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

D3.4 Guidance improvement - Final

Revision: v.1.0

Work package	WP 3
Task	Task 3.1
Due date	30/11/2025
Submission date	
Deliverable lead	FHUNJ
Version	1.0
Authors	Andrés Castillo (FUHNJ), Santiago Bollain (FUHNJ)
Reviewers	

Abstract	This report, which is the outcome of Task 3.1 in Work Package 3, analyses the risks 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	15.08.25	First draft	Andrés Castillo Santiago Bollaín Dusko Milosevic Ricardo Ruiz Ginevra Campia Alberto Tozzi
V0.2	14.10.25	Ready for first review	Andrés Castillo Santiago Bollaín
V0.3		First Revision	João Rodrigues
V0.4		Comments addressed	Andrés Castillo Santiago Bollaín
V1.0		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 deliverable's goal is to identify gaps and possible areas for improvement in the state of the art regarding the cybersecurity of connected medical devices in different environments. It is expected that the authors of the next edition of the MDCG 2019-16 guide will use these findings to inform their recommendations for improvement.

The analysis was based on two previously published scientific papers [1][2] that summarized the experience of the CYLCOMED project's partners and stakeholders as well as the outcomes of the cluster's other projects. Analysis was also done on scientific literature as well as device manuals, rules, and standards. The project's expert board members, besides the managers and technicians at the participating hospitals, were asked for their insights.

The project's concept architecture served as the framework for the guide's recommendations and language. In addition to following the procedures from the previous D3.3, this deliverable likewise considers the final deliverables from the rest of the project work packages, such as D7.4, D6.3, and D2.2.

Funded by Horizon Europe Framework Programme of the European Union

Table of contents

Funded by Horizon Europe Framework Programme of the European Union

Funded by Horizon Europe Framework Programme of the European Union

Abbreviations

AI	Artificial Intelligence
CIS	Clinical Information System
CMD	Connected Medical Device
CSA	Cyber Security Alert
DPWS	Device Profile for Web Services
ECG	Electrocardiograph
EHR	Electronic Health Record
FSCA	Field Safety Corrective actions
GDPR	General Data Protection Regulation
GSPR	General Safety and Performance Requirements
IEC	International Electrotechnical Commission
IMDRF	International Medical Device Regulators Forum
IEEE	Institute of Electrical and Electronics Engineers
IoMT	Internet of Medical Things
ISMS	Information security management system
ISO	International Organisation for Standardisation
IVDR	In Vitro Diagnostic Medical Devices Regulation
MDCG	Medical Device Coordination Group
MDR	Medical Devices Regulation; EU 2017/745
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
PDMS	Patient Data Management System

Funded by Horizon Europe Framework Programme of the European Union

PKP	Participant Key Purpose
PSR	Periodic Summary Reports
PSUR	Periodic Safety Update Report
SIEM	Security Information and Event Management

Funded by Horizon Europe Framework Programme of the European Union

1 Introduction

The World Economic Forum's **Global Risks Report** 2025 provides a thorough analysis of the cybersecurity environment, especially regarding sensitive data in the healthcare industry. The paper emphasises the increasing risks that clinical data confront in the face of intricate technological and geopolitical issues in an era characterised by rapid digital transformation.

According to the Global Risks Report 2025, cybersecurity plays a crucial role in determining the resilience of healthcare systems and the safeguarding of clinical data. To reduce the risk of sensitive data breaches and guarantee continuous healthcare delivery in an increasingly digital world, proactive prevention, efficient regulation, and specialised education are crucial. This is highlighted by the convergence of technological innovation, geopolitical uncertainty, and human factors.

The acknowledgement that healthcare systems are becoming more reliant on complex networks of suppliers, digital platforms, and third-party service providers is at the heart of the report. Due to the numerous possible points of compromise brought about by this interconnectedness, third-party assaults are now the main worry when it comes to protecting patient records and medical histories. Additionally, essential health infrastructures may be disrupted by geopolitical tensions and cyber warfare, which could influence clinical information confidentiality as well as service continuity.

The report also highlights how quickly new technologies like artificial intelligence, the Internet of Things, and sophisticated digital health platforms are being adopted. These developments increase the attack surface for cyber threats even while they have significant positive effects on patient care and operational effectiveness. More advanced social engineering, focused phishing tactics, and the illegal harvest of private medical data are all made possible by generative AI.

The fragmentation of regulations is still a significant obstacle. According to the survey, only a small percentage of organisations have made significant strides in improving their cybersecurity posture, and different legislative frameworks across jurisdictions make it more difficult to securely manage cross-border medical data. The risk to health institutions is increased by this legislative discrepancy as well as a worldwide lack of qualified cybersecurity specialists.

There are significant ramifications for clinical data. Patient privacy may be directly threatened by technological or governance flaws as telemedicine apps, electronic health records, and institutional data exchanges proliferate. Thus, maintaining cyber resilience in healthcare is presented as a social necessity rather than just a technological requirement, protecting patient privacy and the provision of critical medical services.

The report suggests a multifaceted approach to address these issues: investing in robust digital healthcare infrastructures, encouraging global collaboration to standardise data protection laws, cultivating skilled cybersecurity personnel in the healthcare industry, and putting continuous risk assessment into practice by keeping an eye on and auditing external providers and connected systems.

The MDCG 2019-16 guide outlines certain guidelines on how to address cybersecurity for medical devices, the CYLCOMED project focus on connected medical devices and this document proposes several suggestions and improvements to the MDCG guide.

1.1 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, it benefits from information security and risk

Funded by Horizon Europe Framework Programme of the European Union

management disciplines and incorporates them into legal research to assess the current legal rules and best practices available. In addition, the use cases deployed in the CYLCOMED project have provided feedback and lessons learnt that have been incorporated in this document. 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. 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, best practices and CYLCOMED use cases.

1.2 Structure of the document

The document is structured as follows:

Section 2 reviews the relevant *regulations* (2.2), *guidance documents* (2.4), and *standards* (2.5) related to cybersecurity for connected medical devices, encompassing both *hard-law* and *soft-law* requirements. *Ethical considerations* are also addressed in subsection 2.3.

Section 3 examines medical devices in greater detail. It first analyses the use of password-protected menus (3.1), followed by a review of the various technologies used to connect medical devices currently available on the market (3.2), as each technology requires a different cybersecurity approach. Subsection 3.3 provides an overview of existing sources and databases of known vulnerabilities, while subsection 3.4 reviews the different communication protocols implemented by manufacturers.

Section 4 presents the perspectives of the different stakeholders and reviews the lessons learned from the use cases deployed during the CYLCOMED project, including both hospital environments and telemedicine scenarios.

Section 5 discusses the emerging challenges associated with new AI-based solutions available on the market.

Funded by Horizon Europe Framework Programme of the European Union

2 Insights from legal and ethical perspectives

2.1 Introduction

There are many different regulations, standards and frameworks related to cybersecurity for healthcare devices. Connecting medical devices deployments include several components (hardware and software):

- Medical devices (Infusion pumps, mechanical ventilators, anaesthesia machines, monitors, etc.) that must comply the 2017/745 and 2017/746 regulations and where the MDCG Guide applies directly
- Networks and connections: Ethernet, Wi-Fi, Bluetooth, serial, etc.
- Clinical Information Systems (CIS). [3] There are different CIS solutions available in the market, and they can be either a medical device under the 2017/745 regulation or not, so that must be considered when deploying the solution.
- Electronic Health Records (EHRs) that usually are not a medical device under the 2017/745 regulation. That means that even the MDCG guide does not apply directly to them, their integration should be considered under the cybersecurity standpoint.

Regulations must be complied with when deploying solutions with connected medical devices, whereas compliance with guidance and standards are usually optional. A relationship of the most relevant regulations and standards related to medical devices connected deployments are presented here, grouped by its goals. We should emphasize that medical devices, CISs and EHRs are far from being standardised. In addition, CISs can or cannot be under the MDR, while EHRs are typically not under the MDR.

One of the responses to the risks and challenges posed by technological advancements in healthcare has been the revision of the EU regulatory framework for medical devices and the subsequent adoption of the Medical Devices Regulation (MDR). Among its provisions, the MDR introduced stringent requirements to ensure a high level of safety and performance for medical devices incorporating electronic programmable systems, as well as for software that qualifies as a medical device. The MDR requires a demonstration of compliance with the cybersecurity rules encompassed in the General and Safety Performance Requirements (GSPR) listed in Annex I (Article 5(2)). To assist manufacturers in fulfilling these obligations, the Medical Device Coordination Group of the European Commission has endorsed the Guidance on Cybersecurity for Medical Devices (MDCG 2019-16 Rev.1), providing recommendations on how to meet the cybersecurity-related provisions of Annex I.

The MDCG guidance on cybersecurity for medical devices is instrumental in harmonising regulatory compliance with technical standards, thereby fostering consistency across the EU. Being the first Guidance on medical device cybersecurity, it was a significant step forward in facilitating the implementation of MDR and In Vitro Diagnostic Regulation (IVDR) cybersecurity requirements. However, the medical device cybersecurity landscape is a dynamic field that has undergone significant changes since the Guidance endorsement in 2019. The following subsections will provide insights into the shortcomings and challenges identified over the course of the project.

Funded by Horizon Europe Framework Programme of the European Union

There are many regulations, ethical requirements, guidance and standards that can be relevant from a cybersecurity perspective when connecting medical devices.

Recommendation
The incorporation into the guidance of a list of relevant regulations, ethical requirements, guidelines, and standards would greatly assist integrators in the connection of medical devices. Chapter 2 of this document presents a reference that may serve as an initial list

2.2 Legal (Regulations)

1 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices

2 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices

3 GDPR (EU): General Data Protection Regulation. Manufacturers of connected medical devices shall ensure compliance with the GDPR, given that such devices process personal data, including special categories of health data, which require reinforced protection measures. In line with GDPR requirements, appropriate technical and organizational safeguards shall be implemented to ensure confidentiality, integrity, and availability of data, and to effectively mitigate risks of unauthorized access, alteration, or disclosure.

4 Directive on privacy and electronic communications The Directive on Privacy and Electronic Communications (2002/58/EC), commonly referred to as the ePrivacy Directive, is an EU legal framework that complements the GDPR by addressing privacy and data protection specifically in the electronic communications sector. It regulates confidentiality of communications, security of networks and services, as well as the use of traffic, location data, and cookies.

5 Directive (EU) 2022/2555 on measures for a high common level of network and information security across the Union. The NIS2 Directive (Directive (EU) 2022/2555) sets binding cybersecurity obligations for essential and important entities, with specific requirements on risk management, incident notification, and the implementation of appropriate technical, operational, and organizational measures. For medical devices connected to networks, NIS2 compliance is particularly relevant to ensure resilience against cyber threats and protection of critical health infrastructure.

Recommendation
It is recommended that MDCG 2019-16 place greater emphasis on compliance with the ePrivacy Directive by requiring manufacturers to implement safeguards against unlawful interception, monitoring, or unauthorized access to electronic communications generated by medical devices.

Recommendation
References to NIS directive in the MDCG 2019-16 should be updated to NIS2 and in general it is recommended that processes be put in place and enacted periodically to keep the MDCG guidelines current with respect to evolving standards and state of the art for the implementation of the MDR / IVDR, as well as to keep pace with evolutions of the regulations themselves

Funded by Horizon Europe Framework Programme of the European Union

It is interesting to note that neither MDR nor IVDR expressly refer to cybersecurity [4]. To assist device manufacturers in meeting the essential requirements of Annex I to the MDR/IVDR related to cybersecurity, the Medical Device Coordination Group of the European Commission in December 2019 endorsed the Guidance on Cybersecurity for Medical Devices (MDCG 2019-16 Rev.1) [3]. However, as same as the MDR/IVDR, the MDCG Guidance does not include explicit definitions nor reference to terms such as "cybersecurity," "security-by-design," and "security-by-default." Instead, the guidance outlines provisions related to cybersecurity for medical devices and emphasizes conceptual connections between safety and security. Additionally, key terms such as “layered defense” and “good security hygiene” are undefined. However, leaving these terms theoretical and undefined may present challenges for stakeholders seeking to implement practical cybersecurity measures effectively. Clear and concrete definitions would enhance understanding and support the practical implementation of cybersecurity principles in the context of medical devices [2].

Recommendation
Key concepts such as cybersecurity, security-by-design, and security-by-default should be explicitly defined, either by referring to legal acts that provide such definitions or following established terminology defined by frameworks such as ISO/IEC standards.

Next, the MDCG Guidance, spanning 46 pages, addresses various topics. While its primary focus is to assist manufacturers in meeting the General and Safety Performance Requirements of the MDR/IVDR related to cybersecurity, it also offers insights and suggestions for addressing cybersecurity challenges to other stakeholders in the medical device supply chain, such as integrators and operators. The main goal of MDCG Guidance is to provide device manufacturers with guidance on how to meet all the relevant essential requirements of Annex I to the MDR and IVDR about cybersecurity.

As the MDCG guidance, at the beginning of the document, sets out that “any views expressed in this document are not legally binding”, it is essential to note that the MDCG Guidance **is not a legally binding document**. Hence, in practice, manufacturers of medical devices are not legally bound by the Guidance and may interpret its content differently. Consequently, this approach undermines the overall harmonization approach of the MDR/IVDR.

Recommendation
As a soft-law instrument, explicitly indicating in the Guidance that cybersecurity requirements will be assessed against those identified in the guidance would enhance medical device manufacturers' adherence to the guidance.

As stated above, the medical device cybersecurity landscape is a dynamic field that has undergone significant changes since the Guidance endorsement in 2019. Although outdated to some extent in light of the recent EU legislative activities, Figure 1 depicts the requirements covering cybersecurity that the manufacturers should be particularly aware of, as well as their

Funded by Horizon Europe Framework Programme of the European Union

relationship with other legal frameworks. More specifically, MDCG's **Section 6** provides an overview of legislative intersections with different legal frameworks that might apply in parallel with MDR, particularly CSA, GDPR, and NIS Directive.

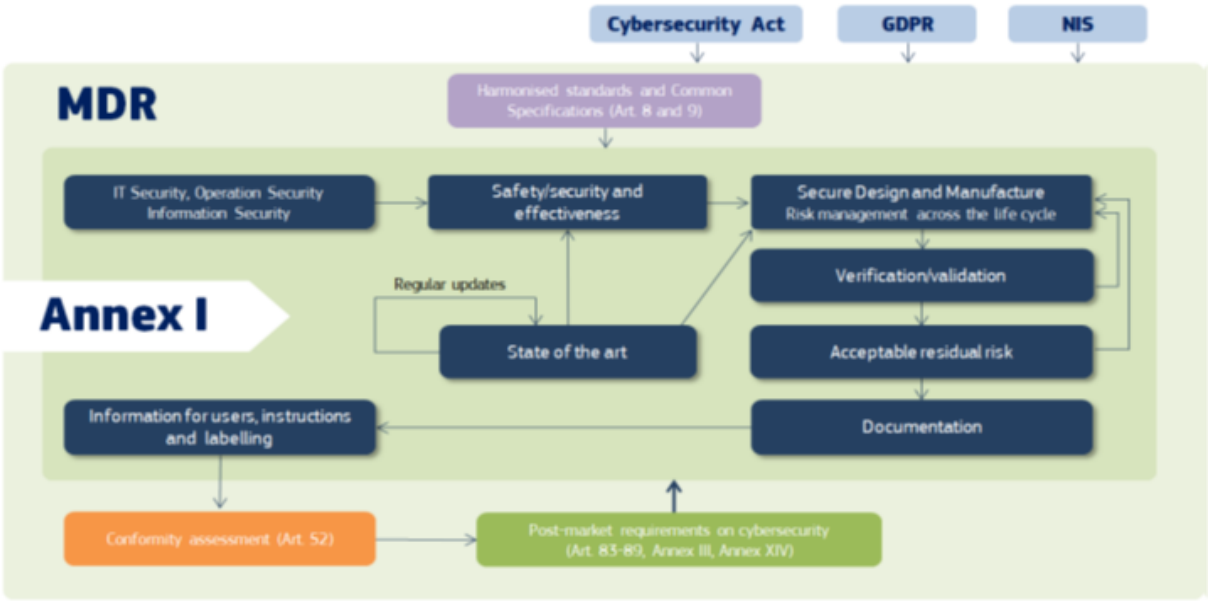

Figure 1 Cybersecurity Requirements in the MDR. Source: *MDCG Guidance, p6.*[5]

However, since the publication of MDCG 2019-16 in December 2019 and its subsequent revision in July 2020, the EU legislative framework governing medical device cybersecurity has undergone substantial transformation. Key developments include the adoption of new legislative initiatives in the fields of cybersecurity (e.g., Cyber Resilience Act) and data governance (European Health Data Spaces), as well as the emergence of regulatory instruments addressing artificial intelligence. However, since its endorsement, MDCG 2019-16 has not been updated to reflect these significant legislative developments, leading to a discrepancy that may complicate effective compliance and risk management practices

Recommendation
It is strongly recommended that the Guidance undergo regular updates to align with the evolving legal and regulatory landscape, thereby maintaining its practical relevance and supporting manufacturers in effectively addressing emerging cybersecurity requirements.

Although MDCG Guidance has not been updated to reflect the evolving legal landscape, it briefly touches upon the primary purposes of the identified legal frameworks presented in the previous figure. However, the MDCG Guidance does not dive deeper into resolving overlapping and conflicting issues that might arise in practical implementation, nor does it establish any closer link with these acts. While this analysis will be delved into more in depth

Funded by Horizon Europe Framework Programme of the European Union

in the Deliverable D2.3, some examples that clearly illustrate the necessity for more clarity are provided in this deliverable.

For instance, the MDCG Guidance briefly references the Cyber Security Act (CSA), which introduces an EU-wide cybersecurity certification framework. However, it does not establish a clear connection between the MDR and CSA, neither in terms of terminology nor substance. Regarding terminological inconsistency, the Guidance does not provide any reference to the definition of “cybersecurity”, thus missing the opportunity to establish a connection between the Guidance as a soft-law instrument and the CSA. Undoubtedly, by aligning soft-law guidance with hard-law definitions and requirements, stakeholders would benefit from clearer and more consistent guidelines for implementing cybersecurity measures in the context of medical devices and reduce ambiguity surrounding terms like "cybersecurity" [4].

Recommendation
It is essential to establish a stronger link between the soft-law guidance and hard-law definitions and requirements within the EU regulatory framework for connected medical devices. The MDCG 2019-16 guidance could be enhanced by ensuring that its recommendations are explicitly aligned with binding legislative instruments such as the Medical Device Regulation (MDR), the GDPR, the ePrivacy Directive, and the NIS2 Directive. Strengthening this alignment would improve legal coherence, facilitate consistent implementation across Member States, and ensure that manufacturers clearly understand how to translate regulatory obligations into concrete cybersecurity and data protection practices

Furthermore, clarifying the interplay between the MDR and CSA, for instance, regarding cybersecurity certification, would be highly beneficial for stakeholders. In regard to certification, according to Article 56(2) of the CSA, cybersecurity certification is voluntary unless mandated explicitly by EU or Member State regulations. If certain Member States were to require mandatory cybersecurity certification, manufacturers would need to obtain such certification for their devices to be marketed in those Member States. However, this requirement might not apply in other Member States, leading to inconsistencies across Member States and potential regulatory shopping. In such scenarios, manufacturers who have already obtained CE marking for their devices may be required to undergo an additional certification process, leading to duplicated requirements and increased costs. This highlights potential challenges arising from differing regulatory approaches within the EU regarding cybersecurity certification for medical devices. Therefore, the MDCG Guidance could play a crucial role in providing clarity on the interplay between the Medical Device Regulation (MDR) and the Cyber Security Act (CSA). By addressing how these regulatory acts intersect and complement each other, the guidance could enhance stakeholders' understanding and facilitate compliance with both frameworks. This clarity would ultimately promote cybersecurity in the context of medical devices by helping manufacturers navigate potential requirements and certifications effectively across different Member States of the EU.

Next, MDCG Guidance does not address any connection between the MDR and Radio Equipment Directive (RED), which establishes a regulatory framework for placing radio equipment on the Single Market. All internet-connected radio equipment that is Wi-Fi, Bluetooth, LTE, 5G, or GPS enabled falls under the RED's scope. Consequently, the RED applies to medical devices if they include components such as Wi-Fi or Bluetooth modules,

Funded by Horizon Europe Framework Programme of the European Union

which means that, apart from meeting stringent MDR requirements, medical device manufacturers will need to comply with RED, conduct conformity assessment under its rules, and declare conformity with RED, in addition to the MDR. However, the MDCG Guidance does not address the applicability of the Radio Equipment Directive (RED), which is a notable omission considering its relevance. The RED should be acknowledged and included in the guidance to ensure comprehensive coverage of regulatory considerations related to medical devices incorporating radio technologies.

It is important to note that the Commission adopted a Delegated Act of the Radio Equipment Directive at the end of 2021, which aims to increase the level of cybersecurity, personal data protection, and privacy for specific categories of radio equipment. The Delegated Regulation has brought some clarity and relief to the medical device manufacturers as it excludes medical devices from its scope regarding cybersecurity requirements (Article 2(1a)).

Recommendation
It is strongly recommended to systematically identify and map overlapping issues arising from multiple legislative acts governing cybersecurity requirements for medical device manufacturers, to provide clear and detailed guidance and mitigate potential compliance gaps and regulatory inconsistencies.

Next, while the MDCG primarily provides manufacturers with the necessary guidance on meeting the relevant General and Safety Performance Requirements of MDR regarding cybersecurity, it also gives some hints on addressing cybersecurity challenges to other players in the medical device supply chains (e.g., Integrators and operators). For instance, Guidance states that healthcare and medical professionals are responsible for the use of medical devices for their purposes, such as diagnosing or monitoring patients. These users may access, review, and exchange data with the devices and may be responsible for the patient's education and establishing software and device parameters of usage. Furthermore, Guidance encourages patients and consumers to employ cyber-smart behaviour, such as paying attention to privacy, being aware of suspicious messaging, and browsing responsibly. Eventually, MDCG guidance states that all stakeholders, such as manufacturers, suppliers, healthcare providers, patients, integrators, operators, and regulators, **share responsibilities for ensuring a secure environment for the benefit of patient' safety.** However, from the space and content devoted to healthcare professionals and patients, MDCG Guidance fails to acknowledge that humans are the weakest link in the cybersecurity chain.

Recommendation
Integrate a human-centric approach into the guidelines and provide targeted guidance on user awareness, training, and operational security practices to enhance cyber threat prevention and mitigation and improve stakeholder preparedness.

Additionally, MDCG Guidance does not delve into how the shared responsibilities of different stakeholders may be affected or potentially conflicted by various applicable laws to the medical device ecosystem. Therefore, more guidance on this subject matter would facilitate the analysis of relevant aspects of other horizontal legislation and contribute to achieving a more

Funded by Horizon Europe Framework Programme of the European Union

coherent cybersecurity regulatory framework overall. By considering the interconnected responsibilities and legal implications across different regulatory domains, the guidance can provide stakeholders with more comprehensive guidance to navigate complex cybersecurity requirements for medical devices.

2.3 Ethical

While some scholars [4] argue that "ethical issues are at the core of cybersecurity practices", it is interesting to note that MDCG Guidance does not contain any reference to ethics. New technologies are an example of where the law lags and where ethics play a crucial role, paving the way to legal norms. The field of artificial intelligence is the most obvious example where ethics shapes legal solutions and plays a gap-filling function in the absence of legally binding norms. Therefore, casting more light on ethical principles and values would facilitate understanding the risks at stake and contribute to the implementation of ethical principles throughout the entire life cycle of medical devices [7].

Recommendation
It is strongly recommended that the Guidance explicitly address ethical principles and values. Integrating ethics would clarify the risks associated with medical device cybersecurity and bridge gaps in the legal framework, ensuring that ethical considerations guide the development, deployment, and life cycle management of medical devices, particularly in emerging areas such as artificial intelligence.

Being the first and only guidance on medical device cybersecurity, the MDCG endorsement was a significant step forward in facilitating the implementation of MDR cybersecurity requirements. However, it is vital to emphasise that the medical device cybersecurity landscape is a dynamic field that has undergone significant changes since the MDCG Guidance endorsement in 2019. Moreover, the regulatory landscape impacting medical device cybersecurity continues to evolve at a fast pace. For instance, it is worth noting that the NIS Directive, referred to in the Guidance, has been repealed by the NIS2 Directive. The new directive introduces various novelties and broadens the scope of its application to include medical device manufacturers. Even acknowledging this change in the Guidance would help readers understand that the Guidance is up to date [7].

2.4 Guidances

1 FDA Guidance (USA): Postmarket cybersecurity management.
2 IMDRF Guidance: Internationally harmonized guidance on medical device cybersecurity

Funded by Horizon Europe Framework Programme of the European Union

2.5 Standards

2.5.1 Foundational medical devices standards: safety

1. IEC 60601-1-8 (Alarm Systems): General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems
2. IEC 60601-2-24 (Infusion Pumps): Requirements for the basic safety and essential performance of infusion pumps and controllers
3. IEC 62304 (Medical Device Software): Software life cycle processes

Recommendation
Ensure the guidelines account for general safety and performance requirements for devices with cybersecurity risks as outlined in Annex I of the MDR and include both functional and non-functional IT security requirements

2.5.2 Risk management

1. ISO 14971 (Medical Devices): Application of risk management to medical devices
2. ISO/TR 24971 (Medical Devices): Guidance on the application of ISO 14971
3. ISO/TR 24971:2020 (Medical Devices): Guidance on the application of ISO 14971
4. IEC 80001-1 (Risk Management for IT Networks): Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software
5. IEC TR 80001-2-2 (Risk Management for IT Networks): Guidance for the communication of medical device security needs, risks and controls
6. AAMI TIR57: This technical Information Report (TIR) provides guidance on methods to perform information security risk management for a medical device in the context of the Safety Risk Management process required by ISO 14971
7. AAMI TIR97: Principles for medical device security - Postmarket risk management for device manufacturers

Recommendation
There is a need to consider relationships between cybersecurity consequences (“A security violation that results from a threat action”) and harms referred to in MDCG 2019-16, which are typically associated with patient harms (“injury or damage to the health of people, or damage to property or the environment” (ISO 14971). The key relationship is which cybersecurity consequences lead to patient harms. There is therefore a related need to consider cybersecurity threats and consequences alongside the existing MD risk assessment proposed in ISO 14971. A reasonable starting point for cybersecurity risk assessment is described in ISO 27005, part of the ISO 27000 series that is concerned with information security risk management.

Recommendation

Funded by Horizon Europe Framework Programme of the European Union

The relationship between safety risk assessments (as addressed by ISO 14971) and security risk assessments (e.g., TIR57) should be clearly explained, including when security risks impact safety and how they must be included in safety risk assessments with clear traceability between security and safety analysis.

2.5.3 Cybersecurity core standards

1. ISO/IEC 27001(ISMS): Information security, cybersecurity and privacy protection, ISMS requirements
2. ISO/IEC 27002: Information security, cybersecurity and privacy protection. Information security controls
3. ISO/IEC 27032 (Cybersecurity): Guidelines for Internet security
4. ISO/IEC 29147 (Vulnerability Disclosure): Vulnerability disclosure enables users to perform technical vulnerability management as specified in ISO/IEC 27002
5. ISO/IEC 30111 (IT security techniques): Vulnerability Handling Processes

Recommendation

There is an absence of guidance in the MDCG on security-related controls with respect to device classes that makes it difficult to identify minimum security control criteria for various types of medical devices. These controls are typically related to risk assessment, where they are used to mitigate identified risks, so it is suggested that reference to relevant cybersecurity risk management standards such as ISO 27002 are recommended by MDCG.

2.5.4 Secure communications

- IEC 62443 Series (Industrial Communication Networks): Security for industrial control systems (relevant to connected medical devices).
- ISO/IEC 27033 Series (IT): Security techniques. Network security.

2.5.5 Interoperability standards

- ISO/IEEE 11073-10101 Nomenclature for Medical Device Communication

From the risk management perspective, one of the risks to be taken into account is the nomenclature for the vital signs. An error mapping a vital sign can obviously be critical. This problem only arises when connecting medical devices and that is what the CYLCOMED project is about. The first point is to understand if medical devices being used today are following any standard for the nomenclature. To analyse this problem let's start by checking the medical devices we are working with or have worked with, classified by their use of the 11073:10101standard (usually hl7v2 + 11073:10101):

1. Using hl7v2 + 11073:10101

Funded by Horizon Europe Framework Programme of the European Union

2. Monitors Cetusx12, Cetusx15, Cetusx1 and Pavo from Axcent
3. Anaesthesia machines A5, A7, A8 and A9 from Mindray
4. Mechanical ventilators SV300, SV600 and SV800 from Mindray
5. Monitors Benevision from Mindray
6. Anaesthesia machine Genesis from Hersill
7. Cardiac monitor Starling from Baxter (partially)
8. Cardiac monitor Mostacare from Vygon (partially)
9. Using proprietary protocols
10. Mechanical ventilators Servo-i and Servo-u from Getinge
11. Anaesthesia machine Flow-i from Getinge
12. Monitors Life Scope from Nihon-Kode
13. Mechanical ventilator Vivo V45 from Breas
14. Monitors Vista 120, Delta, Gamma, Kappa and Vista from Drager
15. Mechanical ventilators Babylog, Evita and Oxylog from Drager
16. Anaesthesia machines Perseus, Primus and Fabius from Drager
17. Cardiac monitor Hemosphere from Edwards
18. Anaesthesia machines Aestiva, Aespire and Carestation from General Electric
19. Mechanical ventilators Carestation R860, Engstrom and iVent from General Electric
20. Monitors B30, B40, B105, B125, Carescape B450 and Carescape B850 from General Electric
21. Monitors Radical, Rad 8, Rad 97 and Root from Masimo
22. Mechanical ventilator PB840 from Medtronic
23. Monitors Capnostream20, BIS Vista and PM1000N from Medtronic
24. Mechanical ventilators Trilogy EVO and Respironics V60 from Philips
25. Monitors IntelliVue and SureSigns families from Philips
26. Monitor Sentec Digital Monitoring from Sentec

From the risk perspective, the fact that the nomenclature standard is not always used, creates a risk issue that must be considered when implementing a solution to connect medical devices. Most of the proprietary protocols used by the medical devices manufacturers have been used for many years and we understand the difficulty to introduce any changes on these protocols, as that will be disruptive.

Recommendation
The guidance should request medical devices manufacturers to include a map in their technical documentation from their proprietary names to the nomenclature provided by the ISO11073 standard, as this is easy to implement and will reduce the risk to the connected medical devices solutions.

From a cybersecurity point of view, the Service-oriented Device Connectivity (SDC) component of the ISO/IEEE 11073 is a key standard. The SDC family comprises "Core Standards," "Participant Key Purpose (PKP) standards," and "Device Specialization (DevSpec) standards."

- **Core Standards (e.g., ISO/IEEE 11073-20702 Medical DPWS, ISO/IEEE 11073-10207 Domain Information and Service Model, ISO/IEEE 11073-20701 Architecture and Binding):** These lay the foundational interoperability and

Funded by Horizon Europe Framework Programme of the European Union

include mechanisms for safe and secure data exchange in a distributed system, and dynamic network participant discovery. Medical DPWS (MDPWS) is derived from OASIS DPWS and defines extensions and restrictions for medical device safety requirements.

- **Participant Key Purpose (PKP) Standards (e.g., ISO/IEEE 11073-10700 Base PKP, P11073-10701 for metric data, P11073-10702 for alerts, P11073-10703 for external control):** These define requirements for participating providers and consumers, allowing manufacturers to have expectations about how other manufacturers' devices will behave. This common understanding is crucial for performing risk management, verification, validation, and usability engineering for safe and secure system functions. The latest versions of PKP standards, like ISO/IEEE 11073-10700-2024, explicitly address requirements for the allocation of responsibilities for SDC base participants, contributing to overall system safety and security

2.5.6 Risk assessment

1. Information security, cybersecurity and privacy protection. Evaluation criteria for IT security ISO/IEC 15408.
2. ISO/IEC 27005 Information security, cybersecurity and privacy protection. Guidance on managing information security risks.
3. ISO 13485:2016 Medical devices — Quality management systems.
4. IEC 82304-1 (Health Software): General requirements for product safety.
5. ISO/IEC 81001-5-1 (Health Software and Health IT Systems Safety): Activities in the product life cycle.

2.5.7 Best practice frameworks

- NIST SP 1800-8 (Securing Wireless Infusion Pumps): Practical guidance for wireless infusion pumps.
- NIST Cybersecurity Framework2.0 (2024): A structured approach to managing cybersecurity risks.
- UL 2900 Series: Standards for cybersecurity of network connectable products.

Recommendation
The guidance should indicate some principles about the necessity of conformance to which standards, because the standards landscape has grown so much that it is impossible to keep track of all of them, so they are just all ignored.

Funded by Horizon Europe Framework Programme of the European Union

3 Insights from manufacturers

MDCG 2019-16 provides key cybersecurity recommendations for medical device manufacturers to ensure their products remain secure against cyber threats. Manufacturers should integrate cybersecurity measures from the early stages of product development, ensuring devices are designed with security in mind. A comprehensive cybersecurity risk management process should be implemented, assessing potential threats and vulnerabilities throughout the device's lifecycle. Devices should incorporate security features to prevent unauthorized access, including authentication mechanisms and encryption. Manufacturers should provide timely security updates and patches to address vulnerabilities and maintain device integrity. Clear cybersecurity-related information should be provided to healthcare providers and end-users, ensuring they understand how to securely operate the device. A system for monitoring cybersecurity incidents should be in place, allowing manufacturers to respond effectively to potential threats

Not all medical devices pose the same level of risk to patients; their vulnerability to cyberattacks largely depends on the type of device. At least, for all the medical devices, the potential dangers of a cyberattack may include:

1. Delay in treatment;
2. Failure of life support;
3. Privacy violations;
4. Identity theft.

On top of that, there are medical devices whose improper manipulation could directly impact patient health. Examples include altering the infusion rate of a medication pump, modifying the settings of a mechanical ventilator, or tampering with an anaesthesia machine. In extreme cases, such actions could even endanger the patient’s life.

Our recommendation for medical device integration projects is to classify all connected medical devices into two categories: *"non-critical"* and *"critical"*, depending on whether their manipulation could directly affect the patient's condition.

3.1 Medical device menus

In general, the menus on the screens of medical devices do not require a username and password for access. This is because, in emergency situations, the risk of a clinician being unable to access the device outweighs the risk of unauthorized access. Critical medical devices (see Section 3.1) are typically located in intensive care units and operating rooms, where physical access is highly controlled. As a result, their security relies primarily on restricting physical access to the location of the medical device.

Many medical devices include certain menus (sometimes multiple) protected by a username and password or by a password alone. While each manufacturer organizes functionality differently within these menus, they typically allow for the configuration of communication protocols, network settings, language selection, unit preferences, software updates, error log access, and more.

For example:

Funded by Horizon Europe Framework Programme of the European Union

- The General Electric B850 monitor includes a service menu for communication settings, which requires a password.
- The Axcent PAVO monitor features a user maintenance menu, also password protected, that allows network configuration, among other options.

From the hospital perspective, it is essential to document the existence of these menus in the inventory of connected medical devices within the facility. Furthermore, these passwords should be incorporated into the hospital's general security policy, including guidelines for password management, such as the frequency of password changes. In general, in an environment like intensive care the perception of potential cybersecurity issues is almost zero compared to patient management

Recommendation
Suggest keeping an inventory of medical devices deployed at the hospital with details of existing passwords for each device, its software version and its serial number

3.2 Communication interfaces

3.2.1 Introduction

Medical devices available on the market utilize various technologies to connect to Clinical Information Systems (CIS). Ideally, regardless of the communication interface used, the transmitted information should be encrypted. However, this depends on the specific medical device, and in general, most medical devices do not encrypt the measurements they transmit. From the hospital perspective, keeping an inventory for all the connected medical devices and their interfaces will help to design a secure infrastructure, as each communication interface has different security considerations. The guidelines focus predominantly on the software components of medical devices without considering the broader spectrum of Internet of Medical Things (IoMT) system vulnerabilities [8].

Recommendation
Expanding the guidelines to include specific security considerations tailored to IoMT could mitigate these risks by providing clear directives on securing varied device architectures within healthcare ecosystems

While the guidelines advocate for rigorous risk management, they lack detailed protocols for the unique risk landscape of IoMT systems [8].

Recommendation

Funded by Horizon Europe Framework Programme of the European Union

Implementing a more nuanced risk management framework that includes specific methodologies for assessing and mitigating risks unique to IoMT such as cross-device data breaches or network-based vulnerabilities would greatly enhance the robustness of these critical systems

3.2.2 Serial RS232

Legacy technology with limited bandwidth is highly recommended from a cybersecurity perspective and is therefore widely used in medical devices, particularly in critical ones. Examples include the Getinge Flow-i anaesthesia machine, the General Electric Carescape monitors, and the Masimo Radical pulse oximeter.

Unfortunately, there are many different types of connectors used for these connections, such as DB9F, DB9M, DB15F, as well as proprietary connectors that do not adhere to any standard. Some medical devices also use a USB output with a converter to RS232 for communication, such as the Getinge PulsioFlex hemodynamic monitor.

Additionally, two types of cables are used in serial communications: straight-through cables and null modem cables. The correct cable to use is specified in the manufacturer's manual.

3.2.3 USB

There are few devices on the market that use the USB protocol for communication. An example is the Breas Vivo 45 ventilators. USB is more modern than RS232 and, from a cybersecurity perspective, represents an intermediate position between RS232 communications and TCP/IP communications used in Ethernet or Wi-Fi connections.

3.2.4 Ethernet / TCP/IP

Widely used and offering higher bandwidth, TCP/IP communications require additional security considerations since devices connected to a network can potentially be accessed from various points within that network. Devices on the market operate either as TCP/IP servers or clients. Examples include the Dräger Vista120 monitor and the Axcent Cetus system.

When designing networks to connect medical devices, there are two main approaches:

- Each medical device is assigned a unique IP address that is accessible from the hospital's network.
- A private network is created, accessible only through the communication device. In this setup, identical IP addresses can be assigned to identical medical devices in different hospital beds. This approach enables seamless management of medical devices when transferred between rooms, maintaining the association between the medical device and the patient. The communication device handles this relationship, ensuring continuity regardless of device relocation.

Funded by Horizon Europe Framework Programme of the European Union

In general, option 2 is preferred over option 1 from a cybersecurity perspective, as medical devices, being connected to a private network separate from the hospital's main network, are much more isolated in this setup than in option 1. This isolation reduces the exposure of medical devices to potential security threats from the broader hospital network.

Recommendation
Introduce stronger network security requirements, particularly mandating strict network segmentation to separate critical medical devices from general hospital IT systems

3.2.5 WiFi / TCP/IP

Less commonly used than the previous option, Wi-Fi is typically employed as an additional option for devices that primarily operate over Ethernet. An example is the Axcent Cetus monitor. In addition to all the cybersecurity considerations for TCP/IP networks, it is necessary to consider the specific cybersecurity measures required for Wi-Fi networks. These include securing wireless access points, encrypting communication channels, and ensuring robust authentication mechanisms to protect against unauthorized access.

3.2.6 Bluetooth

Typically used in medical devices employed in telemedicine or devices that are worn by patients outside the hospital, an example being the Nonin Onyx 9560 pulse oximeter.

Recommendation
The guidance should indicate some references to relevant standards for each technology deployed. The inventory proposed in 3.1 should also include the communication interface for each medical device

3.3 Known vulnerabilities

3.3.1 Introduction

There are different repositories for already known vulnerabilities, and several organizations that provide alerts when a security problem is identified. A summary for some of the most relevant ones is included in the following sections.

Recommendation

Funded by Horizon Europe Framework Programme of the European Union

Keep an inventory (suggested in 3.1) for all the medical devices deployed and match them against the different databases and subscribe to the alerts generated from the different organizations

3.3.2 CVE

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. They keep a database for known software vulnerabilities that can include medical devices or software solutions connected to medical devices. As an example, vulnerability CVE-2023-30559 affects to BD (Becton&Dickinson) Carefusion Alaris PCU 8015: The firmware update package for the wireless card is not properly signed and can be modified

Figure 2 Becton & Dickinson Alaris PCU

3.3.3 CISA

America´s cyberdefense agency is an official organization of the United States government and provides warning that can relate to medical devices. As an example, they have issued a

Funded by Horizon Europe Framework Programme of the European Union

critical warning for the Contec CMS800, as it has a back door that sends sensitive information to China.

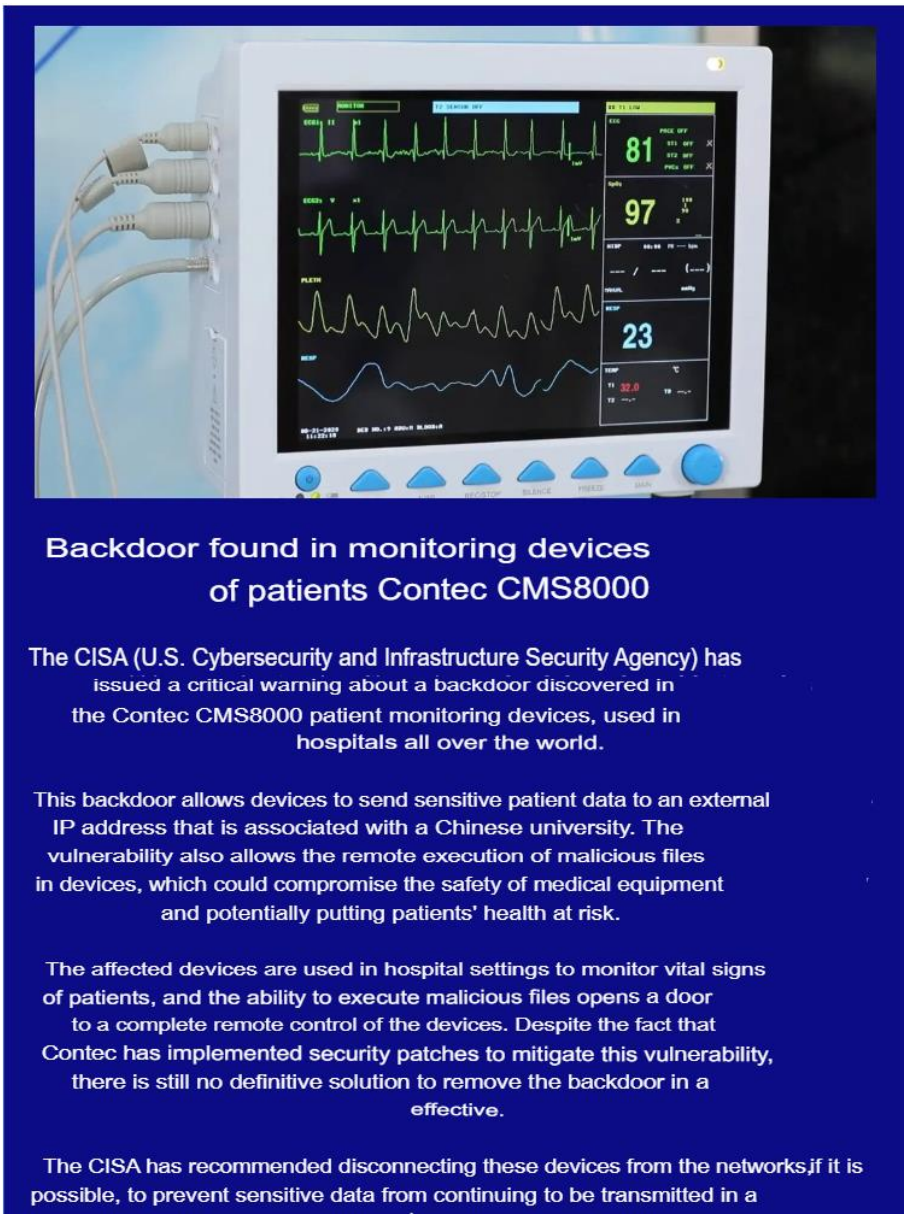

Figure 3 Backdoor in Contec CMS8000

3.3.4 FDA

U.S. Food and drug administration provide alerts that can relate to medical devices, mainly related to risk:

- Devices recall according to "U.S Food and Drugs Administration" (https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfres/res.cfm).
- **FDA-TPLC (Total Product Life Cycle):** data about medical devices problems and recalls reported. (https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfTPLC/tplc.cfm)

Funded by Horizon Europe Framework Programme of the European Union

A subscription service is available. (https://www.fda.gov/about-fda/center-devices-and-radiological-health/subscribe-cdrh-email-lists)

Some examples are included (alerts received on February, 2nd, 2025) to provide an idea from what to expect from FDA:

- Potential to Miss Critical Safety Alerts for Smartphone-Compatible Diabetes Devices.
- Gas Powered Emergency Resuscitator Recall: Mercury Medical Removes Neo-Tee T-Piece Resuscitator.
- Oxygen Concentrator Recall: JIANGSU JUMAO X-CARE MEDICAL EQUIPMENT CO LTD Removes JMC5A Ni/TruAire-5 Oxygen Concentrator due to the devices spontaneously catching fire.

3.3.5 EUDAMED

EUDAMED is the IT system established by Regulation (EU) 2017/745 on medical devices and Regulation (EU) 2017/746 on in vitro diagnosis medical devices.

EUDAMED will keep an updated database for all the medical devices approved under the Regulation (EU) 2017/745 and Regulation (EU) 2017/746.

EUDAMED will provide 6 different modules, the Vigilance and Post-market Surveillance module being the one related to cybersecurity and risk management.

Various reports will be submitted via the Vigilance Module, and be used to report incidents:

- Submission of Periodic Safety Update Report (PSUR).
- Submission of Periodic Summary Reports (PSR).
- Reporting of Serious Incidents and Field Safety Corrective Actions (FSCAs) and Field Safety Notices (FSNs).

FSCAs are automatically distributed to the appropriate authorities after they are reported in the Vigilance Module. FSNs are published. There will also be a function in the module to generate summary reports.

The Vigilance module is expected to be mandatory beginning in Q3 2026 with full EUDAMED functionality planned for Q2 2027.

Recommendation
Despite the EUDAMED Vigilance Module not being available until Q2 2027, a reference in the Guide to its goals and functionality would be very helpful.

3.4 Communication protocols

Unfortunately, most communication protocols used to connect medical devices are proprietary. When a manufacturer does use a standard protocol, it is typically HL7 version 2 and its various

Funded by Horizon Europe Framework Programme of the European Union

variants (2.3.1, 2.4, 2.5, 2.6, etc.). Some examples of medical devices that communicate through HL7 include the Nihon Koden Life Scope BSM-3562, the Mindray A5 anesthesia machine, and the Vygon Mostcare system.

Among proprietary protocols, examples include SCI (Servo-u), FCI (Flow), and CIE (Servo-i) from Getinge, the Data Export Interface (IntelliVue MX700) from Philips, Export (Gamma), Medibus (Evita XL), and Medibus.X (Perseus A500) from Dräger, Com Output (Carestation R860) and S5 (Carescape B850) from General Electric, and ASCII-1 (Root) from Masimo.

This brief list illustrates the complexity faced by solutions that integrate the various types of medical devices available on the market.

From a cybersecurity perspective, it is essential to understand the type of communication used by each protocol. The communications between the medical device and the communication device (element 3 in the data journey) can be:

- **Unidirectional**: Messages with the values from the medical device are received, but there is no communication in the reverse direction, from the communication device to the medical device.

- **Bidirectional**: Communication occurs between the communication device and the medical device. Within this category, two subcategories can be distinguished:

    - **Communication between the communication device and the medical device is solely related to the communication itself** (e.g., requesting measurements, starting the communication, requesting alarms, selecting medical parameters to receive, frequency of data transmission, etc.). Most medical devices operate in this manner.
    - **Communication between the communication device and the medical device can modify its settings** (e.g., ventilation mode, units, ventilation settings, infusion pump rate, etc.). Very few medical devices on the market allow this type of operation due to the obvious risks it entails. However, if such a device exists in a facility, it must be clearly identified, and cybersecurity measures for its connection must be strictly enforced.

It is important to document the different types of communications deployed within the facility. This documentation helps to ensure proper management of security risks and enables effective monitoring of device interactions, especially when integrating various medical devices with different communication protocols. Detailed records also aid in compliance with cybersecurity standards and best practices.

Recommendation
Inventory suggested in 3.1, should include the protocol used to connect each medical device and the type of the medical device: mechanical ventilator, infusion pump, monitor, etc.

Funded by Horizon Europe Framework Programme of the European Union

Funded by Horizon Europe Framework Programme of the European Union

4 Joint responsibility from other stakeholders. Pilots

4.1 Introduction

MDCG 2019-16 highlights the joint responsibility of various stakeholders in ensuring cybersecurity for medical devices. Regulatory authorities must oversee compliance with cybersecurity regulations and provide guidance. Patients and other end-users are expected to follow security best practices, such as using strong authentication and keeping devices updated. Supply chain partners, such as distributors and service providers, must ensure secure handling and maintenance of medical devices.

Regulatory authorities play a crucial role in ensuring the cybersecurity of medical devices, as outlined in MDCG 2019-16. They are responsible for setting cybersecurity requirements, establishing clear cybersecurity guidelines for medical device manufacturers, ensuring compliance with Regulation (EU) 2017/745 and Regulation (EU) 2017/746. They must monitor compliance supervising the implementation of cybersecurity measures by manufacturers and healthcare providers, ensuring adherence to best practices. Regulatory bodies should facilitate mechanisms for reporting cybersecurity incidents and coordinate responses to mitigate risks. The authorities must work closely with manufacturers, healthcare institutions, and cybersecurity experts to enhance medical device security. Given the evolving nature of cyber threats, regulatory authorities should continuously update cybersecurity guidelines to address emerging risks.

MDCG 2019-16 provides cybersecurity recommendations for patients and end-users to ensure the safe use of medical devices. Patients should follow manufacturer's guidelines to prevent unauthorized access to their medical devices. End-users must use secure passwords and authentication methods to protect personal health data. Patients should be informed about cybersecurity risks and best practices. IT personnel must ensure that medical devices receive necessary software updates and security patches. Health data should be transmitted only through encrypted communication channels.

MDCG 2019-16 also acknowledges the critical role of supply chain partners in ensuring the cybersecurity of medical devices. Supply chain partners must ensure that medical devices are transported and stored securely, preventing unauthorized access or tampering. They should implement cybersecurity risk assessments to identify vulnerabilities in the supply chain. Close coordination with device manufacturers is essential to maintain security standards and address potential threats. Supply chain partners must adhere to cybersecurity requirements outlined in Regulation (EU) 2017/745 and Regulation (EU) 2017/746, establishing protocols for reporting cybersecurity incidents and responding effectively to threats.

4.2 Hospital environment

Hospitals play a crucial role in ensuring the cybersecurity of medical devices, and will review the main recommendations to deploy a connected medical device solution

Recommendation

Funded by Horizon Europe Framework Programme of the European Union

Strong cybersecurity measures should be implemented, including firewalls, intrusion detection systems, and network segmentation to protect medical devices from cyber threats.

Recommendation
Healthcare providers should enforce strict access controls, ensuring that only authorized personnel can interact with medical devices and sensitive patient data. IT department must ensure that medical devices receive timely security updates and patches to mitigate vulnerabilities.

Recommendation
Medical and all the staff should be trained on cybersecurity best practices, including recognizing phishing attempts and securing patient data. Incident response plans should be established, and medical devices should continuously be monitored for potential threats.

Recommendation
Healthcare institutions should work closely with medical device manufacturers to ensure compliance with cybersecurity standards and receive necessary support.

Integration of CYLCOMED Tools into a Legacy Medical Device

CYLCOMED has taken into consideration the requirements for regulatory compliance. Its primary purpose has been to ensure that highly sensitive medical data remains secure, thus encryption stands as the fundamental piece. In this use case, the implemented tools have been integrated into a multi-parameter monitor from the company RGB Medical Devices, designed for closed-loop neuromuscular relaxation control. Therefore, it is responsible for measuring neuromuscular relaxation, calculating the drug dose to be injected, to maintain the neuromuscular transmission (NMT) measurement within target values by autonomously controlling an infusion pump to administer the drug.

In the real world, medical data is often exported to external cloud systems (EHR systems and similar). Therefore, the device will operate in a hyper-connected environment, and this is where the tools and technologies developed throughout the CYLCOMED project come into play. These security tools have been designed to be usable in any type of medical device different from the present use case. Therefore, it's important to understand the steps and developments required for successful integration.

As can be presumed, modifying a medical device is a complex task with numerous implications regarding both security and regulations. Additionally, medical devices typically lack sufficient power to run the developed tools or don't have an operating system that allows their execution.

Funded by Horizon Europe Framework Programme of the European Union

For all these reasons, the chosen approach is to use an external device that connects directly to the monitor, integrating all the tools, and acting as the intermediary between the monitor and the external world. In this case, a Raspberry Pi 4 minicomputer was used, which has sufficient power for deploying the applications that comprise the CYLCOMED toolbox, as well as the necessary communication ports.

Key point
The cybersecurity recommendation is to encrypt all data coming from the medical devices. Most medical devices in the market today do not encrypt the data, the CYLCOMED approach in pilot 1 has been to use a Raspberry PI connected to the medical device and do the encryption in the Raspberry PI.

This ensures that once the data leaves the device, it travels across the encrypted network, so only entities with permission can decrypt it. To use this tool, a specific application needs to be developed for each device and deployed on the Raspberry Pi board. This tool is responsible for receiving data sent by the monitor, formatting it appropriately for encryption, and establishing or requesting suitable policies for data decryption.

Relevant output of CYLCOMED

As mentioned before, a big limitation in the wide deployment of cybersecurity standards is the lack of an interoperability standard that could operate like a universal language among devices. This would relieve a great amount of engineering workload devoted to system´s integration. Fortunately, one of the most important and relevant standards that has been identified by CYLCOMED is ISO/IEEE 11073 standard. ISO/IEEE 11073 standard, also known as **SDC protocol (Service Device Communication)**, is finally being deployed. ISO/IEEE 11073 standard also includes a nomenclature that is starting to be adopted by manufacturers

CYLCOMED is promoting this standard among MD manufacturers. This standard will change the medical equipment landscape in the forthcoming years: from centralized to specialized interoperable devices. But manufacturers will have to be compliant with ISO/IEEE 11073.

What is SDC? SDC is an interoperability protocol based on ISO 11073, designed as a common language among devices to ensure reliable communication and data exchange. It will unlock a new range of opportunities, improving usability and performance, ultimately enhancing patient safety. Connectivity issues will soon be a thing of the past.

Imagine the possibilities: Upcoming devices such as our Vision DUO neuromuscular transmission (NMT) monitor will not only report a patient's status in real time but also exchange data simultaneously with all other connected devices at the bedside.

Funded by Horizon Europe Framework Programme of the European Union

Here are just a few examples of what SDC makes possible:

- Combining NIBP and ECG waveforms, using the QRS complex to accelerate and improve the reliability of blood pressure measurements.
- Regulating vital signs such as BP, NMT, pain, or consciousness through automated drug infusion, providing safer and more personalized care.

Managing alarms from all devices through a single output, simplifying workflow, reducing false positives, and improving user focus.

The ISO/IEEE 11073 Service-oriented Device Connectivity (SDC) family of standards is a crucial development for medical device interoperability, especially in acute care settings. Regarding cybersecurity implementation, here's a breakdown of the current situation:

- **Cybersecurity is a Core Design Principle:**
  - **Integrated Security Features:** SDC standards are designed with security in mind. They incorporate stringent security protocols, including **TLS-based security mechanisms with mutual authentication** to ensure that only approved devices and systems can interact, and data transmitted are encrypted. This protects hospital assets and patient information from misuse or theft.
  - **Data Integrity and Confidentiality:** The use of TLS protocols ensures the integrity and confidentiality of information. Secure data transport is achieved through **end-to-end encryption based on X.509 public key infrastructure** for digital certificate creation.
  - **Authorization and Access Control:** Connectivity to identified devices on the network is managed based on **whitelists for authorization**. Manufacturers and healthcare organizations also need to implement and manage trust stores, permit/deny lists, and action authorization matrices.
  - **Zero-Trust Cybersecurity:** Some implementations and kits for SDC are already incorporating a zero-trust cybersecurity approach, further enhancing security.

Key point

Funded by Horizon Europe Framework Programme of the European Union

Commitment from medical devices manufacturers to SDC is key to improve the cybersecurity when connecting medical devices.

Ongoing Challenges and Mitigation:

- **Expanded Attack Surface:** Increased connectivity, while beneficial, expands the attack surface for cyber threats like data breaches, ransomware, and Denial-of-Service (DoS) attacks.
- **IoMT Vulnerabilities:** IoMT (Internet of Medical Things) devices can have vulnerabilities (e.g., unpatched firmware, default credentials).
- **Balancing Security and Usability/Patient Safety:** A significant challenge is to implement robust security measures without negatively impacting clinical treatment and patient safety by preventing or delaying authorized access.
- **Legacy Device Integration:** Integrating older devices that may not fully support SDC's security features presents a challenge.
- **Compliance and Regulatory Adherence:** Adhering to regulations like HIPAA and GDPR for patient data protection is paramount.

Recommendation (Mitigation strategies)

- **Robust Encryption and Authentication:** Strong encryption (e.g., AES-256 for data at rest, TLS/SSL for data in transit) and robust authentication (e.g., MFA, X.509 certificates) are critical.
- **Access Controls and Network Segmentation:** Role-based access controls (RBAC) and network segmentation help isolate medical devices and limit the impact of a breach.
- **Regular Audits and Patch Management:** Regular security audits, vulnerability assessments, and timely patching of firmware and software are essential.
- **Secure API Design and Incident Response:** Secure API design and a comprehensive, tested incident response plan are also vital.
- **Collaboration:** Continued collaboration between healthcare providers, policymakers, and technology developers is necessary to address implementation challenges and ensure compliance.

In summary, ISO/IEEE 11073-SDC is actively addressing cybersecurity through its inherent design principles of mutual authentication, encryption, and robust data integrity measures. However, the dynamic nature of cyber threats in healthcare means continuous vigilance, updates to standards, and strong implementation practices are essential for maintaining a secure interoperable medical device ecosystem.

Big players such as Philips or Dräger involvement in the SDC adoption is a significant step towards wider deployment of ISO/IEEE 11073-SDC.

So, rather than waiting for "cybersecurity tools to be included in a hospital deployment," it's more accurate to say that:

- The fundamental security mechanisms are part of the SDC standard and are implemented within the SDC stacks and integration kits provided by companies or

Funded by Horizon Europe Framework Programme of the European Union

developed internally, even most of the actual medical devices today in the market are not yet SDC compliant

- **The focus is on effective implementation and ongoing management:** The challenge isn't the *availability* of security features in the standard, but rather ensuring that manufacturers correctly implement them, that healthcare organizations manage the associated infrastructure (like certificate authorities and trust stores), and that systems are continuously monitored and updated against emerging threats.
- **Future "cybersecurity tools" will likely focus on orchestration, automation, and advanced threat detection:** As SDC implementations mature and become more widespread, we can expect to see:
    - **Centralized security management platforms:** Tools for managing certificates, access policies, and security configurations across a large fleet of SDC-enabled devices.
    - **Automated vulnerability scanning and penetration testing tools specifically for SDC environments.**
    - **AI/ML-driven anomaly detection and threat intelligence for SDC networks:** Systems that can identify unusual behaviour indicative of a cyberattack.
    - **Integration with broader hospital cybersecurity frameworks:** Tools that bridge the gap between medical device cybersecurity and the hospital's overall IT security posture.

In essence, the foundation for cybersecurity in SDC is already laid within the standard itself and its associated implementation of toolboxes. The ongoing evolution will likely see more sophisticated, specialized tools for *managing, monitoring, and responding to* cybersecurity threats within the SDC ecosystem, rather than adding new security protocols to the core communication. These will be crucial for scaling SDC adoption securely in complex clinical environments.

4.3 Telemedicine at home

For telemonitoring at home, MDCG 2019-16 emphasizes cybersecurity measures to protect patient data and ensure the integrity of medical devices used remotely. It recommends that medical devices should use encrypted communication channels to protect sensitive health data from unauthorized access. Patients and healthcare providers should use strong authentication methods to access telemonitoring systems, preventing unauthorized use. Devices should receive timely security patches to address vulnerabilities and maintain system integrity. Patients and healthcare professionals should be educated on cybersecurity best practices, such as cyber hygiene, preventing and recognizing phishing attempts and securing home networks. Healthcare providers should have systems in place to detect and respond to cybersecurity threats affecting telemonitoring devices.

Integration of CYLCOMED tools in Connected Medical Devices for remote cardiological patients' monitoring

Based on insights from the pilot phase and the interviews conducted with the hospital stakeholders, the following recommendations have been proposed to enhance the cybersecurity guidance in hospital environments:

Recommendation

Funded by Horizon Europe Framework Programme of the European Union

Strengthening the protection of clinical data: the top priority in terms of cybersecurity is the protection of electronic health records (EHRs), as they contain highly sensitive and personally identifiable health information (an additional difficulty is that EHRs are typically not under MDR). In this context, the implementation of advanced encryption methods becomes essential, not just to shield the data from external threats, but also to ensure that, if intercepted, the information remains unreadable and secure. Additionally, the use of multi-factor authentication is seen as a fundamental layer of defence, helping to control and restrict access only to authorized personnel. This is particularly relevant in scenarios involving remote patient monitoring through CMDs involved in the CYLCOMED project, where data flows continuously and must maintain its integrity throughout transmission and storage. Ensuring that this information remains accurate and unaltered is just as important as protecting it from unauthorized access.

Recommendation

Use of pseudo-anonymization techniques: MDCG 2019-16 does not specifically address the safe and responsible use of pseudo-anonymized datasets, which represents a fundamental point for the Ethical Committee for the proper conduction of the CYLCOMED Clinical Trial. The guidance mainly focuses on securing real patient data, with little mention of how to properly implement and govern anonymized data in the healthcare ecosystem. This gap highlights the need for updated frameworks or additional recommendations that can guide the safe application of these techniques, ensuring both privacy and compliance with data protection laws.

Recommendation

Automated Log collection and analysis: in case of data breach, hospitals often lack the ability to reconstruct events within the GDPR's 72-hour reporting window. Therefore, MDCG guidance should include specific requirements for continuous logging, timestamping, and accessibility to system logs. The expected impact would be increased transparency and improved incident response capability

Recommendation

Patch management and continuous updates are critical aspects of maintaining cybersecurity in CMDs. However, lots of legacy devices are notoriously difficult to update, which can leave persistent vulnerabilities in systems that manage or transmit sensitive patient data. Establishing clear minimum requirements to support timely and secure updates is therefore essential, especially in healthcare environments where infrastructure may not be easily modernized. In this context, training and awareness programs become equally vital. As updates and cybersecurity protocols evolve, similarly must be the

Funded by Horizon Europe Framework Programme of the European Union

knowledge of end-users. In the case of CYLCOMED, training initiatives that can exploit also the use of practical simulations, are fundamental not only to raise awareness of potential cybersecurity threats affecting hospital IT systems and CMDs, but also to ensure that staff are fully equipped to implement and respond to ongoing system changes. Without continuous education alongside technical updates, even the most advanced security measures may fall short of practice

Recommendation

Rapid incident response protocols: the current guidance generally refers to incident detection and response plan; however, it doesn't highlight a specific predefined time and response of action in case of incident. In the hospital scenario where the CYLCOMED system is deployed, having cross-functional teams in place to manage cybersecurity incidents appears fundamental. Rather than relying solely on IT or technical staff, a heterogeneous approach that brings together professionals from legal, clinical, technical, and even ethical backgrounds must be put in place. This kind of interdisciplinary coordination ensures that incident response is not only swift and technically sound but also aligned with patient safety, regulatory requirements, and institutional values

Recommendation

Integration with existing SIEM system: the current guidance does not consider integration of the system with the SIEM system already in place in the hospitals. However, CMDs and telemonitoring software should produce structured logs compatible with SIEM systems to enable centralized event monitoring. Thus, with the CYLCOMED system integration, the expected impact is the enhancement of efficiency in detecting and responding to cybersecurity incidents.

Recommendation

Ease of use and intuitive design: an often overlooked but essential aspect of guidance for implementing systems like CYLCOMED is ease of use. Security must go hand in hand with simple, intuitive design, especially for routine actions like logging in. If systems are too complex or inconsistent, users may bypass procedures, increasing risk. On the other hand, user-friendly interfaces encourage proper use of security measures, helping to protect data and support smooth operations, especially in high-pressure environment like hospitals

Funded by Horizon Europe Framework Programme of the European Union

4.4 Telemonitoring in vehicles

MDCG 2019-16 does not specifically address cybersecurity recommendations for emergency vehicles, but its general principles for medical devices and healthcare infrastructure can still apply. For emergency medical services (EMS), cybersecurity measures should focus on Secure Communication Systems, ensuring encrypted and protected data transmission between emergency vehicles and hospitals. Access to medical devices and patient data within ambulances must be restricted to authorized personnel.

Onboard medical equipment must be updated to prevent cybersecurity vulnerabilities. Real-time monitoring systems must be implemented to detect and respond to potential cyber threats. Emergency responders must be educated on cybersecurity best practices to prevent data breaches.

Funded by Horizon Europe Framework Programme of the European Union

5 Technological trends

5.1 AI in Connected Medical Devices

About half of AI-enabled medical devices had clinical performance studies reported at the time of approval, according to a recent cross-sectional study [9]. However, the data was frequently insufficient for a thorough evaluation of the devices' clinical generalisability, highlighting the necessity of continuous monitoring and frequent re-evaluation to spot and address unforeseen performance changes during wider use.

After being approved for clinical usage, artificial intelligence (AI)-enabled medical devices must be continuously monitored and regularly re-evaluated to detect and rectify any unanticipated changes in their performance when they are implemented in larger clinical settings. To prevent bias and guarantee accurate findings across various populations and clinical scenarios, it is also crucial to make sure that AI models are trained using representative and varied datasets.

To ensure the safety and clinical effectiveness of medical devices with AI capabilities, regulatory agencies must constantly modify their regulatory frameworks. This entails creating uniform procedures for post-market monitoring as well as encouraging accountability and transparency. The safe and ethical use of AI in clinical practice depends on cooperation between industry, academics, and regulators. Special attention should be paid to providing medical practitioners with the necessary training so they can keep an eye on how well these devices are doing in real-world situations.

Recommendation
Artificial intelligence in medical devices introduces new cybersecurity challenges that should be addressed in the guide.

5.2 5G networks

5G is not just "faster 4G." Its core characteristics directly benefit connected medical devices:

- **Enhanced Mobile Broadband (eMBB):** Enables high-data-rate applications like real-time transmission of high-resolution medical imaging (MRI, CT scans) and telesurgery.
- **Ultra-Reliable Low-Latency Communications (URLLC):** Critical for time-sensitive applications such as remote patient monitoring (RPM) for critical conditions, robotic surgery, and emergency response systems.
- **Massive Machine-Type Communications (mMTC):** Supports a vast ecosystem of sensors and wearable devices (e.g., ECG patches, glucose monitors) within a hospital or city.

While these benefits are transformative, they expand the attack surface and introduce new risks that must be proactively managed.

Funded by Horizon Europe Framework Programme of the European Union

5.2.1 Key Cybersecurity Challenges & Threat Vectors Specific to 5G

A. Network Architecture & Virtualization Risks:

- **Software-Defined Networking (SDN) & Network Function Virtualization (NFV):** 5G core networks are software-based. This introduces new attack surfaces in the form of hypervisors, orchestration platforms, and virtual network functions. A compromise here could disrupt entire segments of medical services.
- **Network Slicing:** While a security feature (isolating traffic), misconfiguration of network slices is a major risk. An attacker gaining access to the orchestration system could reconfigure or breach the slice intended for critical medical devices, potentially mixing it with public, less-secure traffic.
- **Edge Computing (MEC):** Processing data closer to the devices reduces latency but decentralizes security. Each Multi-access Edge Computing (MEC) node becomes a new, physically accessible target that must be hardened, as it may handle sensitive, unencrypted patient data.

B. Supply Chain & Multi-Tenancy Risks:

- **Complex Supply Chain:** 5G infrastructure involves multiple vendors for hardware, software, and cloud services. A vulnerability in any component (e.g., a baseband chip, a virtualized network function) can propagate through the entire ecosystem supporting medical devices.
- **Multi-Tenancy:** 5G networks are shared resources. While isolation is a goal, sophisticated attacks could potentially lead to "side-channel" attacks or a "noisy neighbour" effect, where a compromised device on a public slice impacts the performance or security of a nearby medical slice.

C. Increased Attack Surface & Device Proliferation:

- **Massive IoT Scale:** The ability to connect thousands of devices per square kilometer makes asset management and inventory a monumental challenge. A single, vulnerable, low-power sensor can be a pivot point for an attacker to move laterally towards more critical systems.
- **Device Diversity:** Medical devices run on a variety of often outdated operating systems and have long lifecycles (10-15 years). Ensuring all these devices can securely authenticate and communicate on a 5G network is difficult.

D. Identity and Access Management (IAM) Challenges:

- **New Authentication Frameworks:** 5G introduces new protocols like 5G-AKA and EAP-AKA'. While more secure than previous generations, flawed implementations in medical devices or carrier networks could be exploited.
- **Subscriber Permanent Identifier (SUPI) Protection:** The SUPI is a unique, permanent identifier for a device (like an IMSI). 5G mandates its encryption as the Subscription Concealed Identifier (SUCI) to prevent tracking and spoofing. However, the strength of this protection depends on the underlying public key infrastructure (PKI), which could be a target.

E. Availability & Denial-of-Service (DoS) Risks:

- **Critical Dependence:** As healthcare becomes reliant on always-on 5G connectivity for life-critical functions, any network outage—whether from a technical fault, a natural disaster, or a targeted DDoS attack—becomes a direct threat to patient safety.
- **New DoS Vectors:** The signalling storm attacks seen in 4G could be amplified in 5G due to the sheer number of connected devices.

Funded by Horizon Europe Framework Programme of the European Union

5.2.2 Essential Security Considerations & Mitigation Strategies

A. For Medical Device Manufacturers (OEMs):

- **Security by Design:** Integrate security from the initial design phase, following principles like "zero trust."
- **Hardened Device Identity:** Implement secure, hardware-based roots of trust (e.g., TPM, Secure Element) to store credentials and handle the encryption of the SUCI. Ensure devices support the latest 5G security features.
- **Secure Lifecycle Management:** Plan for secure firmware/software Over-The-Air (OTA) updates for the entire device lifecycle. Have a clear vulnerability management and patch deployment policy.
- **Data Protection:** Encrypt sensitive patient data **end-to-end** (E2EE), not just between the device and the network. The device or a trusted gateway should be the endpoint for encryption, not the carrier's tower.

B. For Healthcare Providers (Hospitals, Clinics):

- **Comprehensive Risk Assessment:** Conduct specific threat modelling for 5G-connected medical systems. Understand the impact of network slice failure, MEC node compromise, or service degradation.
- **Robust Network Segmentation:** Work with your Mobile Network Operator (MNO) to design and strictly enforce **private network slices** for medical devices. Isolate critical devices (e.g., ventilators, infusion pumps) from non-critical ones (e.g., patient entertainment).
- **Vigilant Monitoring & Inventory:** Deploy network monitoring solutions that understand 5G protocols and can detect anomalies in device behaviour or network traffic. Maintain a **real-time, accurate inventory** of all 5G-connected assets.
- **Vendor Management:** Include stringent 5G security requirements in procurement contracts. Demand transparency about the device's 5G security features and its software bill of materials (SBOM).

C. For Mobile Network Operators (MNOs) & Integrators:

- **Secure Slice Isolation:** Guarantee the integrity and isolation of network slices for healthcare customers through robust configuration management and continuous auditing.
- **MEC Security:** Harden MEC nodes with strict access controls, intrusion detection systems, and physical security measures.
- **Transparency and SLAs:** Provide healthcare providers with clear visibility into their slice performance and security events. Service Level Agreements (SLAs) must include security metrics, not just uptime.

5.2.3 Conclusion

5G is a powerful enabler for the next generation of connected healthcare, offering speed, reliability, and scale. However, its software-defined, distributed nature introduces a new and complex threat landscape. A shared responsibility model is essential. **Security cannot be an afterthought;** it must be a collaborative, proactive effort between device manufacturers, healthcare providers, and network operators to ensure that patient safety and data integrity are never compromised.

.

Recommendation

Funded by Horizon Europe Framework Programme of the European Union

By understanding these unique considerations and implementing a defence-in-depth strategy that spans the device, the network, and the cloud, the healthcare industry can securely harness the transformative power of 5G

5.3 Cloud computing

5.3.1 Introduction: The Cloud as the Core Platform

Cloud computing is the engine that makes large-scale IoMT deployments feasible and valuable. It provides:

1. **Scalable Data Storage & Analytics:** Centralizes vast amounts of data from millions of devices for population health analysis, predictive analytics, and machine learning.
2. **Global Accessibility & Interoperability:** Enables clinicians to access patient data from anywhere and facilitates data sharing between different healthcare systems (EHRs, labs, etc.).
3. **Orchestration and Management:** Provides the platforms for managing device fleets, deploying over-the-air (OTA) updates, and monitoring device health.

This centralization of critical functions and sensitive data makes the cloud a high-value target, shifting the security paradigm from protecting a network perimeter to protecting a dynamic, shared environment.

5.3.2 Key Cybersecurity Challenges & Threat Vectors in the Cloud

A. Shared Responsibility Model Confusion:

- **The #1 Cloud Risk:** A widespread and dangerous misconception is that the cloud provider (AWS, Azure, Google Cloud) is responsible for *all* security. Security is a **shared responsibility**.
    - **Cloud Provider Responsibility:** Security *of* the cloud (physical infrastructure, hypervisor, core network services).
    - **Customer Responsibility:** Security *in* the cloud (data classification, access management, application security, patient data encryption, secure configuration of services).
- **Impact:** Misconfiguration of customer-controlled settings is the leading cause of cloud data breaches (e.g., publicly exposed storage buckets, unsecured databases).

B. Identity and Access Management (IAM) Complexity:

- **Privilege Escalation:** Overly permissive user and service accounts can be exploited by attackers to gain unauthorized access to sensitive data or to manipulate device controls.
- **Secret Management:** Hard-coding API keys and passwords into device firmware or application code is a common critical failure. These secrets can be easily extracted and abused.

Funded by Horizon Europe Framework Programme of the European Union

- **Lack of Zero Trust:** Not enforcing the principle of "never trust, always verify" for every access request, regardless of source (inside or outside the network).

C. Data Sovereignty, Privacy, and Protection:

- **Data in Transit and at Rest:** Data must be encrypted end-to-end, from the device to the cloud application. Data at rest in cloud storage must also be encrypted by default.
- **Data Residency:** Healthcare regulations (like GDPR) may require that patient data is stored and processed within specific geographic boundaries. Cloud architectures must be designed to comply with these laws.
- **Data Lifecycle Management:** Lack of policies for securely archiving and destroying patient data when it is no longer needed.

D. Increased Attack Surface via APIs:

- **Cloud-native Communication:** Cloud services and applications communicate extensively via APIs. These APIs, if not properly secured (authenticated, authorized, and throttled), become a primary vector for data exfiltration, account takeover, and DDoS attacks.

E. Visibility and Logging Challenges:

- **Lack of Centralized Monitoring:** Without a dedicated Cloud Security Posture Management (CSPM) tool and a Security Information and Event Management (SIEM) system integrated with cloud logs, it is impossible to detect misconfigurations or malicious activity in real-time.
- **"Shadow IT":** The ease of spinning up new cloud services can lead to unvetted and unmanaged resources (shadow IT) that fall outside the purview of the security team.

5.3.3 Essential Security Considerations & Mitigation Strategies

A. Foundational: Mastering the Shared Responsibility Model

- **Formalize Ownership:** Clearly document and internalize the division of security responsibilities between your organization and your cloud provider(s).
- **Leverage Cloud-Native Security Services:** Use the tools provided by the cloud platform (e.g., AWS Security Hub, Azure Security Center, Google Cloud Security Command Center) for continuous monitoring and compliance checking.

B. Identity and Access Management (IAM)

1. **Principle of Least Privilege:** Grant users and services the minimum permissions they need to perform their tasks. Conduct regular access reviews.
2. **Enforce Multi-Factor Authentication (MFA):** Mandate MFA for all human users, especially administrators.
3. **Implement Zero Trust Network Access (ZTNA):** Replace traditional VPNs with ZTNA solutions that verify identity and context before granting access to applications.
4. **Secure Secrets Management:** Use dedicated services (e.g., AWS Secrets Manager, Azure Key Vault) to manage, rotate, and retrieve API keys, passwords, and certificates—never store them in code.

Funded by Horizon Europe Framework Programme of the European Union

C. Data Protection

1. **Encrypt Everything by Default:** Ensure all Protected Health Information (PHI) is encrypted both in transit (using TLS 1.2+) and at rest. Prefer cloud services that offer and default to encryption.
2. **Manage Your Own Keys:** For highly sensitive data, consider using Customer-Managed Keys (CMKs) instead of the cloud provider's default key management, giving you full control over the encryption keys.
3. **Classify Data:** Tag and classify data based on sensitivity (e.g., PHI, public, internal) to apply appropriate security policies.

D. DevSecOps and Secure Deployment

1. **Infrastructure as Code (IaC) Security:** Use tools (e.g., Terraform, CloudFormation) to define and version your cloud infrastructure. Scan IaC templates for security misconfigurations *before* deployment.
2. **Secure API Gateways:** Use managed API gateways to enforce authentication, authorization, rate limiting, and logging for all API traffic.
3. **Vulnerability Management:** Integrate static (SAST) and dynamic (DAST) application security testing into your CI/CD pipeline to find and fix vulnerabilities in your custom applications before they reach production.

E. Proactive Monitoring and Incident Response

1. **Enable Comprehensive Logging:** Ensure all relevant logs are collected and centralized.
2. **Implement a Cloud SIEM:** Use a SIEM to correlate logs and set up alerts for suspicious activity (e.g., anomalous logins from unusual locations, large data downloads).
3. **Develop a Cloud-Specific IR Plan:** Your incident response plan must account for the cloud shared responsibility model. Practice how you would isolate a compromised cloud workload and what your cloud provider's role would be in the investigation.

5.3.4 Conclusion

Cloud computing provides the agility, scale, and intelligence that modern connected healthcare requires. However, it demands a fundamentally different security approach centred on **identity, data, and resilient architecture**.

Recommendation
For medical device manufacturers and healthcare providers, mastering the shared responsibility model and implementing a proactive, "secure-by-design" cloud strategy is not optional—it is a critical component of patient safety and regulatory compliance. The security of the device, and the cloud platform must be designed as a single, integrated system.

Funded by Horizon Europe Framework Programme of the European Union

5.4 Blockchain

5.4.1 Key Cybersecurity Challenges & Limitations of Blockchain

A. The Data On-Chain Problem:

- **Data Exposure:** A common misconception is that blockchain automatically means encryption. Data written to a *public* blockchain is typically visible to all participants. Storing Protected Health Information (PHI) directly on-chain would violate privacy laws like HIPAA.
- **Immutability vs. The "Right to be Forgotten":** Regulations like GDPR grant individuals the "right to erasure." The immutable nature of blockchain directly conflicts with this principle. You cannot simply "delete" a record from a blockchain.
- **Storage Cost and Scalability:** Storing large amounts of data (e.g., firmware files, high-resolution medical images) directly on-chain is prohibitively expensive and slow. Blockchains are designed for ledger data, not bulk storage.

B. Private vs. Public Blockchain Dilemma:

- **Public Blockchains (e.g., Ethereum):**
  - *Pros:* Truly decentralized, highly resilient to censorship.
  - *Cons:* Performance is slow, transaction costs can be high, and data visibility is public (unsuitable for PHI).
- **Private/Permissioned Blockchains (e.g., Hyperledger Fabric):**
  - *Pros:* Access is controlled, performance is faster, and data visibility can be restricted to authorized participants (e.g., a consortium of hospitals, manufacturers, and regulators). This is the **only viable model for healthcare PHI**.
  - *Cons:* Introduces a degree of centralization. The consortium members become the trusted authorities, which partially negates the "decentralized trust" benefit.

C. Smart Contract Risks:

- **Code is Law:** Smart contracts are immutable programs that run on the blockchain. If a smart contract governing a device update or a data-sharing agreement contains a bug, it cannot be patched easily. A flawed contract could lock funds, share data incorrectly, or halt critical processes.
- **Vulnerability to Exploitation:** Smart contracts have been notoriously hacked due to coding errors (e.g., re-entrancy attacks, integer overflows). Their security is only as good as the code and the audit it has undergone.

D. Key Management - A Single Point of Failure:

- **User-Controlled Keys:** In most blockchain systems, users control their own private keys, which are their digital identity. **There is no "Forgot Password" feature.**
- **Irreversible Loss:** If a hospital loses the private key for a device identity wallet, they permanently lose access to the data and functions controlled by that identity. There is no central admin to reset it.
- **Theft:** If a private key is stolen, an attacker can impersonate the device or organization with no recourse.

E. Integration and Oracle Challenges:

Funded by Horizon Europe Framework Programme of the European Union

- **The Oracle Problem:** Blockchains are sealed systems. They cannot natively access external data. "Oracles" are services that feed external data (e.g., a device's sensor reading, a lab result) onto the blockchain.
- **Oracle as a Weak Link:** If the oracle is compromised or provides faulty data, the blockchain will faithfully record and execute based on that incorrect data. **Garbage in, immutable garbage out.**

5.4.2 Potential Use Cases and Mitigation Strategies

A. Appropriate Use Cases:

1. **Secure Device Identity and Provenance:** Create a tamper-proof record of a device's manufacturing, shipping, and ownership history. This helps combat counterfeit devices.
2. **Audit Trail for Data Access:** Record every instance of who accessed patient data from a device, when, and for what purpose. The log itself is immutable and verifiable.
3. **Consent Management:** Use smart contracts to manage patient consent for data sharing, allowing patients to see a transparent record of who their data has been shared with.
4. **Research and Integrity:** Hash research data from clinical trials and store the hash on-chain. This provides a timestamped, immutable proof that the data existed in that exact form at a specific time, preventing scientific fraud.

B. Essential Security Mitigations:

1. **Store Hashes, Not Data: This is the most critical pattern.** Do not store PHI on-chain. Instead, store the cryptographically hashed "fingerprint" of the data. The actual data is stored securely off-chain (e.g., in a traditional, HIPAA-compliant cloud database). The hash on-chain serves as a tamper-proof seal, verifying the data's integrity.
2. **Rigorous Smart Contract Auditing:** Any smart contract used in a medical context must undergo multiple, professional security audits before deployment. Treat this code with the same gravity as the firmware on a life-critical device.
3. **Robust Key Management Solutions:** Implement enterprise-grade Hardware Security Modules (HSMs) or secure key management services to generate, store, and manage private keys, preventing loss and theft.
4. **Use Permissioned Blockchains:** For any use case involving PHI or regulated processes, a private/permissioned blockchain is the only architecturally sound choice.
5. **Secure Oracle Design:** Use decentralized oracle networks that pull data from multiple sources to reduce the risk of a single point of failure or manipulation.

5.4.3 Conclusion: A Specialized Tool, not a Magic Bullet

Blockchain is a powerful technology for creating **verifiable trust and integrity** in multi-party, adversarial, or low-trust environments. However, it is computationally expensive, complex, and introduces new unique risks, particularly around key management and smart contracts.

Recommendation
For connected medical devices, blockchain should be considered a specialized component of a larger security architecture, not the architecture itself. Its best use

Funded by Horizon Europe Framework Programme of the European Union

is as an immutable notary service for critical metadata, audit logs, and provenance information—not as a replacement for databases, secure communication protocols (like TLS), or cloud computing.

Recommendation

Before choosing blockchain, ask: **"Is my problem fundamentally about creating a verifiable, tamper-proof record of events or transactions between entities that do not fully trust each other?"** If the answer is yes, then blockchain may be a viable solution. If not, a traditional centralized or cloud-based solution is likely more efficient, secure, and manageable. In fact, we have not identified any medical devices connected project using blockchain, double check before introducing the blockchain technology that it is providing value to your project

Funded by Horizon Europe Framework Programme of the European Union

Conclusion

The CYLCOMED project has demonstrated that cybersecurity in the context of connected medical devices is a highly complex matter, involving a wide range of stakeholders, including IT personnel, clinicians, software developers, and security officers.

Recommendation
It is recommended that the MDCG guidelines provide guidance on how to use its guidelines, i.e. provide guidance on different stakeholders use of the guidelines, especially providing entry points, and sequences of operations that index the guidance from the MDCG.

Recommendation
Clearly delineate responsibilities among manufacturers, integrators, operators, and regulators

Connecting medical devices includes different components, mainly:

- The medical devices
- The networks where the medical devices are connected
- The software to capture and process the measurements from the medical devices (CIS, PDMS)
- The EHR (and probably other hospital systems) that need to be integrated in the solution

The critical point here is that while medical devices are under the MDR and IVDR regulations, CIS and PDMS are usually not, and the EHR is, in general, are not under the MDR.

Recommendation
Keeping track of connected medical devices is a must. As a summary of chapter 3 recommendations for the medical devices inventory, it should include: • Medical device model • Manufacturer • Serial number • SW version • Protected menus and its passwords

Recommendation
The MDCG guide covers the medical devices under the MDR/IVDR regulations, but there are many more critical components from the cybersecurity perspective that should be considered when connecting medical devices. MDCG should include all those

Funded by Horizon Europe Framework Programme of the European Union

components, or a more general cybersecurity guide for connecting medical devices should be created

Funded by Horizon Europe Framework Programme of the European Union

Bibliography

[1] Steve Taylor et al., 'A Way Forward for the MDCG 2019-16 Medical Device Security Guidance', https://doi.org/10.1145/3652037.366389

[2] Christos Androutsos et al., 'MDCG 2019-16 Guidelines: Case Study-Based Assessment and Path Forward', https://doi.org/10.1007/978-3-031-94855-8_22

[3] J. I. Muñoz-Bonet *et al.*, 'Exploring the clinical relevance of vital signs statistical calculations from a new-generation clinical information system', *Sci Rep*, vol. 13, no. 1, p. 15068, Sep. 2023, doi: 10.1038/s41598-023-40769-3. https://www.nature.com/articles/s41598-023-40769-3/figures/3

[4] E. Biasin and E. Kamenjasevic, 'Cybersecurity of Medical Devices: Regulatory Challenges in the European Union', in *The Future of Medical Device Regulation*, 1st ed., I. G. Cohen, T. Minssen, W. N. Price Ii, C. Robertson, and C. Shachar, Eds., Cambridge University Press, 2022, pp. 51–62. doi: 10.1017/9781108975452.005.

[5] 'Guidance - MDCG endorsed documents and other guidance - European Commission'. Accessed: Jan. 03, 2025. [Online]. Available: https://health.ec.europa.eu/document/download/b23b362f-8a56-434c-922a-5b3ca4d0a7a1_en?filename=md_cybersecurity_en.pdf

[6] Vallor, Shanon, 'An Introduction to Cybersecurity Ethics'. [Online]. Available: https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf

[7] Milojevic, Dusko, 'Is it time to update the Medical Device Coordination Group's Guidance on Cybersecurity for Medical Devices?' [Online]. Available: https://www.law.kuleuven.be/citip/blog/is-it-time-to-update-the-medical-device-coordination-groups-guidance-on-cybersecurity-for-medical-devices/

[8] Christos Androutsos, Steve Taylor, Karin Bernsmed, Andrea Neverdal Skytterholm, Gregory Epiphaniou, Nabil Moukafih, Theodoros N. Arvanitis, Sotiris Messinis, Nikos Papadakis, Marco Fruscione, Andrés Castillo, Dusko Milojevic, Dimitrios S. Karas, Nikolaos Fotos, Max Ostermann, Oscar Freyer, Stephen Gilbert, Vasilis Pezoulas, Lambros Athanasiou, George Gkois, Dimitrios I. Fotiadis, 'MDCG 2019-16 Guidelines: Case Study-Based Assessment and Path Forward', *Communications in Computer and Information Science*, doi: https://doi.org/10.1007/978-3-031-94855-8_22.

[9] Windecker D, Baj G, Shiri I, et al. Generalizability of FDA-Approved AI-Enabled Medical Devices for Clinical Use. *JAMA Netw Open.* 2025;8(4):e258052. doi:10.1001/jamanetworkopen.2025.8052

Funded by Horizon Europe Framework Programme of the European Union