MDCG 2019-16 Guidelines: Case Study-based Assessment and Path Forward

Christos Androutsos[1], Steve Taylor[2], Karin Bernsmed[3], Andrea Neverdal Skytterholm[3], Gregory Epiphaniou[4], Nabil Moukafih[4], Theodoros N. Arvanitis[5], Sotiris Messinis[6], Nikos Papadakis[7], Marco Fruscione[8], Andrés Castillo[9], Dusko Milojevic[10], Dimitrios S. Karas[11], Nikolaos Fotos[11], Max Ostermann[12], Oscar Freyer[12], Stephen Gilbert[12], Vasilis Pezoulas[1], Lambros Athanasiou[1], George Gkois[1], and Dimitrios I. Fotiadis[1,13]

[1] University of Ioannina, Ioannina, Greece
[2] University of Southampton, Southampton, United Kingdom
[3] SINTEF Digital, Trondheim, Norway
[4] University of Warwick, Coventry, United Kingdom
[5] University of Birmingham, Birmingham, United Kingdom
[6] Institute of Communication and Computer Systems, Athens, Greece
[7] SPACE Hellas, Athens, Greece
[8] EBIT, Genoa, Italy
[9] Fundación Para La Investigación Biomédica Hospital Infantil Universitario Niño Jesús, Madrid, Spain
[10] KU Leuven, Leuven, Belgium
[11] UBITECH Ltd., Athens, Greece
[12] Dresden University of Technology, Dresden, Germany
[13] Biomedical Research Institute, FORTH, Ioannina, Greece

Abstract. The Medical Device Coordination Group (MDCG) 2019-16 guidelines provide a structured framework for cybersecurity in Connected Medical Devices (CMDs) throughout their lifecycle, offering guidance on how to fulfil all the relevant essential requirements outlined in Annex I of both the Medical Device Regulation (MDR) and the In Vitro Diagnostic Medical Devices Regulation (IVDR). This paper evaluates the practical applicability and limitations of these guidelines based on feedback from six Horizon Europe (HEU) projects. Each project employed case studies reflecting diverse CMD environments and operational contexts to assess the guidelines' relevance and effectiveness in real-words scenarios. The paper identifies gaps in the practical application of the guidelines and explores their impact on different stages of the CMD lifecycle, from design and development to deployment and post-market activities. Based on these findings, the paper proposes targeted recommendations aimed at enhancing the usability and effectiveness of the MDCG 2019-16 guidelines. The insights contribute to the ongoing evolution of cybersecurity practices in medical technology, ensuring the guidelines are better aligned with the needs of CMD stakeholders, including manufacturers, integrators, and operators, while supporting the development of more resilient and secure medical devices.

Keywords: Medical Device Coordination Group · Cybersecurity · Medical Devices.

1 Introduction

1.1 Overview of the MDCG 2019-16 guidelines

The MDCG 2019-16 guidelines [1] provide a structured approach to integrating cybersecurity measures across the lifecycle of CMDs. Recognizing the increasing complexity of CMDs and their vulnerabilities to cyber threats, the guidelines aim to support manufacturers, integrators, and operators in mitigating risks while ensuring compliance with regulatory frameworks, such as the MDR and IVDR. The guidelines emphasize a risk-based approach, requiring stakeholders to assess and address cybersecurity risks at every stage of a device's lifecycle, from design and development to deployment and post-market surveillance. Key measures outlined in the guidelines include preventing unauthorized access to sensitive medical data, safeguarding data from unauthorized modifications and ensuring continuous functionality of medical devices. The guidelines also advocate for the adoption of a defense-in-depth strategy, which involves implementing layered security measures to mitigate potential cybersecurity threats. They provide detailed requirements for device manufacturers, integrators, and operators, making them highly relevant to the diverse CMD scenarios of use.

1.2 Objectives

The primary objective of this paper is to evaluate the practical application of the MDCG 2019-16 guidelines in the context of CMDs by utilizing insights gathered from six collaborative HEU projects: NEMECYS, MEDSECURANCE, SEPTON, CYLCOMED, ENTRUST, and CYMEDSEC, which share the common objective. A first attempt at this collaboration provided some initial recommendations for the MDCG 2019-16 guidelines showcasing existing gaps regarding the applicability and assessment of the guidelines [2]. In this paper, these results are extended by utilizing real-world case studies, to assess the guidelines' relevance, practicality, and alignment with the cybersecurity needs of CMDs. By focusing on stakeholder feedback across diverse device types and operational settings, the paper contributes unique evidence-based recommendations for improving MDCG utility in future revisions. The aim is to identify gaps, particularly in addressing the complexities of cybersecurity within real-world contexts and to provide recommendations, ensuring their clarity and effectiveness for medical device manufacturers, integrators, and operators. Consolidating feedback from the six projects, the paper offers a unified perspective on the strengths and limitations of the guidelines. The paper is structured as follows: Section 2 presents the methodology for feedback collection. Sections 3 through 8 describe the case study contexts, identified gaps, and corresponding recommendations from each of the six Horizon Europe projects: NEMECYS, MEDSECURANCE, SEPTON, CYLCOMED, ENTRUST, and CYMEDSEC. Finally, Section 9 concludes the paper and outlines directions for future work.

2 Methodologies for Feedback Collection

To systematically evaluate the applicability and relevance of the guidelines in real-world CMD scenarios, a structured and collaborative methodology was employed by the NEMECYS and SEPTON projects. This process ensured a detailed, scenario-driven assessment of the guidelines across the case studies and provided actionable feedback for their refinement. A structured feedback framework was designed to enable a consistent and in-depth review of the MDCG 2019-16 guidelines. Each guideline was assigned a unique identifier to enable traceability and simplify reference across the project's documentation and discussions. To reflect the multi-layered approach required to protect CMDs against cybersecurity risks, the guidelines were categorized based on the principles of defense-in-depth security strategies. The guidelines were further broken down into IT related subcategories, such as basic principles and general security requirements for operating environments. Alignment with the MDR was highlighted, providing stakeholders with specific requirements the guidelines aim to address. Each guideline was outlined in detail, ensuring case studies had the full text for review and analysis. Initial observations and assessments were then gathered to provide actionable insights into the practical application of the guidelines.

The process followed by the MEDSECURANCE project for identifying gaps in the MDCG guidelines involved a structured approach engaging stakeholders and case studies. Feedback was collected through collaborative workshops, and structured templates focusing on practical challenges stakeholders face when striving to comply with these standards. The process also includes testing the tools developed within the project against three case studies. These tests were designed to evaluate the tools' effectiveness in securing medical devices and Internet of Medical Things (IoMT) systems under scenarios that simulate actual healthcare environments. The observational data collected from these tests capture where the tools successfully mitigate risks and where they fall short, specifically in areas not adequately covered by current MDCG guidelines. This direct comparison and data collection help pinpoint precise gaps in the guidelines, highlighting areas for potential enhancement and to better address contemporary cybersecurity challenges in healthcare.

In the CYLCOMED project it was argued whether the guidelines outlined in Section 2.6 of the MDCG "Joint Responsibility - Specific expectations from other stakeholders" may eventually be examined to develop a novel method to enhance cybersecurity for a CMD intended for use in hospitals. Active participation from a broad range of stakeholders including clinicians, nurses, IT staff, patients, and administrators facilitated in-depth discussions on the potential implications of implementing the MDCG 2019-16 guidelines, focusing on how the guidelines may affect daily clinical operations and overall patient care. The pilot validation process involved comparing stakeholder experiences before and after testing the CYLCOMED dashboard with real patients, aimed to identify areas for the refinement of practical guidelines applicable to both new and existing cutting-edge technologies. An important part of this process involved semi-structured interviews, conducted in two distinct stages. The first stage gathered insights on

stakeholder expectations and concerns prior to system's deployment. The second stage captured feedback on the dashboard's performance highlighting any challenges encountered, and benefits realized. These interviews were conducted by experts including cybersecurity specialists, clinical engineers, and data protection officers with a focus on MDCG guidelines based on cybersecurity, ethics, clinical workflows, and compliance.

The initial set of recommendations from the ENTRUST project focused on addressing the absence of a clearly defined Vulnerability Management process, as outlined in Section 2.4 of MDCG 2019-16 guidelines. This was achieved through the design and implementation of a Trust Assessment Framework (TAF) for ensuring that the trustworthiness level of CMDs remains at an acceptable level throughout their operational lifecycle. To this end, a core dimension of the ENTRUST methodology entailed the construction of the threat landscape affecting each medical domain application represented by the use case demonstrators. Thus, a top-to-bottom methodology was applied, beginning with the Top 10 Mobile Risks identified by the Open Worldwide Application Security Project (OWASP) [3] as a generic list of threats and vulnerabilities applicable across domains. To refine this into domain-specific lists, questionnaires were distributed to the case studies to obtain the following information: (i) description of practical, real-world threat scenarios, (ii) correspondence with OWASP threats, and (iii) countermeasures and types of trustworthiness evidence to be monitored to support the safety and security controls for the mitigation of those threats.

As the CYMEDSEC project is still in its early stages the analysis is based on literature reported real-world vulnerabilities and the most impactful Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) [4], rather than in-project de novo collected data from case studies. This data was analyzed in the context of the requirements of MDCG 2019-16 guidelines and the FDA cybersecurity guidance. These requirements were mapped against the developed baseline to identify areas of alignment, partial coverage, or gaps. The vulnerabilities in the previously identified real-world incidents from the Cybersecurity and Infrastructure Security Agency (CISA) database were analyzed to determine whether adherence to the guidance would mitigate vulnerabilities. The coverage of thematic areas was assessed and inconsistencies identified. This mapping allowed regulatory deficiencies and gaps to be identified and the formulation of recommendations to improve the regulations.

3 NEMECYS

3.1 Case Studies

NEMECYS employs four distinct case studies representing diverse device types, operational settings, and cybersecurity challenges, ensuring a multimodal evaluation across a range of CMD scenarios. The case studies analyzed in this evaluation are as follows:

1. Re:Balans patch sensor [5]: A non-invasive wearable sensor device that measures hydration levels in patients with fluid management-related health conditions, such as patients with end-stage renal disease requiring dialysis. The device collects real-time data and wirelessly transmits them to an external unit such as a smart tablet or IoT gateway for remote patient monitoring.
2. PDMonitor [6]: An IoT wearable medical device designed for the continuous monitoring of Parkinson's Disease (PD) patients both in home and hospital settings, through an approach that spans the device's design, development, and operational phases.
3. Diabetes management mobile application: A Class IIb Software as a Medical Device (SaMD) mobile application that assists people with diabetes to correctly manage their therapy [7]. This application provides optimized advice for bolus and basal insulin doses, adjusted according to entries related to meals, blood glucose and other relevant information provided by the patient.
4. Freestyle Libre 2 Continuous Glucose Monitoring (CGM) kit [8]: An in-vitro diagnostic device consisting of a glucose monitor worn on the patient's upper arm to continuously measure glucose levels, a reader used both at home and hospital to scan the sensor and display glucose values and a web-based application for healthcare professionals to access patient data [9].

3.2 Gaps and Recommendations

The evaluation of the MDCG 2019-16 guidelines in the NEMECYS case studies covered multiple dimensions and identified several gaps that hinder their practical application in CMDs. In response to these gaps, targeted recommendations were provided to enhance the guidelines' effectiveness in addressing real-world cybersecurity needs. Both the identified gaps and corresponding recommendations are summarized in Table 1.

Table 1. Gaps and recommendations across NEMECYS case studies.

Category	Gaps	Case Study	Importance	Recommendations
Guidance Completeness	The guidelines do not effectively provide extensive guidance on fulfilling all the relevant requirements for Annex I of the MDR, leaving stakeholders with incomplete support.	1	Without clear MDR alignment, manufacturers face uncertainly compile MDR technical file and get a CE mark.	- Restructure the guidelines into a more straightforward, practical document tailored to manufacturers seeking MDR compliance and CE marking. - Provide detailed descriptions for labeling, instructions for use (IFU) requirements, training protocols, and usability validation processes.
Terminology Clarity	Fail to clearly differentiate between cybersecurity, security, and safety, creating confusion. Key terms such as "layered defense" and "good security hygiene" are undefined.	1-4	Ambiguous terminology complicates secure device design, particularly for wearable and IoT devices where layered security is essential.	- Draw upon established frameworks, such as the FDA Post market Management of Cybersecurity in Medical Devices, FDA Cybersecurity in Medical Devices Guidance, ISO 14971, and AAMI/TIR57, to enhance the clarity and applicability of the guidelines. - Clear terms should be provided regarding tools and standards to be used in threat modeling techniques, such as recommended tools.

Category	Gaps	Case Study	Importance	Recommendations
Risk Management Framework	Reasonably foreseeable misuse is not defined according to ISO 14971 and AAMI TIR57:2016. No specific cybersecurity examples are provided to illustrate risk mitigation strategies.	1,3	As part of risk management, manufacturers must identify and assess potential vulnerabilities that could be exploited, including those arising from reasonably foreseeable misuse of the device.	- Include requirements for comprehensive risk assessments of use case scenarios, implementation of mitigation measures and controls. - Clearly define key terms, such as "reasonably foreseeable misuse," based on recognized standards like ISO 14971 and AAMI/TIR57:2016. Provide documentation on general best practices in risk management.
Stakeholder Responsibilities	The term "integrator" is undefined, and explicit requirements for manufacturers such as the purpose of integration, technical requirements, environmental requirements, verification plan, installation and servicing, and training requirements, are missing. The distinction between "operator" and "user" is also unclear.	1-4	The manufacturer is responsible for safety and effectiveness, and these requirements should be explicitly stated by the MDCG.	- Clearly delineate responsibilities among manufacturers, integrators, operators, and regulators. - Develop a categorized list of common security requirements to assist manufacturers in drafting effective requirements documents.
Defense-in-Depth Strategy	Limited and overly generic guidance on integrating, configuring, and maintaining a defense-in-depth strategy.	1,2	Guidance should be provided to address requirements related to technical descriptions, or rational processes/assessments that the manufacturer needs to implement to achieve a secure design.	- Incorporate practical examples and scenarios to clarify concepts like "layered defense," "depth approach," and "good security hygiene" within medical device cybersecurity contexts. - Provide detailed descriptions, including technical specifications, rational processes, and assessments manufacturers must implement for secure design. - Explicitly state requirements for addressing generic security-related threats, including detailed specifications on when specific security capabilities are needed and what devices or scenarios are relevant.
Verification & Validation (V & V)	Too brief, lacking actionable recommendations, reporting templates, and guidance on testing methodologies.	3	Insufficient V&V guidance hinders the systematic testing and validation of software in medical devices and mobile health applications.	- Offer examples of verification and validation testing, along with best practices for addressing various cybersecurity threats. - Specific templates for reporting verification and validation results should be emphasized.
Safety vs. Security	The guidelines do not clarify the distinction between safety and security in risk management processes, leading to potential overlaps or gaps in mitigation strategies.	1,2,3	Inadequate distinction may lead to overlooked cybersecurity threats that could compromise patient safety in continuous monitoring devices.	- Establish "safety, security, and effectiveness" requirements as concrete outcomes of a systematic design and risk management process. - 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. - 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.
Risk Re-evaluation Frequency	The guidelines do not specify how often security and safety risks should be reassessed or provide measures to manage evolving risks effectively.	3	Without specified risk reevaluation intervals, devices may remain exposed to emerging threats, especially in rapidly evolving healthcare technology landscapes.	-
Post-Market Surveillance	-	1	-	Emphasize post-market cybersecurity maintenance procedures, including protocols for support, maintenance, and anticipated security degradations over time.

4 MEDSECURANCE

4.1 Case Studies

MEDSECURANCE focuses on the enhancement of security-for-safety assurances within the IoMT. With an initial focus on healthcare IT systems, the project explores the intersection of clinical benefits and security vulnerabilities. Through the development of innovative methodologies, infrastructures, and technologies, MEDSECURANCE seeks to advance secure system engineering management activities, addressing the evolving complexity of IoMT. To identify gaps in the MDCG guidelines, MEDSECURANCE focuses on three case studies:

1. Remote Patient Monitoring (RPM) system: This case study evaluates the secure transmission of patient data over networks, highlighting the project's capability to ensure data integrity and confidentiality against cyber threats.
2. Portable Polymerase Chain Reaction (PCR) Testing: This case study focuses on security challenges in diverse environmental conditions, particularly in field settings where the risk of unauthorized access and data breaches could compromise both patient confidentiality and integrity of test result.
3. Virtual Ward: This case study simulates a hospital ward environment managed remotely using a network of CMDs and IT systems.

4.2 Gaps and Recommendations

The evaluation of the MDCG 2019-16 guidelines in the MEDSECURANCE case studies covered multiple dimensions and identified several gaps that hinder their practical application in CMDs. In response to these gaps, targeted recommendations were provided to enhance the guidelines' effectiveness in addressing real-world cybersecurity needs. Both the identified gaps and corresponding recommendations are summarized in Table 2.

Table 2. Gaps and recommendations across MEDSECURANCE case studies.

Category	Gaps	Case Study	Importance	Recommendations
Specific IoMT Security Considerations	The guidelines focus predominantly on the software components of medical devices without considering the broader spectrum of IoMT system vulnerabilities.	1	These systems feature a diverse array of device types and connectivity options, each introducing distinct security challenges that include heterogeneity in device functionality, varied data privacy requirements, and increased exposure to cyberattacks.	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.
IoMT Risk Management	While the guidelines advocate for rigorous risk management, they lack detailed protocols for the unique risk landscape of IoMT systems.	1,2,3	IoMT devices not only enhance healthcare delivery but also expand the potential attack surface due to their interconnected nature.	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.

Category	Gaps	Case Study	Importance	Recommendations
Secure Software Development Lifecycle (SDLC) for IoMT	The guidelines currently touch on software development practices but do not provide an extensive framework for the secure SDLC applicable to IoMT.	2	Given the complexity and the critical nature of IoMT applications, embedding security at each phase of the software development process—from design to deployment and beyond—is vital.	The inclusion of IoMT-specific secure coding practices, threat modelling, and continuous testing within the guidelines would help ensure that IoMT software upholds the highest security standards.
Data Privacy and Consent in IoMT	-	1,2,3	-	- The guidelines should be broadened to include comprehensive strategies for data privacy management, including data consent, data minimisation, and secure data storage and transmission protocols. - Aligning these strategies with general data protection regulations (e.g., GDPR) will further ensure that IoMT systems are not only secure but also respect patient privacy.
Vulnerability and Incident Response for IoMT	Current guidelines offer little detail on managing vulnerabilities and responding to incidents within IoMT frameworks.	1,2,3	IoMT systems routinely handle sensitive health data, making them prime targets for breaches.	- Clear and detailed process for ongoing vulnerability assessment, regular updates, and patch management. - Establish standardised incident response procedures for IoMT can expedite containment and mitigation efforts, minimising the impact of security breaches.
Software Validation and Verification	-	2	-	Enhance validation and verification processes for higher-risk software categories.

5 SEPTON

5.1 Case Studies

The SEPTON project includes four distinct case studies each addressing critical cybersecurity challenges in CMDs, ensuring robust protection and data security across various medical environments. The case studies analyzed in this evaluation are as follws:

1. Implantable Medical Devices (IMDs): This case study focuses on IMDs designed for real-time seizure suppression utilizing prerecorded electrocorticogram data to detect and stop seizures before they manifest. The IMD also securely transmits data, including seizure events and treatment information, to a smartphone acting as a reader.
2. Wearable Medical Devices: This case study focuses on wearable medical devices in various configurations to support RPM. These devices collect health metrics and transmit them through gateways, such as smartphones, to hospital or cloud systems.
3. Hospital Infrastructure Security: This case study focuses on the security of critical devices such as Magnetic Resonance Imaging (MRI) scanners, Picture Archiving and Communication System (PACS) servers, and imaging modalities.
4. Distributed Healthcare Infrastructures: This case study explores secure data sharing utilizng blockchain technology to create an immutable and transpar-

ent ledger for all interactions, while decentralized storage solutions like IPFS [10] ensure efficient and secure data distribution.

5.2 Gaps and Recommendations

The evaluation of the MDCG 2019-16 guidelines in the SEPTON case studies covered multiple dimensions and identified several gaps that hinder their practical application in CMDs. In response to these gaps, targeted recommendations were provided to enhance the guidelines' effectiveness in addressing real-world cybersecurity needs. Both the identified gaps and corresponding recommendations are summarized in Table 3.

Table 3. Gaps and recommendations Across SEPTON Case Studies.

Category	Gaps	Case Study	Importance	Recommendations
Portable/Remote Medical devices	The guidelines do not explicitly address the unique risks of devices that remain in a patient for extended periods without direct manufacturer access.	1,2	Missing updates could lead to long-term security vulnerabilities affecting patient health. A lack of direct manufacturer access increases risks of cyber intrusions.	Introduce specific protocols for secure over-the-air updates to minimize the need for invasive procedures.
Third-Party Mobile Platforms & Software Security	The guidelines do not sufficiently address the risks associated with devices that rely on third-party mobile platforms for patching. No structured framework for evaluating and mitigating third-party security risks, despite many hospital devices depending on vendor-supplied or integrated software components.	1,2,3	Dependence on third-party apps may delay critical security patches.	- Establish minimum security requirements for mobile platforms used in conjunction with medical wearables. - Ensure that security patches are validated by the manufacturer before distribution to prevent unauthorized tampering.
Healthcare Data Protection	The guidelines do not clearly define practices for protecting data when shared across different healthcare institutions, especially in cases with varying regulations.	1-4	Vital for regulatory compliance and patient confidentiality. Weak data protection could expose sensitive medical records. Insecure transmission could lead to unauthorized access.	- Introduce standardized cybersecurity measures for securing cross-institutional data sharing. - Mandate the use of secure transmission protocols, such as FHIR over TLS 1.3, to protect Electronic Health Records (EHR) and real-time data.
International Data Governance	Although GDPR compliance is acknowledged, there is no in-depth discussion on data sovereignty and governance challenges when medical information is exchanged internationally.	4	Unclear governance policies may lead to compliance violations, legal challenges, and potential security breaches when transferring medical records between jurisdictions.	Expand security requirements to account for personal use environments, recognizing the additional risks associated with compromised personal devices compared to hospital-controlled settings.
Interoperability & Secure Data Transmission	Insufficient coverage of interoperability and secure transmission standards such as FHIR, DICOM, or HL7, creating vulnerabilities in data structuring and protection.	3-4	Inconsistent interoperability standards risk data loss or corruption. Insecure transmission protocols may expose patient records to cyber threats.	Mandate structured vendor security assessments before software integration, ensuring that third-party components comply with strict cybersecurity requirements.
Safety vs. Security	The guidelines do not clarify the distinction between safety and security in risk management processes, leading to potential overlaps or gaps in mitigation strategies.	1-4	Inadequate distinction may lead to overlooked cybersecurity threats that could compromise patient safety in continuous monitoring devices.	- Introduce stronger network security requirements, particularly mandating strict network segmentation to separate critical medical devices from general hospital IT systems. - Establish minimum cybersecurity baselines for legacy devices, including firewall-based isolation, Virtual Local Area Network (VLAN) segmentation, and role-based access controls.
Post-market Surveillance	-	1-4	-	Enhance post-market surveillance frameworks to include long-term cybersecurity monitoring, incorporating proactive vulnerability assessments and periodic risk analysis to identify emerging threats throughout the device's lifespan.

6 CYLCOMED

6.1 Case Studies

The introduction of pilots within the CYLCOMED project is a crucial tactic to actively involve end-users and gain a deeper understanding of the challenges associated with integrating cutting-edge technologies in healthcare scenarios as follows:

1. Hospital Equipment: Although there are no clinical trials planned for the first pilot related to hospital equipment, collaboration with the Hospital Niño Jesús of Madrid [11] ensures valuable feedback to support the improvement of tools under evaluation.
2. Telemedicine Implementation in Hospital Environments: In this case study end-users from Hospitals Bambino Gesù of Rome [12], Charité of Berlin [13], and Hospital Niño Jesús of Madrid [11] actively contribute with their experiential insights, which are seamlessly integrated into the definition of the clinical protocol and the formulation of the patient journey, guaranteeing an in-depth approach to technology implementation.

6.2 Gaps and Recommendations

The evaluation of the MDCG 2019-16 guidelines in the CYLCOMED case studies covered multiple dimensions and identified several gaps that hinder their practical application in CMDs. In response to these gaps, targeted recommendations were provided to enhance the guidelines' effectiveness in addressing real-world cybersecurity needs. Both the identified gaps and corresponding recommendations are summarized in Table 4.

Table 4. Gaps and recommendations across CYLCOMED case studies

Category	Gaps	Case Study	Importance	Recommendations
Lack of Terminological Coherence	Does not include explicit definitions or references to terms such as "cybersecurity", "security-by-design", and "security-by-default".	1,2	Leaving these terms theoretical and undefined present challenges for stakeholders seeking to implement practical cybersecurity measures effectively.	Key concepts like 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.
Legal ambiguity and uncertainty	Briefly mentions the intersection of the cybersecurity legal frameworks without providing recommendations on addressing the potential simultaneous applicability of these frameworks, such as notification obligations. Moreover, the medical device cybersecurity landscape is a dynamic field that has undergone significant changes since the MDCG guidance endorsement in 2019.	1,2	Proper guidance is essential to facilitate compliance with various legal requirements scattered across various regulations.	- The MDCG guidelines could clarify the interplay between the MDR and other cybersecurity frameworks. - To enhance the cybersecurity of medical devices, the guidelines should be updated to clarify how different regulatory frameworks, such as GDPR, NIS2, AI Act, and MDR, intersect.
Lack of Acknowledgement of Human Factors in Cybersecurity	Hints at addressing cybersecurity challenges to other stakeholders in the medical device supply chains (e.g., integrators and operators). The concept of "joint responsibility" lacks clarity and remains open to different interpretations. MDCG Guidance fails to acknowledge that humans are frequently portrayed as the weakest link in the cybersecurity chain [14].	1,2	Integrating a human-centric approach and providing more guidance would enhance the capability to prevent and mitigate cyber threats and raise overall awareness.	Providing more insights and guidance for other stakeholders would be essential to mitigate cybersecurity risks.

7 ENTRUST

7.1 Case Studies

The ENTRUST project evaluates the effectiveness of trust assessment controls across four real-world medical application scenarios:

1. KardinBLU ECG [15] and multi-parameter monitoring system: A Bluetooth Low Energy device that collects and transmits cardiological data, SpO_2 levels, and temperature either to a gateway device, which forwards them to a desktop computer, or to a mobile device, which forwards them to the hospital.
2. Tellu Personal Health Gateway (PHG) [16] : This case study focuses on an RPM system where the gateway receives vital health parameters from CMDS in home settings and transmits them to the Tellucare cloud-based eHealth platform for medical use.
3. Patient Care in Hospital Domains: This case study enhances patient care in hospital domains through two demonstrators, the smart ambulance where CMDs transmit real-time data during patient transport and the emergency care unit, which focuses on maintining the integrity and trustworthiness of the legacy CMDs, such as the Econet Compact 7 [17] in hospital environments.
4. Feel Emotion Sensor (FES) [18]: This case study explores the precision biomarkers and digital therapeutics in mental health care using this wearable device that collects data, such as sweat, heartbeat, and skin temperature.

7.2 Gaps and Recommendations

The evaluation of the MDCG 2019-16 guidelines in the ENTRUST case studies covered multiple dimensions and identified several gaps that hinder their practical application in CMDs. In response to these gaps, targeted recommendations were provided to enhance the guidelines' effectiveness in addressing real-world cybersecurity needs. Both the identified gaps and corresponding recommendations are summarized in Table 5.

Table 5. Gaps and recommendations across ENTRUST case studies

Category	Gaps	Case Study	Importance	Recommendations
Insufficient guidance on life-cycle security and post-market	The MDCG guidelines state that medical device manufacturers should be responsible for ensuring that risks associated with reasonably foreseeable environmental conditions are removed or minimized, while ENTRUST argues that dynamic runtime monitoring is required at the side of the domain for identifying and mitigating zero-day threats and vulnerabilities.	1,2,4	It is not realistic to expect manufacturers to be solely responsible for real-time monitoring of devices due to time and resource constraints, as well as domain-specific details.	- The definition of reasonably foreseeable misuse should be expanded in order to consider the opinion of both the manufacturer and the deployment domain (e.g., the domain administrator). - Provide frameworks for the continuous and dynamic trust assessment of devices deployed to a medical domain, enabling the identification of new threats and vulnerabilities and the enforcement of the appropriate mitigation measures.

Category	Gaps	Case Study	Importance	Recommendations
Real-world vulnerabilities	There is limited consideration for domain-specific threats and vulnerabilities, as well as prioritization of the most prominent ones that need to be patched or addressed in the context of specific application scenarios.	1,2,3	Vulnerabilities may arise from the interconnectivity between devices, thus domain-specific considerations are essential.	Introduce a top-to-bottom process for the definition of the do-main-specific threat landscape, starting from a generic list of most prominent threats and leading to its refinement and expansion based on infrastructure and domain information.
Insufficient consideration for addressing real-world and post-market issues	The MDCG guidelines highlight the need for manufacturer side device updates for the mitigation of identified vulnerabilities. However, ENTRUST argues that this may be insufficient (e.g., in cases where manufacturer updates are infrequent).	2,3	It should be feasible to deploy domain-specific updates in a secure manner to address zero-day vulnerabilities in a timely manner.	Introduce a process for securely updating devices to mitigate threats and vulnerabilities, considering the involvement of not only the manufacturer, but also the deployment domain.
Limited or too generic guidance on security measures	The MDCG guidelines dictates that the manufacturer should be responsible for addressing vulnerabilities that may arise from reasonably foreseeable misuse. However, ENTRUST argues that it is not possible to draw such an unambiguous distinction, thus necessitating the presence of runtime security measures.	1,2,4	The notion of reasonably foreseeable misuse cannot be solely defined by the manufacturer, as domain input is also needed.	- Introduce a process for securely updating devices to mitigate threats and vulnerabilities, considering the involvement of not only the manufacturer, but also the deployment domain. - Introduce a process for the identification of domain-specific trust sources to be used in the context of the trust assessment process, such as digital twins, anomaly detection and attestation mechanisms.

8 CYMEDSEC

8.1 Case Studies

The first results of case studies in CYMEDSEC compare the guidance of the MDCG guidelines with the cybersecurity guidance detailed in the FDA. Instead of focusing on individual case studies, CYMEDSEC analyses real-world vulnerabilities of CMDs, such as vitals monitors, medical syringe pumps, medical imaging stations etc. [4]. This analysis determines whether correct adherence to the current state of cybersecurity guidance should have successfully prevented the incidents from occurring and what risks cybersecurity incidents pose in the Hospital-at-Home [19, 20]. The theoretical analysis of both guidance documents also included an independent third checklist that we created as a baseline cybersecurity checklist, derived from recognized standards, such as NIST CSF2.0, IEC-81001-5, AAMI TIR 57 & BSI-03161 [21]. This was done to identify different levels of scope in the guidelines and to determine the level of coverage in different areas of cybersecurity.

8.2 Gaps and Recommendations

The analysis of real-world CVEs and CWEs in the CYMEDSEC project revealed gaps in both MDCG 2019-16 guidelines and FDA cybersecurity guidance, while targeted recommendations are proposed as provided in Table 6. The structure of this table differs from those presented for other projects due to the unique approach adopted in the evaluation of the MDCG 2019-16 guidelines. Instead of focusing on direct case study assessments, CYMEDSEC conducted a broader thematic analysis of cybersecurity challenges.

Table 6. Gaps and recommendations across CYMEDSEC case studies.

Category	Gaps	Recommendations
No actionable requirements	MDCG 2019-16 references security principles but does not provide concrete, actionable steps for mitigating specific vulnerabilities [22].	-
Inconsistent level of detail	Across the guidance documents, different levels of depth can be found. This can lead to confusion regarding requirements, potentially limiting the attention given to less detailed requirements.	- Clearly defining the depth and level of technical detail in the guidance document prevents confusion across requirements. - A consistent level of detail clearly sets expectations to the integrating and validating personnel.
SMART Standards	-	Implementation of SMART standards allows for enhanced accessibility of standards, enabling machine-automated checks, better readability and updatability.
Clear Nomenclature	-	Remaining consistent in nomenclature and redefining recommended principles prevents confusion and allows for easier adherence to the guidance.

9 Conclusions

This study involved an extensive evaluation of the MDCG 2019-16 guidelines, gathering insights from six HEU projects with contributions from medical device manufacturers, integrators, cybersecurity experts, regulatory professionals, healthcare providers, and IT specialists. Beyond the tabulated feedback, several shared themes emerged, such as the lack of clarity in role definitions, challenges in aligning cybersecurity measures with clinical safety, and the need for actionable guidance at implementation level. These insights highlight barriers that stakeholders face when translating the guidelines into practice, indicating opportunities for refinement of terminology and structure. The analysis covered a wide range of CMDs in various real-world applications, including wearable and implantable medical devices, RPM systems, hospital IT infrastructure and secure data-sharing platforms. These devices operate in heterogeneous environments, such as home healthcare, hospital networks, distributed healthcare infrastructures, and telemedicine systems, highlighting the diverse cybersecurity risks that must be addressed across different case studies. The identified gaps along with the recommendations are summarized in Table 7.

Table 7. Identified Gaps in the MDCG 2019-16 Guidelines

Category	Gaps	Recommendations	No. of Projects
Risk-Benefit Analysis	Lack of guidance on risk-benefit analysis, which is essential to support practitioners for trade off analysis in proportional cybersecurity without compromising the safety and effectiveness of CMDs.	Necessity for guidance on risk assessment and risk-benefit trade-offs.	4

Category	Gaps	Recommendations	No. of Projects
Whole-Lifecycle Security	Lack of guidance in whole-lifecycle security for medical devices, especially at operation time such as monitoring intrusions, vulnerabilities, frequency of risk re-assessment and managing risks	Guidance on full lifecycle support for secure device management, including intrusion detection, monitoring, dynamic risk assessment and controls such as secure patching.	4
Terminology and Definitions	Lack of clear and consistent definitions, with discrepancies between the MDCG guidelines and other regulatory standards creating uncertainty in implementation.	- Clear definitions of terms and resolution of definitional inconsistencies between MDCG and other relevant regulations. - Practical and actionable guidance for manufacturers towards MDR compliance and CE marking.	3
Post-Market Cybersecurity Maintenance	Lack of structured post-market monitoring, vulnerability assessments, and response measures.	Emphasize post-market cybersecurity maintenance procedures,	3
Domain-specifc Threats	Lack of guidance on domain-specific threats and vulnerabilities	Provide links to external checklists of common vulnerabilities, threats and mitigations.	3
Security vs. Safety Distinction	Lack of differentiation between security and safety in risk management, leading to potential conflicts.	Clarify how security and safety should be addressed separately within risk management strategies.	2
V & V Processes	Insufficient recommendations for verifying and validating cybersecurity measures in CMDs.	Enhance V & V processes offering examples foe addressing various cybersecurity threats.	1
Regulatory Navigation	Lack of guidance on navigating overlapping regulations and the need for regular MDCG updates to keep pace with evolving legal requirements.	Clarify how manufacturers can navigate the complex and evolving regulatory landscape.	1
Legacy Device Management	Lack of guidance for secure operation and management of legacy devices	Provide guidance on secure management of legacy unpatched devices	1
Secure Data Exchange	Lack of guidance on secure data exchange between institutions.	Establish secure data-sharing protocols and provide guidelines for protecting healthcare data across hea;healthcare institutions.	1
Human Factors in Cybersecurity	Insufficient guidance on operational security related to human factors.	Provide guidance on how to consider human factors in terms of human vulnerabilities and how to address them.	1

While this study provides an assessment of the MDCG 2019-16 guidelines, certain limitations should be acknowledged. The analysis relied on structured expert feedback and scenario-based evaluations, which may not fully capture the complexities of real-world regulatory compliance. Additionally, the findings were derived from specific case studies, and while they cover a broad spectrum of CMDs, expanding the scope to include more diverse environments and stakeholders could further enhance the generalizability of the results. The study recognizes the need to further explore how organizational, management, and operational practices in medical device administration influence cybersecurity. As a next step, this consultation process should continue by collecting additional feedback and may include comparative analysis with other international regulatory frameworks. Overall, the projects concluded that the MDCG guidelines are very useful and beneficial and that the main content of this paper is focused on a gap analysis in a spirit of constructive criticism with an honest intent to suggest potential improvements to make updates to the guidelines more beneficial.

References

1. MDCG 2019-16 - Guidance on Cybersecurity for medical devices. Document date: 06/01/2020 - Created by GROW.R.2.DIR - Last update: 22/06/2020. https://ec.europa.eu/docsroom/documents/41863
2. Taylor, S., Gilje Jaatun, M., Bernsmed, K., Androutsos, C., Frey, D., Favrin, S., ... & Katzis, K.: A Way Forward for the MDCG 2019-16 Medical Device Security Guidance. In: 17th International Conference on PErvasive Technologies Related to Assistive Environments, pp. 593-599. Association for Computing Machinery, (2024).
3. OWASP, https://owasp.org/www-project-mobile-top-10/2023-risks/, last accessed 2025/02/06
4. Mejía-Granda, C. M., Fernández-Alemán, J. L., Carrillo-de-Gea, J. M., & García-Berná, J. A.: Security vulnerabilities in healthcare: an analysis of medical devices and software. Medical & Biological Engineering & Computing 62(1), 257–273 (2024).
5. Mode Sensors AS Homepage, https://www.modesensors.com/, last accessed 2025/02/06
6. PD Neurotechnology Homepage, https://www.pdneurotechnology.com, last accessed 2025/02/06
7. Debiotech Homepage, https://www.debiotech.com, last accessed 06/02/05
8. FreeStyle Libre Homepage, https://www.freestyle.abbott/us-en/products/freestyle-libre-2.html, last accessed 2025/02/06
9. Ospedale San Raffaele Homepage, https://research.hsr.it/en/index.html, last accessed 2025/02/06
10. IPFS Homepage, https://ipfs.tech, last accessed 2025/02/06
11. Hospital Niño Jesús Homepage, https://www.comunidad.madrid/hospital/ninojesus/, last accessed 2025/02/06
12. Hospitals Bambino Gesù of Rome, https://www.ospedalebambinogesu.it, last accessed 2025/02/06
13. Charité of Berlin, https://claim.charite.de/en, last accessed 2025/02/06
14. Cartwright, A. J.: The elephant in the room: cybersecurity in healthcare. Journal of Clinical Monitoring and Computing 37(5), 1123-1132 (2023)
15. KARDINBLU project Homepage, https://www.kardinero.com.tr/english/news/tubitak-grant-for-our-kardinblu-project, last accessed 2025/02/06
16. Tellu Homepage, https://www.tellu.no/en/services/remote-patient-monitoring/, last accessed 2025/02/06
17. Eukon Homepage, https://www.eukon.it/products/compact-7/, last accessed 2025/02/06
18. Feel Homepage, https://rpm.feeltherapeutics.com, last accessed 2025/02/06
19. Gilbert, S., Ricciardi, F., Mehrali, T., & Patsakis, C.: Can we learn from an imagined ransomware attack on a hospital at home platform?. NPJ Digital Medicine 7(1), 65 (2024)
20. Ostermann, M., Freyer, O., Jahed, F., Rosenzweig, C., & Gilbert, S.: Cybersecurity in the Hospital at Home: Assessment of Patient Risks when using IoMT devices. Zenodo, (2024)
21. Ostermann, M., Gilbert, S., & Freyer, O.: Cybersecurity Requirements for Medical Devices in the EU and US - A Comparison and Gap Analysis. Zenodo, (2024)
22. Freyer, O., Jahed, F., Ostermann, M., Rosenzweig, C., Werner, P., & Gilbert, S.: Consideration of Cybersecurity Risks in the Benefit-Risk Analysis of Medical Devices: Scoping Review. Journal of Medical Internet Research 26, e65528 (2024)