGAs. This encompasses a wide range of diagnostic equipment (ultrasound, PET scanners, CT scanners, MRI, X-ray, etc.), physical therapy devices like CPM machines, therapeutic tools (infusion pumps, medical lasers, LASIK surgical machines), and life support machinery (heart-lung machines, medical ventilators, ECMO machines, dialysis machines). Additionally, medical laboratory equipment used for blood, urine, gene, and blood gas analysis, as well as medical monitors such as ECG, EEG, and blood pressure machines, are susceptible to hacking. Even modern electronic stethoscopes are not immune to potential security breaches.

Funded by Horizon Europe Framework Programme of the European Union

3 Guidance for cybersecurity for new technologies in healthcare

The emerging concept of Health 4.0 is focused on enhancing healthcare services through advanced technologies, leading to more efficient processes and improved reliability. The implementation of healthcare software aligned with Health 4.0 requires specialized expertise not commonly found in hospitals. The COVID-19 pandemic has accelerated the adoption of these technologies, originally implemented in other sectors, to meet the demand for remote healthcare services. Health 4.0 relies on cutting-edge technologies like Big Data Analytics, Machine Learning, and Blockchain to improve diagnostics, treatment planning, and data security. Despite the opportunities presented by these technologies, some new challenges and threats have yet to be fully addressed in regulations or guidelines from the MDCG.

Security recommendations for different stakeholders, such as clinicians, IT departments, medical device manufacturers, system integrators, or ISVs, when handling medical device data greatly depend on the selected deployment architecture. It is crucial to prioritize identifying the data owner and its exact storage location. With multiple strategies in use, data ownership may differ, with data potentially belonging to the hospital, the medical device manufacturer, or the ISV, and stored either at the hospital or in a private cloud.

This section addresses the emerging threats brought about by technology and emphasizes the necessity for updated guidance to effectively prevent and manage them.

3.1 Machine Learning and Big Data Analytics

Artificial intelligence is revolutionizing clinical research and healthcare delivery, but it also brings forth concerns regarding security and privacy. The foremost consideration is to guarantee online privacy and security. AI models rely on extensive datasets, and without proper safeguards, patient information could be jeopardized. It is the responsibility of hospitals and research institutions to safeguard patient data. Establishing agreements to ensure strict data protection standards is crucial when collaborating with third-party AI vendors [17] [11].

In addition, regulatory challenges arise as AI technologies advance at a faster pace than regulatory agencies can keep up with. Compliance with the General Data Protection Regulation remains a hurdle for AI providers in the health sector. Gaps in the regulatory framework pose a risk to patient security and privacy.

There are additional worries regarding the ethical and safety aspects. AI has the ability to process vast quantities of data. Nevertheless, ethical dilemmas emerge when medical decisions impact individuals. To prevent discriminatory results, it is important to guarantee that AI models remain unbiased, impartial, and transparent. One of the safety concerns is the risk of incorrect diagnosis or inaccurate treatment recommendations.

The fourth concern revolves around the interaction between humans and artificial intelligence. The effectiveness of artificial intelligence tools relies on how humans utilize them. Mistakes and unintended consequences can occur if AI is used incorrectly. Patients and healthcare professionals play a vital role in ensuring the ethical deployment of AI [18].

3.2 Blockchain

The utilization of blockchain technology can improve the security of healthcare data due to its decentralized nature and data-sharing capabilities. By distributing information across the network, blockchain eliminates the risk of a single point of failure, thus reducing the likelihood

Funded by Horizon Europe Framework Programme of the European Union

of data loss. Enhanced data security and resilience against breaches are achieved through the removal of central control [26] [27].

Additionally, cryptographic algorithms protect the data stored on a blockchain, ensuring that the information is safeguarded against manipulation.

Moreover, blockchain enables the tracing and verification of data records. Changes to patient information are transparently recorded, creating a tamper-proof and reliable system.

Blockchain's immutability, traceability, and openness contribute to an overall improvement in security. Decentralized patient data management powered by blockchain technology can enhance efficiency and care delivery in hospitals.

However, it is important to acknowledge the potential dangers and obstacles associated with blockchain technology in healthcare. One such concern is the presence of coding flaws in smart contracts that automate processes. These vulnerabilities can result in unauthorized access or unintended actions. To address these risks, regular code audits and security testing are essential.

Another potential threat is the occurrence of "51% attacks" in public blockchains. In such cases, individuals with more than half of the network's computing power can manipulate transactions. Hospitals utilizing public blockchains should be cautious of this risk and consider utilizing private or consortium blockchains as an alternative solution [28].

Data leakage through private keys is a serious concern. The blockchain relies on cryptographic keys for security. If private keys are compromised, criminals could gain unauthorized access to sensitive medical data. Proper key management practices are crucial to prevent potential data breaches.

The transparency and immutability of blockchain technology may conflict with privacy regulations such as GDPR. It is important to carefully balance transparency with patient privacy rights.

Integrating blockchain with existing medical systems can introduce new challenges. Misconfigurations can expose vulnerabilities, and human error and social engineering are significant risks. While blockchain can enhance security, it does not eliminate the possibility of human mistakes leading to security breaches. Social engineering attacks can also compromise blockchain systems [29].

Despite the enhanced security provided by the blockchain, it is imperative for the MDCG guidance to address these challenges in order to fully leverage its benefits and ensure the protection of patient data.

3.3 IoMT and 5G Networks

The Internet of Medical Things (IoMT) encompasses a network of medical devices, software applications, and services that connect to healthcare and telemedicine platforms. These interconnected layers work together to improve healthcare delivery. The number of connected IoT sensors has increased significantly, making it a prominent trend in the healthcare industry [19][20].

IoMT requires multiple layers of interaction, as outlined in D3.1. The initial step involves sensors and data sources, such as wearables and medical sensors, which capture vital signs. The data is then transmitted through gateways and high-speed 4G/5G networks for processing. The final stage involves management services and data storage, which handle large amounts of raw data and extract valuable insights from it.

Funded by Horizon Europe Framework Programme of the European Union

The growing adoption of IoMT can be attributed to its numerous benefits and applications. IoT devices enable healthcare professionals to automate data recording, ensuring accuracy and efficiency. Real-time data exchange facilitates seamless collaboration among care teams. Connected devices allow for continuous monitoring of patients' health conditions, making remote health monitoring possible and enhancing patient engagement. IoMT also contributes to reducing healthcare costs while improving treatment outcomes. Ultimately, IoT in healthcare empowers doctors, streamlines processes, and leads to better patient care and operational effectiveness [21].

The integration of Internet of Things (IoT) devices in the healthcare industry has brought about both convenience and risks. The adoption of IoT in healthcare has introduced vulnerabilities in medical devices and software, posing potential threats to patient safety and system integrity. Specifically, electronic health records, wireless infusion pumps, endoscope cameras, and radiology information systems have been identified as particularly susceptible. Critical vulnerabilities include poor credential management and hard-coded credentials, which can be exploited by malicious actors to gain unauthorized access or manipulate health data.

Determining ownership and control of the data generated by IoT devices can be a complex task. The collection and utilization of location data can raise privacy concerns. Distributed Denial of Service (DDoS) attacks have the potential to disrupt healthcare services. Additionally, unauthorized access (known as medjacking) to medical devices can compromise patient safety. It is worth noting that legacy medical devices may lack robust security features, further exacerbating the risks associated with IoT integration in healthcare.

Some measures can be taken to mitigate the risks. Developers must adhere to secure coding practices in order to minimize vulnerabilities. It is important to properly segment networks to limit the impact of a breach. By having separate networks for different device types, such as patient monitoring and administrative devices, the lateral movement can be prevented. Continuous security monitoring is essential to promptly detect and address threats. Collaborative efforts, regulatory compliance, and a proactive approach to security are necessary to safeguard medical IoT devices. Ensuring the protection of Internet of Things devices in hospitals from cyber-attacks is crucial for patient safety and data integrity. Effective strategies include the implementation of firewalls to control incoming and outgoing traffic for IoT devices, regular scanning and updating of devices to detect and remove malware, and the use of Intrusion Detection/Prevention Systems (IDS/IPS) to monitor network traffic for any suspicious activity.

Identity and Access Management (IAM) tools are essential for managing user access to devices and data, although it is usually not possible to incorporate them into connected medical devices in critical environments, such as surgery rooms and intensive care units. Clinical centers have strict controls in place to limit physical access to critical infrastructure and sensitive areas.

It is crucial to regularly update all applications, internal software, network tools, and operating systems with the latest patches and updates. Security vulnerabilities should be promptly addressed by applying patches provided by vendors. Manufacturers need to collaborate closely with third-party vendors to ensure that security features are integrated into devices and that vendors adhere to best practices for device security.

Protecting IoT devices in hospitals requires a comprehensive approach that involves technology, policies, and well-trained staff. Hospital employees should receive training on cybersecurity best practices to increase their awareness of the risks associated with IoT devices and to promote vigilance. Collaboration with Government Agencies is also essential for enhancing security measures in hospitals.

The integration of IoMT with the 5G network is essential for enhancing connectivity and efficiency in the medical field. 5G technology empowers IoMT by enabling seamless

Funded by Horizon Europe Framework Programme of the European Union

communication and data sharing among various devices and software through advanced features like machine learning and automation. The high-speed transmissions, extensive coverage, low latency, and increased capacity provided by the 5G network are crucial for supporting IoT applications, telemedicine, and other medical advancements. Additionally, the combination of 5G and IoMT allows for the development of highly secure networks, ensuring the protection of sensitive medical data [22].

Preserving privacy in the Internet of Medical Things (IoMT) is crucial, particularly in the context of rolling out 5G networks. Employing robust encryption to safeguard the transmission of data between IoT devices and 5G infrastructure is essential. Encryption guarantees that data remains inaccessible to unauthorized third parties. Prior to gaining access to the 5G network, IoT devices must undergo authentication. This measure prevents unauthorized devices from connecting and obtaining sensitive data [11].

Segmenting the network enables the division of the network into smaller sections, aiding in the isolation of IoT devices. Additionally, virtual networks can offer further segmentation. Consequently, IoT devices are restricted to communicating solely with other devices within their respective segment, thereby minimizing the risk of potential attacks.

The guidance must recommend that privacy in IoMT with 5G is accomplished through a blend of encryption, authentication, network segmentation, secure design, and adherence to regulatory standards.

3.4 Cloud and Edge Computing

Cloud computing has become an essential technology in the healthcare industry, revolutionizing the way services are created, delivered, and utilized. By utilizing cloud-based platforms, patients and healthcare providers can now consult with each other remotely, enhancing telemedicine and teleconsulting services. Additionally, real-time communication and data sharing capabilities have greatly improved these services. The introduction of cloud storage has allowed for the secure storage and retrieval of medical images, such as X-rays, MRIs, and CT scans. This means that healthcare professionals can access these images from any location, leading to improved diagnostics and treatment plans[23].

Cloud solutions have also played a significant role in public health initiatives by facilitating the collection and analysis of large datasets. Furthermore, patients now have the ability to access their health records and manage their well-being through cloud-based applications, which greatly enhances self-management. Cloud-based hospital management systems have automated administrative tasks, including patient scheduling, billing, and inventory management. This automation has resulted in improved operational efficiency and data accuracy. Moreover, cloud computing aids in the development of personalized treatment plans, helps identify potential drug interactions and enables continuous patient monitoring. It also fosters seamless collaboration among healthcare professionals. Additionally, researchers can utilize cloud resources to conduct secondary analyses of health data, such as population health studies, clinical trials, and epidemiological research.

Cloud services offer the flexibility to adapt to changing computing needs, resulting in efficient use of resources. This pay-as-you-go model allows organizations to only pay for the resources they actually use, minimizing upfront costs.

However, there are challenges and threats associated with relying on external cloud partners, particularly in terms of data protection and privacy. It is crucial to address security and privacy concerns to ensure widespread adoption of cloud computing. In the healthcare industry, the security of sensitive patient data is of utmost importance. If a social engineering attacks, which exploit human psychology to trick individuals into revealing confidential information like

Funded by Horizon Europe Framework Programme of the European Union

passwords or personal data, is successful an attacker can easily gain access to the information stored in the cloud, and potentially alter them [24].

Moreover, ransomware and other malicious software pose a significant risk by encrypting user data and demanding a ransom for decryption. Physical theft of devices or accidental data loss can also compromise patient information. Additionally, insider threats can occur when employees or authorized personnel with malicious intent misuse their access to sensitive data.

Edge computing revolutionizes data processing in healthcare by analyzing and acting upon data right at the point of collection. Instead of relying on centralized cloud systems, edge devices bring data processing closer to the source, enabling real-time insights for clinical and research teams. This proximity to the data allows healthcare professionals to make quicker clinical decisions, minimizing network latency and ensuring timely patient care. AI-powered edge technologies further enhance patient monitoring, reducing risks and improving outcomes. Additionally, edge-enabled devices enhance medical image acquisition, reconstruction, and workflow optimization, ultimately benefiting diagnosis and therapy planning [25].

Edge computing presents a dual impact on patient privacy. Local data processing by edge devices reduces the necessity to send sensitive information to centralized servers, thereby lowering the risk of data breaches during transmission. This approach allows for the removal or anonymization of personal identifiers before data is transmitted, facilitating real-time decision-making without relying on distant servers. This speed can improve patient care while safeguarding privacy.

However, edge devices are vulnerable to physical theft or unauthorized access, necessitating robust security measures. Without proper security, these devices may inadvertently expose sensitive data. Encryption and access controls are critical safeguards. Patients should be informed about data collection, processing, and storage at the edge, with transparent consent mechanisms in place. Striking a balance between privacy rights and efficient healthcare delivery poses a challenge, requiring regulatory evolution to address the implications of edge computing.

To effectively address security concerns, it is crucial to implement various measures. These measures should encompass encrypting data during transmission and storage on edge devices, restricting access to authorized personnel exclusively, regularly evaluating security protocols, and educating patients about edge computing and their rights [11].

Funded by Horizon Europe Framework Programme of the European Union

4 MDCG Improvements

4.1 Introduction

MDCG 2019-16 was developed to aid practitioners in adhering to the Medical Device Regulation and the In-Vitro Device Regulation. This segment provides an analysis of the gaps found in MDCG 2019-16, highlighting key areas for improvement in the regulatory framework for the Internet of Medical Things (IoMT). The analysis was conducted by a group of ongoing projects (2023-2025) that received funding through the Horizon Europe call "Enhancing cybersecurity of connected medical devices": HORIZON-HLTH-2022-IND-13-01. This section provides a summary of the findings and recommendations gathered from CYLCOMED and these projects (SEPTON, NEMECYS, MEDSECURANCE, and ENTRUST), showcasing a significant consensus on various themes such as integrating cybersecurity with patient safety and privacy, maintaining up-to-date guidelines, and providing practical usage instructions for the guidelines. Additionally, the section outlines suggested toolkit solutions to address some of the recommendations.

4.2 Medical Device Coordination Group

The Medical Device Coordination Group (MDCG) is an expert group established under Regulation (EU) 2017/745 on medical devices and Regulation (EU) 2017/746 on in vitro diagnostic medical devices. Its members are experts who represent the competent authorities of the countries of the European Union. The MDCG oversees key issues in the medical device industry, including notified body supervision, standardization, market surveillance, international affairs, new technologies, and clinical research. The MDCG advises the European Commission and helps ensure a harmonized implementation of the Medical Device Regulations throughout the European Union.

The Medical Device Coordination Group (MDCG) addresses key issues in the medical device sector, ranging from Notified Body oversight or standardisation to market surveillance, as well as international matters, new technologies, and clinical investigation.

Its expertise stems from its division into 13 subgroups, each of which provides advice and drafts guidance in their respective areas of expertise.

Members of the subgroups are appointed by the Member States for a three-year term. Stakeholders and European-based associations attend the meetings after responding to dedicated calls for expressions of interest. They have regular meetings with the EU Commission as Chair.

The MDCG has several **working groups**:

Notified Bodies Oversight (NBO): This group shares its experiences and perspectives on notified bodies, including activities outlined in Article 48 of the MDR Regulation (Medical Devices Regulation) and Article 44 of the IVDR Regulation (Regulation on in vitro diagnostic medical devices). It also prepares technical recommendations on issues concerning notified bodies and conformity assessment. The group shares experiences and exchanges views on issues related to notified bodies (including activities laid down in Article 48 MDR/Article 44

Funded by Horizon Europe Framework Programme of the European Union

IVDR) and the application of conformity assessment procedures with the goal of a consistent application of requirements and procedures.

It develops technical recommendations on issues concerning notified bodies and conformity assessment. It advises the Commission on matters pertaining to the coordination group of notified bodies when requested.

The subgroup Notified Bodies joint assessment could be formed to help with the joint assessment process. Topics of interest include administrative practice coordination, cooperation among authorities responsible for notified bodies (designating authorities), and conformity assessment activities.

Standards: This group discusses general standardization issues and coordinates proposals for developing and implementing specific technical documents and standards in a variety of fields. It also addresses the alignment of standards with the MDR and IVDR Regulations. Its topics include the availability of harmonized standards in the context of the preparation of common specifications, collaboration with European (CEN and Cenelec) and international (ISO and IEC) standardization organizations, particularly the International Medical Device Regulators Forum (IMDRF), and standardization requests to European standardization organizations.

Clinical investigation and evaluation (CIE): It develops and promotes consistent interpretation and implementation in clinical evaluation and investigation. It also helps other working groups with clinical investigations and evaluation issues. It seeks common specifications for clinical investigation, evaluation, and post-market clinical follow-up.

Post-market surveillance and vigilance (PMSV) assists the MDCG with post-market surveillance, incident reporting, and vigilance issues in order to ensure the Regulation's effective and harmonized implementation. It creates and revises guidance documents, exchanges information, discusses actual incident cases, and evaluates current reporting practices, including measures to improve all actors' reporting behaviour. Topics of interest include:

- Revision of incident reporting practices.
- Development and updating standardized reporting forms for incidents, field safety corrective actions, field safety notices, periodic summary reports, trend reports, and periodic safety update reports.

Market Surveillance (MS) focuses on competent authorities' enforcement activities and administrative measures related to the surveillance and control of devices placed on the market. It addresses the application and implementation of general safety and performance requirements, the general obligations of economic operators, and conformity assessment for products that do not require the involvement of notified bodies.

Borderline and classification (B&C) assists the MDCG with questions about a product's qualification as a medical device or an accessory for a medical device (including an in vitro diagnostic medical device), as well as the qualification of products with no intended medical use. Provides guidance on the qualification of a product as a medical device. It addresses matters concerning the appropriate classification for a specific medical device, including IVDs. If necessary, this working group collaborates closely with the IVD working group on IVD-specific topics. The "Helsinki Procedure" describes practices for device qualification and classification.

New technologies work group provides advice on the application of new and emerging technologies to medical devices, such as software, apps, and cybersecurity. Works closely with the Borderline and classification working group to address qualification and classification issues related to new technologies. Identifies upcoming issues, such as new and emerging technologies in the field of medical devices, including IVDs. Examines the effectiveness of the

Funded by Horizon Europe Framework Programme of the European Union

current regulatory regime in relation to those issues and technologies. In order to address shortcomings, the group makes recommendations to the MDCG and collaborates with the IMDRF group. Topics of interest include the adequacy of the existing regulatory framework in relation to those issues and technologies, the development of proposals for guidance and common specifications, and electronic medical device user instructions.

EUDAMED work group facilitates the implementation of the EUDAMED database by providing advice and as needed, coordinating the work of other MDCG working groups when input is required for a specific EUDAMED module. Topics of interest include EUDAMED management and maintenance, policy and technical advice, including implementation and application of relevant MDR and IVDR provisions.

Unique Device Identification (UDI) working group makes it easier to implement UDI. The group works closely with the EUDAMED working group on issues concerning the operation of the UDI database. It provides advice on all aspects of device identification and traceability (including the implementation of relevant provisions on implant cards). Topics of concern include all matters concerning device identification and traceability, including the implementation of the relevant MDR provisions on implant cards.

International matters working group prepares a common European viewpoint on IMDRF issues and discusses other international issues concerning medical devices and in-vitro diagnostic medical devices, with a focus on monitoring international regulatory trends. Topics include the development of common views and positions of EU Member States on harmonization issues discussed within the IMDRF.

In vitro diagnostic medical devices (IVD) working group develops and promotes consistent interpretation and implementation of IVD-specific issues. It supports other working groups on IVD-related topics. Furthermore, it addresses clinical issues specific to IVDs, as needed, in collaboration with the CIE WG. This group is interested in coordinating activities with other MDCG working groups as appropriate and, whenever necessary, providing them with input on IVD-specific aspects of their work (such as in the field of classification, performance studies, performance evaluation, and post-market performance follow-up of IVDs)

Nomenclature working group provides assistance with all implementation issues concerning medical device nomenclature in order to support the operation of the future European database on medical devices (EUDAMED). This group is interested in updating and maintaining the EU nomenclature, as well as using nomenclature in contexts other than UDI registration, such as market surveillance.

"Annex XVI" products working group creates common specifications for the groups of products without a medical purpose listed in Regulation (EU) 2017/745 Annex XVI. The application and implementation of the general safety and performance requirements specified in Annex I of the MDR for Annex XVI devices; general obligations of economic operators in relation to Annex XVI devices; product qualification and technical aspects.

4.3 MDCG 2019-16

The guidance document MDCG 2019-16 offers crucial advice to medical device manufacturers regarding cybersecurity. Its purpose is to assist manufacturers in meeting the necessary requirements outlined in Annex I of the Medical Devices Regulations related to cybersecurity. The document delves into topics like IT security, safety, risk management, and post-market

Funded by Horizon Europe Framework Programme of the European Union

surveillance. Furthermore, it discusses pertinent EU and international laws and guidelines concerning cybersecurity for medical devices.

The MDCG guidance on cybersecurity for medical devices has been available for some time now, allowing ample opportunity for individuals to become familiar with its contents. The document offers valuable insights into the expectations of the EU regulator regarding cybersecurity for medical devices governed by the MDR and IVDR. This includes both standalone software and devices that utilize software. One of the key benefits of the guidance is its illustration of the interconnectedness of various components and requirements outlined in the MDR and IVDR, particularly in the realms of PMS and risk management. The EU anticipates significant enhancements in these areas from all stakeholders. The guidance draws heavily from the work of the IMDRF on cybersecurity for medical devices, specifically referencing the informative "IMDRF's Principles and Practices for Medical Device Cybersecurity[2]" document.

The guidance comprises of

- An introduction;
- Basic cybersecurity concepts;
- Secure design and manufacture;
- Documentation and instructions for use;
- PMS and vigilance;
- Links to other EU and International legislation and guidance; and
- Annexes with examples and reference material.

The MDR and IVDR include new (cyber)security GSPRs in GSPR 17 and 16, respectively, but both require a much broader view of cybersecurity.

The FDA has also released multiple guidelines concerning cybersecurity for medical devices, encompassing premarket and post-market factors. The MDCG 2019-16 guidance supplements the FDA guidelines by addressing both premarket and post-market cybersecurity aspects for medical devices. Manufacturers targeting the international market should adhere to both sets of guidelines to guarantee compliance and the safety of device design.

4.4 Improvements on the guidance

This section presents multiple areas of enhancement for future iterations of the guide. It also encompasses the recommendations put forth in collaboration with other projects funded under the same Horizon Europe topic, which have been documented in a collective scientific article.

Cybersecurity concerns vary depending on the stakeholder's role, and addressing perception misalignment can be quite challenging. One key takeaway from the CYLCOMED project is the significant difficulty in establishing a common language and mutual understanding between clinical practitioners and technology solution providers. This disparity in perception results in added complexity, especially when implementing new technology solutions within an existing framework. For instance, the introduction of a new medical device like telemonitoring requires consideration of a wide range of issues (e.g. ethical concerns, infrastructure requirements) that may not be readily apparent to technology providers alone. A comprehensive chart to navigate this complexity would greatly benefit all parties involved.

The fast-paced advancement of technology requires regular updates and modifications to guidance to maintain its relevance. It is advised to establish and implement processes

[2] *https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity*

Funded by Horizon Europe Framework Programme of the European Union

periodically to ensure that the MDCG guidelines are aligned with the changing standards and best practices for the implementation of the MDR / IVDR, as well as to adapt to the evolving regulations. Additionally, it is recommended to periodically release new versions of the MDCG guidelines based on state-of-the-art surveys to ensure that the guidance remains current and provides valuable insights on meeting security standards and continuous monitoring of cybersecurity protocols and controls.

It is common in risk management standards and frameworks to find measures that improve cybersecurity while also protecting patient data privacy. The guide itself reminds that violations in medical device safety can endanger patients as well as property and the environment. However, the relationship between the two concepts is not fully developed.

Many incident studies show that the key to integrating cybersecurity and patient safety is found in physiological data captured by medical devices [30][16]. The set of risks is related to the cybersecurity triad of confidentiality, integrity, and availability. These concepts serve as a guide for identifying risks and assessing their impact on patient safety. For example, if the availability or integrity of data from a patient-connected sensor is compromised, it can result in a delayed or inaccurate diagnosis, potentially causing harm to the patient or affecting the quality of treatment.

The lack of direction in the MDCG regarding security-related controls for different device classes poses a challenge in determining the minimum-security control criteria for various medical devices. These controls usually pertain to risk assessment and are crucial in mitigating identified risks. Therefore, it is advisable that MDCG references relevant cybersecurity risk standards like ISO 27001, ISO 27002 or ISO 27005.

The MDCG guidelines should include recommendations on resolving conflicts, particularly those arising between privacy requirements, such as GDPR compliance, and medical necessities. While it is important to safeguard personal data, it should not impede the provision of medical care. However, it is equally crucial to mitigate privacy risks associated with medical devices and establish guidelines that address these concerns. Providing guidance on evaluating the trade-offs between these conflicts will empower decision-makers to establish a well-defined policy that strikes an acceptable balance between patient healthcare and privacy.

The MDCG guidelines must align the guidance with the various stages of the entire MD lifecycle - starting from design and production, through deployment in various scenarios, the operation of devices in those scenarios, and finally their decommissioning or disposal. Due to the fact that one device can be utilized in multiple contexts and the same scenario can have different environments for devices, there exists a many-to-many relationship between these phases, making the lifecycle intricate. It is crucial that each device operation undergoes a cybersecurity assessment, with a clearly identified responsible party who must evaluate and ensure that risks are at an acceptable level. Additionally, different stages of a medical device's lifecycle may present varying priorities for cybersecurity or patient safety concerns, hence the lifecycle stage should be factored in when determining the significance of consequences and harms.

MDCG guidelines also should advocate a system-wide approach when assessing harms, threats, vulnerabilities, and controls, related to valid intended usage scenarios. The manufacturer already needs to describe the intended use, which will very likely involve a device’s operation in an environment connected with other devices, networks, people, and places and will thus be exposed to threats resulting from connection with these other entities and actors. Further, there are likely to be many situations where the environment has multiple domains of control. For example, it can be controlled by different legal entities when a medical device in a patient’s house connects to a 3rd party cloud service that is also accessed by a hospital. We can see three legal entities here. Therefore, there are multiple sources of threats and risks. It is unlikely that one entity will be able to exercise total control. Consequently, cooperation between entities will be required to address the threats and risks, and guidance

Funded by Horizon Europe Framework Programme of the European Union

on the assessment and control of threats and risks in such multi-party situations would greatly assist practitioners.

Certainly, it would be highly beneficial if the MDCG guidelines provided instructions on how to effectively utilize its guidelines. This would offer valuable direction on how various stakeholders should implement the guidelines, particularly by offering entry points and a sequence of operations that index the guidance from the MDCG. For medical device software with higher risk levels, it is essential to have detailed guidance on validation and verification processes in order to ensure both safety and performance. It is advisable for the MDCG guidelines to be structured as "recipes" that outline different compliance scenarios, processes, and objectives for specific user types. For instance, a device manufacturer seeking compliance with the MDR or a system integrator aiming to ensure their usage scenario is compliant. These "recipes" would organize the MDCG guidance into easy-to-follow, step-by-step guides. Additionally, the inclusion of practical case studies and examples would greatly facilitate the application of MDCG, assisting manufacturers in achieving regulatory compliance. Furthermore, it would be beneficial to develop a comprehensive training and education resource based on the MDCG guidance. This resource would serve as a knowledge base, providing manufacturers with cohesive and coherent support in meeting regulatory demands.

The implementation of the MDR and IVDR has caused uncertainty in the industry, impacting market access and compliance strategies. Ongoing monitoring of device performance is now required, which requires additional resources. The new regulations have also introduced complexities with the roles of economic operators and clinical investigation prerequisites. The device classification system under the new regulations may also pose challenges, requiring precise interpretation and application of guidance. The generic guidelines provided by the MDCG often lack specificity for advanced technologies, leading to a reliance on guidance documents rather than legislative texts, which introduces subjectivity into the regulatory assessment process. It is crucial to continuously refine guidance to ensure compliance in this ever-changing regulatory environment. With the increasing use of Artificial Intelligence and Machine Learning in medical devices, tailored guidance that addresses the unique verification, validation, and transparency of these technologies is necessary. This guidance should be integrated with continuous monitoring protocols.

The assessment of incidents during post-market surveillance is a complex process that necessitates a careful evaluation of their severity and potential impact. Manufacturers make a clear distinction between serious and non-serious incidents, a classification that is essential for determining the urgency and extent of subsequent actions. According to MDCG 2019-16, the evaluation of whether to report serious or non-serious incidents and the subsequent implementation of Field Safety Corrective Actions (FSCA) are fundamental components of post-market surveillance for medical devices. FSCA involves corrective measures implemented by manufacturers to prevent or mitigate serious incidents. This comprehensive assessment process aligns with regulatory standards and guarantees that the appropriate measures are taken in response to identified incidents to uphold the safety and efficacy of medical devices in the market. Nevertheless, there are deficiencies in establishing clear and enforceable deadlines for reporting these incidents. Delays in reporting could impede the ability to promptly implement corrective actions. MDCG 2019-16 urges manufacturers to adopt a proactive approach by investing in research and development endeavors focused on integrating advanced encryption mechanisms, improved access controls, and cutting-edge threat intelligence. While emphasis is placed on integrating advanced encryption mechanisms, there may be gaps in the guidelines concerning the adaptability of post-market surveillance practices to rapidly evolving technologies. Additionally, potential deficiencies may exist in terms of guidelines for communication and information exchange among manufacturers, competent authorities, and other stakeholders to collectively address emerging cybersecurity threats. Furthermore, given the global nature of the medical device market, harmonizing post-market surveillance requirements worldwide could enhance uniformity and efficacy in

Funded by Horizon Europe Framework Programme of the European Union

addressing cybersecurity issues. Therefore, enhancing the security capabilities in post-market surveillance is crucial for further improvement.

Understanding the fundamental reasons behind cybersecurity incidents is crucial for implementing effective measures to mitigate risks and prevent future occurrences. After a product or system is launched, it is essential to closely examine the factors that contributed to these incidents, taking into account both technical and contextual aspects. The objective of root cause analysis is to identify the underlying issues that resulted in vulnerabilities and incidents, which in turn serves as a foundation for implementing targeted corrective actions. The taxonomy of root causes encompasses various dimensions, including software vulnerabilities, unauthorized access, and systemic weaknesses. Manufacturers can utilize standardized frameworks and the codes provided by the International Medical Device Regulators Forum (IMDRF)[3] to systematically categorize and analyze the root causes of incidents. It is advisable for guidelines to outline a standardized approach or methodology for conducting root cause analyses. The iterative nature of this analysis plays a significant role in continuously improving post-market cybersecurity strategies and ensuring the ongoing safety and effectiveness of medical devices.

Vulnerability management plays a crucial role in ensuring cybersecurity for medical devices. It involves identifying and assessing vulnerabilities that may impact a medical device throughout its operational lifespan. By evaluating these vulnerabilities, organizations can determine the most suitable actions to address and mitigate them, taking into account their severity and prevalence. Despite its significance, vulnerability management for medical devices has received limited attention, as discussed in Section 2.4 of MDCG 2019-16.

The MDCG guidelines suggest that it is prudent to assume that any vulnerability in a software implementation could potentially be discovered and exploited in the future. Therefore, it is important to consider these vulnerabilities as potential facilitators for foreseeable misuse. However, this recommendation may be seen as overly restrictive when it comes to other types of devices, as end users often agree with manufacturers that certain vulnerabilities are not worth patching due to low CVSS or EPSS scores.[4] Nevertheless, it is likely that most users of medical devices, such as hospitals, will agree that all verified exploitable vulnerabilities in the device should be addressed through patching.

In relation to the monitoring of vulnerabilities in the field, the guidelines provided by the MDCG emphasize the responsibility of medical device manufacturers to ensure that their devices are designed and produced in a manner that effectively eliminates or reduces the risks associated with reasonably foreseeable environmental conditions. It is worth mentioning that, in the majority of instances, it may not be feasible for the manufacturer to carry out this monitoring. However, it is encouraging to note that organizations utilizing these devices, such as hospitals, have the potential to undertake this monitoring, and it is hoped that this practice is already widespread.

The guidelines emphasize the option of delivering patches to perform a device update, separate from any field safety corrective action, in order to maintain the device's security. However, it is contended that numerous device manufacturers do not frequently provide software updates for their devices, leaving users susceptible to attacks that exploit vulnerabilities before they can be patched in the next update. Consequently, there is a need

---

[3] *https://www.imdrf.org/documents*

[4] *Vulnerability assessment systems like CVSS, CVE, CWE, and EPSS are tools utilized to evaluate and measure the seriousness and possible consequences of security flaws in software, hardware, or systems. These assessment systems offer a means to rank and deal with vulnerabilities according to their perceived risk and importance. They are widely employed by companies, security experts, and software developers to classify vulnerabilities, enabling them to effectively allocate resources for remediation endeavors.*

Funded by Horizon Europe Framework Programme of the European Union

to implement security measures that can effectively and promptly address such critical vulnerabilities. These measures may involve utilizing remote attestation enablers offered by an AI-based Misbehaviour Detection module, as well as identifying attacks through simulation in the Digital Twin of the device.

The guidelines from the MDCG suggest that, in the process of risk management, the manufacturer must anticipate or assess the potential exploitation of vulnerabilities that could arise from a misuse that is reasonably foreseeable. However, this may vary depending on the specific circumstances. For instance, the utilization of an insecure memory stick to input data into a medical IT system might be considered a reasonably foreseeable misuse but could pose significant security risks if it inadvertently introduces malware into the system. Consequently, although it may not be feasible to establish a clear-cut distinction, it is essential to implement security measures that can function as continuous security monitors to ensure operational assurance in medical devices.

In section 1.4 of the guidance**,** Figure 2 does not include Annex II, III, and XIV, even though they are mentioned in the text that outlines cybersecurity requirements. In order to provide a complete overview of the cybersecurity requirements in the MDR and IVDR, it is crucial to include these references in the figure.

The current definition of IT security in section 2.1 of the document is insufficient as it does not cover all the necessary elements for protecting assets from potential harm. It should encompass protection against unauthorized use or provision of services, as well as ensuring accountability and non-repudiation. By incorporating these aspects, the definition would become more comprehensive and align with the ENISA definition of cybersecurity.

The absence of a mention of the "privacy by design" principle in Section 3.1 of the document is a significant oversight, especially when it comes to ensuring the cybersecurity of medical devices that handle personal data in accordance with the GDPR. It is highly advised to integrate the privacy by design principle into this section, emphasizing its importance in the development and manufacturing of medical devices. This involves minimizing the collection and processing of personal data, carrying out data protection impact assessments, employing pseudonymization or encryption techniques, and other relevant measures.

The MDCG guidelines briefly mention the Cyber Security Act (CSA), which introduces an EU-wide cybersecurity certification framework. However, there is no established connection between the MDR and CSA, whether terminological or substantial. Establishing such a connection would be highly beneficial, especially in clarifying how MDR and CSA interact in terms of cybersecurity certification [34] . While many scholars highlight the importance of ethical considerations in cybersecurity practices, the MDCG guidelines do not address ethics. Therefore, incorporating ethical principles and values would improve understanding of the risks involved and promote the implementation of ethical standards across the entire life cycle of medical devices.

Medical device stakeholders navigate a multifaceted legal landscape, further complicated by recent legislative proposals like the AI Act [35] and the Cyber Resilience Act [36]. While clear guidance is essential for ensuring compliance with the numerous legal obligations outlined in different regulations, relying solely on MDCG guidelines as a solution for unraveling the complexities of medical device cybersecurity law would be impractical. However, stakeholders would greatly benefit from additional direction provided in section 6 of the guidelines.

The endorsement of the MDCG as the first and only guidance on medical device cybersecurity marked a significant milestone in the implementation of MDR cybersecurity requirements. However, it is crucial to emphasize that the landscape of medical device cybersecurity is constantly evolving since the endorsement of the MDCG Guidance in 2019. Furthermore, the regulatory framework governing medical device cybersecurity is rapidly evolving. Notably, the NIS Directive mentioned in the Guidance has been replaced by the NIS2 Directive, which

Funded by Horizon Europe Framework Programme of the European Union

introduces new elements and expands its application to encompass medical device manufacturers. Acknowledging this change in the Guidance would ensure that readers understand its relevance and up-to-date nature.

The MDCG Guidance does not make any mention of ethics. Emerging technologies are a prime illustration of how legislation falls short and how ethics are pivotal, leading the path to regulatory standards. Artificial intelligence stands out as a clear-cut case where ethical considerations influence legal frameworks and serve as a stopgap measure in the absence of enforceable regulations. Hence, shedding more light on ethical standards and values would enhance comprehension of the potential risks involved and aid in embedding ethical principles across the complete lifespan of medical devices.

Furthermore, the MDCG Guidance fails to address the potential impact or conflicts that may arise among different stakeholders due to the diverse laws governing the medical device ecosystem. Consequently, additional guidance on this matter would greatly assist in analyzing the pertinent aspects of other horizontal legislation and ultimately contribute to establishing a more cohesive regulatory framework for cybersecurity. By taking into account the interrelated responsibilities and legal ramifications across various regulatory domains, this guidance can offer stakeholders a more comprehensive understanding of how to navigate the intricate cybersecurity requirements for medical devices.

The Guidance emphasizes that healthcare and medical professionals have the responsibility of utilizing medical devices for diagnostic and monitoring purposes. These users are able to access, review, and exchange data with the devices, and are also accountable for educating patients and setting up software and device parameters. Additionally, the guidance advises patients and consumers to practice cyber-smart behavior, including being mindful of privacy, recognizing suspicious messages, and browsing responsibly. Ultimately, the MDCG guidance highlights that all stakeholders, including manufacturers, suppliers, healthcare providers, patients, integrators, operators, and regulators, must collaborate to ensure a secure environment for the safety of patients. Despite the focus on healthcare professionals and patients, it is important to note that humans are often the weakest link in the cybersecurity chain.

4.5 Terminology Issues

It is worth noting that both the MDR and IVDR do not specifically mention cybersecurity. In order to assist device manufacturers in meeting the essential requirements of Annex I to the MDR/IVDR regarding cybersecurity, the European Commission's Medical Device Coordination Group endorsed the Guidance on Cybersecurity for Medical Devices (MDCG 2019-16 Rev.1) in December 2019.

However, similar to the MDR/IVDR, the MDCG Guidance does not provide explicit definitions or references to terms like "cybersecurity," "security-by-design," and "security-by-default." Instead, the guidance focuses on provisions related to cybersecurity for medical devices and highlights the conceptual connections between safety and security. Nevertheless, the absence of clear and defined terms may pose challenges for stakeholders who aim to effectively implement practical cybersecurity measures. Having precise and concrete definitions would improve comprehension and facilitate the practical application of cybersecurity principles in the realm of medical devices. IT security, information security, and operational security are all crucial aspects of protecting computer systems and networks. IT security focuses on defending against threats and attacks, while information security is concerned with preserving the confidentiality, integrity, and availability of data. On the other hand, operational security involves managing risks and safeguarding operational assets.

Funded by Horizon Europe Framework Programme of the European Union

Similarly, when it comes to devices, security, effectiveness, and intended use play vital roles. Security ensures that the device does not pose any harm to the patient or user. Effectiveness ensures that the device performs its intended function successfully. Lastly, intended use describes how the device is expected to be utilized in a specific environment. By considering these factors, we can ensure the safety, functionality, and appropriate usage of devices.

The operating environment of the device includes various conditions, such as the location, network, and connected systems, in which it will be used. Considering these factors is essential for optimizing the device's performance and safety.

The joint responsibility concept involves both the integrator, who assembles or combines components to create a system, and the operator, who utilizes the device in the operating environment. This shared responsibility ensures that the device functions properly and safely throughout its lifecycle.

Section 6 of MDCG 2019-16 offers insight into how legislative aspects intersect with various legal frameworks that could run concurrently with MDR, notably GDPR [31] and NIS Directive [32]. It provides a brief overview of the general objectives of these legal frameworks in a descriptive fashion. Nevertheless, given the widely recognized challenges of overlapping and conflicting issues during practical application, there is a clear need to address these issues more comprehensively. This includes clarifying the notions of "joint responsibility" [33] and "improving of terminological consistency," among other key areas that would benefit all relevant stakeholders.

4.6 Toolkits as a Suggestion

To enhance security capabilities in accordance with MDCG 2019-16, the CYLCOMED project has suggested that the MDCG assess tools and put forward a toolkit solution. This toolkit could consist of various tools for threat intelligence gathering, penetration testing frameworks, continuous monitoring systems, risk assessment, encryption key management solutions, secure coding policies, and automatic security updates to fortify devices against emerging threats. The collaboration platforms integrated within the toolkit can facilitate knowledge sharing, aligning with the collaborative spirit highlighted in the guidelines. Moreover, visualization tools like interactive dashboards can aid in comprehending the complexities of incidents. As part of the research initiative, CYLCOMED is actively involved in developing a cutting-edge toolkit (outlined in D5.1) with the goal of bolstering the cybersecurity of interconnected medical devices and systems. This toolkit will undergo validation through two pilot projects as detailed in D6.1 and D3.3.

CYLCOMED offers a risk assessment framework that includes risk benefit analysis schemes and a toolbox designed to tackle cybersecurity risks and gaps in connected medical devices. It also involves evaluating and enhancing baseline standards, best practices, and guidelines to address challenges related to CMDs, such as software, ensuring their compatibility with new technologies.

Funded by Horizon Europe Framework Programme of the European Union

Conclusion

The deliverable provided an initial assessment of MDCG 2019-16, highlighting areas for enhancement and suggesting a series of recommendations to strengthen the European CMD regulatory framework. The legal deficiencies identified in the previous section are further addressed and expanded upon in D2.2.

The significance of cybersecurity in the healthcare field cannot be emphasized enough. It is of utmost importance due to the fact that healthcare organizations possess extensive amounts of sensitive patient data, encompassing personal and medical information. Implementing cybersecurity measures is crucial in order to safeguard this data from unauthorized access and breaches. Cyberattacks have the potential to directly impact patient safety. For instance, if a hacker gains control over medical devices or manipulates medical records, it could result in incorrect treatments or diagnoses. The average cost of a data breach within the healthcare industry is considerably higher compared to other sectors. A robust cybersecurity framework plays a vital role in upholding the trust of patients and the reputation of healthcare institutions. Patients must have confidence in the security of their data. A cyberattack can disrupt services, leading to care delays and potentially harming patients. Lastly, cybersecurity serves to protect the intellectual property of medical research from theft or sabotage.

The MDCG Guidance has been analyzed through the utilization of a qualitative approach relying on secondary resources and industry standards. The evaluation of the guidance and suggested enhancements will persist until the completion of the CYLCOMED project and will culminate in the production of deliverable D3.4. This deliverable will encompass a more extensive array of recommendations. This report will encompass comprehensive recommendations from both technical and organizational perspectives.

Funded by Horizon Europe Framework Programme of the European Union

References and Bibliography

[1] Christoph Thuemmler and Chunxue Bai. 2018. Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare (1st. ed.). Springer Publishing Company, Incorporated

[2] Rekha, G., Yashaswini, J. (2022). Industry 4.0: A Revolution in Healthcare Sector via Cloud, Fog Technologies. In: Tyagi, A.K., Abraham, A., Kaklauskas, A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. https://doi.org/10.1007/978-981-16-6542-4_16

[3] Mishra, A., Kumari, N., Bisoy, S.K., Sahoo, S. (2022). Integration of Medical Internet of Things with Big Data in Healthcare Industry. In: Mishra, S., González-Briones, A., Bhoi, A.K., Mallick, P.K., Corchado, J.M. (eds) Connected e-Health. Studies in Computational Intelligence, vol 1021. Springer, Cham. https://doi.org/10.1007/978-3-030-97929-4_2

[4] Khan, A.A., Siddiqui, S., Dey, I. (2023). Applications of 4.0 Technologies in Healthcare. In: Battineni, G., Mittal, M., Chintalapudi, N. (eds) Computational Methods in Psychiatry. Springer, Singapore. https://doi.org/10.1007/978-981-99-6637-0_15

[5] Hu, Yan & Bai, Guohua. (2014). A Systematic Literature Review of Cloud Computing in Ehealth. Health Informatics - An International Journal. 3. 10.5121/hiij.2014.3402.

[6] Shreshth Tuli, Nipam Basumatary, Sukhpal Singh Gill, Mohsen Kahani, Rajesh Chand Arya, Gurpreet Singh Wander, Rajkumar Buyya,

[7] HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments, Future Generation Computer Systems, Vol 104, 2020, pages 187-200, doi.org/10.1016/j.future.2019.10.043.

[8] Constant, N., Borthakur, D., Abtahi, M., Dubey, H., & Mankodiya, K. (2017). Fog-Assisted wIoT: A Smart Fog Gateway for End-to-End Analytics in Wearable Internet of Things, doi.org/10.48550/arXiv.1701.08680.

[9] Alonso, S.G., de la Torre Díez, I. & Zapiraín, B.G. Predictive, Personalized, Preventive and Participatory (4P) Medicine Applied to Telemedicine and eHealth in the Literature. J Med Syst 43, 140 (2019). https://doi.org/10.1007/s10916-019-1279-4

[10] Ayala, L. (2016). Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention. Springer. https://doi.org/10.1007/978-1-4842-2155-6

[11] Kelly, B., Quinn, C., Lawlor, A., Killeen, R., Burrell, J. (2022). Cybersecurity in Healthcare. In: Sakly, H., Yeom, K., Halabi, S., Said, M., Seekins, J., Tagina, M. (eds) Trends of Artificial Intelligence and Big Data for E-Health. Integrated Science, vol 9. Springer, Cham. https://doi.org/10.1007/978-3-031-11199-0_11

[12] S. A. E. Hoffman, "Cybersecurity threats in healthcare organizations: Exposing vulnerabilities in the healthcare information infrastructure", Inf. Secur. Emerg. Voices, vol. 24, no. 1, pp. 1-20, 2020.

[13] Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. J Med Internet Res. 2018 May 28;20(5):e10059. doi: 10.2196/10059. PMID: 29807882; PMCID: PMC5996174

[14] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D. et al. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak 20, 146 (2020). https://doi.org/10.1186/s12911-020-01161-7

Funded by Horizon Europe Framework Programme of the European Union

[15] Haider, N., Gates, C., Sengupta, V., Qian, S. (2019). Cybersecurity of Medical Devices: Past, Present, and Future. In: Deer, T., Pope, J., Lamer, T., Provenzano, D. (eds) Deer's Treatment of Pain. Springer, Cham. https://doi.org/10.1007/978-3-030-12281-2_100

[16] Biasin, E., Kamenjašević, E. Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. Int. Cybersecur. Law Rev. 3, 163–180 (2022). https://doi.org/10.1365/s43439-022-00054-x

[17] Aldossri, R., Hafizur Rahman, M.M. (2023). A Systematic Literature Review on Cybersecurity Issues in Healthcare. In: Smys, S., Tavares, J.M.R.S., Shi, F. (eds) Computational Vision and Bio-Inspired Computing. Advances in Intelligent Systems and Computing, vol 1439. Springer, Singapore. https://doi.org/10.1007/978-981-19-9819-5_58

[18] Jelić, L. (2024). Cybersecurity, Data Protection, and Artificial Intelligence in Medical Devices. In: Badnjević, A., Cifrek, M., Magjarević, R., Džemić, Z. (eds) Inspection of Medical Devices . Series in Biomedical Engineering. Springer, Cham. https://doi.org/10.1007/978-3-031-43444-0_17

[19] Bhushan, Bharat, Avinash Kumar, Ambuj Kumar Agarwal, Amit Kumar, Pronaya Bhattacharya, and Arun Kumar. 2023. "Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends" Sustainability 15, no. 7: 6177. https://doi.org/10.3390/su15076177

[20] Hireche, Rachida, Houssem Mansouri, and Al-Sakib Khan Pathan. 2022. "Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis" Journal of Cybersecurity and Privacy 2, no. 3: 640-661. https://doi.org/10.3390/jcp2030033

[21] Hameed SS, Hassan WH, Abdul Latiff L, Ghabban F. 2021. A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. PeerJ Computer Science 7:e414 https://doi.org/10.7717/peerj-cs.414

[22] Dananjayan, S., Raj, G.M. 5G in healthcare: how fast will be the transformation?. Ir J Med Sci 190, 497–501 (2021). https://doi.org/10.1007/s11845-020-02329-w

[23] Rai, V. et al. (2022). Cloud Computing in Healthcare Industries: Opportunities and Challenges. In: Singh, P.K., Singh, Y., Chhabra, J.K., Illés, Z., Verma, C. (eds) Recent Innovations in Computing. Lecture Notes in Electrical Engineering, vol 855. Springer, Singapore. https://doi.org/10.1007/978-981-16-8892-8_53

[24] Mulimani, M.S., Rachh, R.R. (2021). Edge Computing in Healthcare Systems. In: Suresh, A., Paiva, S. (eds) Deep Learning and Edge Computing Solutions for High Performance Computing. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-60265-9_5

[25] Aldossri, R., Hafizur Rahman, M.M. (2023). A Systematic Literature Review on Cybersecurity Issues in Healthcare. In: Smys, S., Tavares, J.M.R.S., Shi, F. (eds) Computational Vision and Bio-Inspired Computing. Advances in Intelligent Systems and Computing, vol 1439. Springer, Singapore. https://doi.org/10.1007/978-981-19-9819-5_58

[26] S. Barbaria, M. C. Mont, E. Ghadafi, H. Mahjoubi Machraoui and H. B. Rahmouni, "Leveraging Patient Information Sharing Using Blockchain-Based Distributed Networks," in IEEE Access, vol. 10, pp. 106334-106351, 2022, doi: 10.1109/ACCESS.2022.3206046.

[27] A. A. Monrat, O. Schelén and K. Andersson, "A survey of blockchain from the perspectives of applications challenges and opportunities", IEEE Access, vol. 7, pp. 117134-117151, 2019.

Funded by Horizon Europe Framework Programme of the European Union

[28] N. Fatima et al., "Security and privacy issues of blockchain technology in health care—A review", ICT Anal. Appl., pp. 193-201, 2022.

[29] L. Campanile et al., "Risk analysis of a GDPR-compliant deletion technique for consortium blockchains based on pseudonymization", Proc. Int. Conf. Comput. Sci. Appl, pp. 3-14, 2021.

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

[31] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eurlex. europa.eu/eli/reg/2016/679/oj

[32] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555

[33] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at: Directive - 2016/1148 - EN - EUR-Lex (europa.eu)

[34] Biasin, Elisabetta and Kamenjasevic, Erik, Cybersecurity of Medical Devices: Regulatory Challenges in the EU (September 30, 2020). The Future of Medical Device Regulation: Innovation and Protection, Cambridge University Press, 2020, Available at SSRN: https://ssrn.com/abstract=3855491

[35] European Union. 2019. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). EUR-Lex - 32019R0881 - EN - EUR-Lex (europa.eu)

[36] Milojevic, Dusko. “Is it time to update the Medical Device Coordination Group’s Guidance on Cybersecurity for Medical Devices?” Blog Post, 14 NOVEMBER 2023. Available at: Is it time to update the Medical Device Coordination Group's Guidance on Cybersecurity for Medical Devices? - CiTiP blog (kuleuven.be)

MDCG 2019-16 - Guidance on Cybersecurity for medical devices. Document date: 06/01/2020 - Created by GROW.R.2.DIR - Publication date: n/a - Last update: 22/06/2020. https://ec.europa.eu/docsroom/documents/41863

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.) https://eur-lex.europa.eu/eli/reg/2017/746/oj

ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems: Requirements. https://www.iso.org/standard/iso-iec-27001-2022-v1

Funded by Horizon Europe Framework Programme of the European Union

ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks. https://www.iso.org/standard/80585.html

NIST Risk Management Framework (RMF) https://csrc.nist.gov/projects/risk-management/about-rmf

NIST Cybersecurity Framework https://www.nist.gov/cyberframework

NIST Privacy Framework https://www.nist.gov/privacy-framework

ISO/IEC 27701:2019. Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines. https://www.iso.org/standard/71670.html

ISO 14971:2019. Medical devices: Application of risk management to medical devices. https://www.iso.org/standard/72704.html

ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection: Information security controls. https://www.iso.org/standard/75652.html

R. Shirey, Network Working Group, Request for Comments: 4949. Internet Security Glossary, Version 2. August 2007

Ben-Menahem, S. M., Nistor-Gallo, R., Macia, G., von Krogh, G., & Goldhahn, J. (2020). How the new European regulation on medical devices will affect innovation. Nature biomedical engineering, 4(6), 585-590.

Sigmund, W., Pracyk, J., Karchmer, T., Dias, J., Hoerauf, K., Beer, I., ... & Silverman, R. (2024). Medical Affairs in MedTech. In Medical Affairs (pp. 231-242). CRC Press..

Jelić, L. (2023). Cybersecurity, Data Protection, and Artificial Intelligence in Medical Devices. In Inspection of Medical Devices: For Regulatory Purposes (pp. 417-445). Cham: Springer Nature Switzerland.

Li J, Carayon P. Health Care 4.0: A Vision for Smart and Connected Health Care. IISE Trans Healthc Syst Eng. 2021;11(3):171-180. doi: 10.1080/24725579.2021.1884627. Epub 2021 Feb 15. PMID: 34497970; PMCID: PMC8423174.

Funded by Horizon Europe Framework Programme of the European Union