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

Christos Androutsos, Vasilis Pezoulas, Lambros Athanasiou, George Gkois, and Dimitrios I. Fotiadis, University of Ioannina

Steve Taylor, University of Southampton

Karin Bernsmed, Andrea Neverdal Skytterholm, SINTEF Digital

Gregory Epiphaniou, Nabil Moukafih, University of Warwick

Theodoros N. Arvanitis, University of Birmingham

Sotiris Messinis, Institute of Communication and Computer Systems

Nikos Papadakis, SPACE Hellas

Marco Fruscione, EBIT

Andres Castillo, Fundación Para La Investigación Biomédica Hospital Infantil Universitario Niño Jesús

Duško Milojević, KU Leuven

Dimitrios S. Karras, Nikolaos Fotos, UBITECH Ltd.

Max Ostermann, Oscar Freyer, Stephen Gilbert, Dresden University of Technology

Dimitrios I. Fotiadis, Biomedical Research Institute

NEMECYS
New Medical Cybersecurity and design Solutions

CYLCOMED

MedSecurance
Advanced Security-for-safety Assurance for Medical IoT

SeptOn

Enlightened trust in governance
EnTrust

CYMEDSEC

EICC 2025, Rennes, 18-19 June 2025

NEMECYS
New Medical Cybersecurity and design Solutions

This project has received funding from the European Union HORIZON-HLTH-2022-IND-13-01

Background & Motivation

- Cybersecurity is a key requirement for ensuring the safety and performance of Connected Medical Devices (CMDs).
- The MDCG 2019-16 guidance is an essential document, but feedback from real-world CMD deployments has revealed practical gaps.
- There is a growing need for clarity, completeness, and practical support in implementing the guidance across diverse healthcare environments.

Funded by the European Union

Aim of the Work

- To perform a case study-based assessment of the MDCG 2019-16 guidelines for cybersecurity in CMDs.
- To identify implementation challenges and unmet needs based on structured case studies input.
- To provide constructive, evidence-based recommendations for improving future iterations of the MDCG 2019-16 guidance.

Funded by
the European Union

Our feedback to the MDCG is a joint effort

NEMECYS
New Medical Cybersecurity and design Solutions

https://nemecys.eu/

Septon

https://septon-project.eu/

CYLCOMED

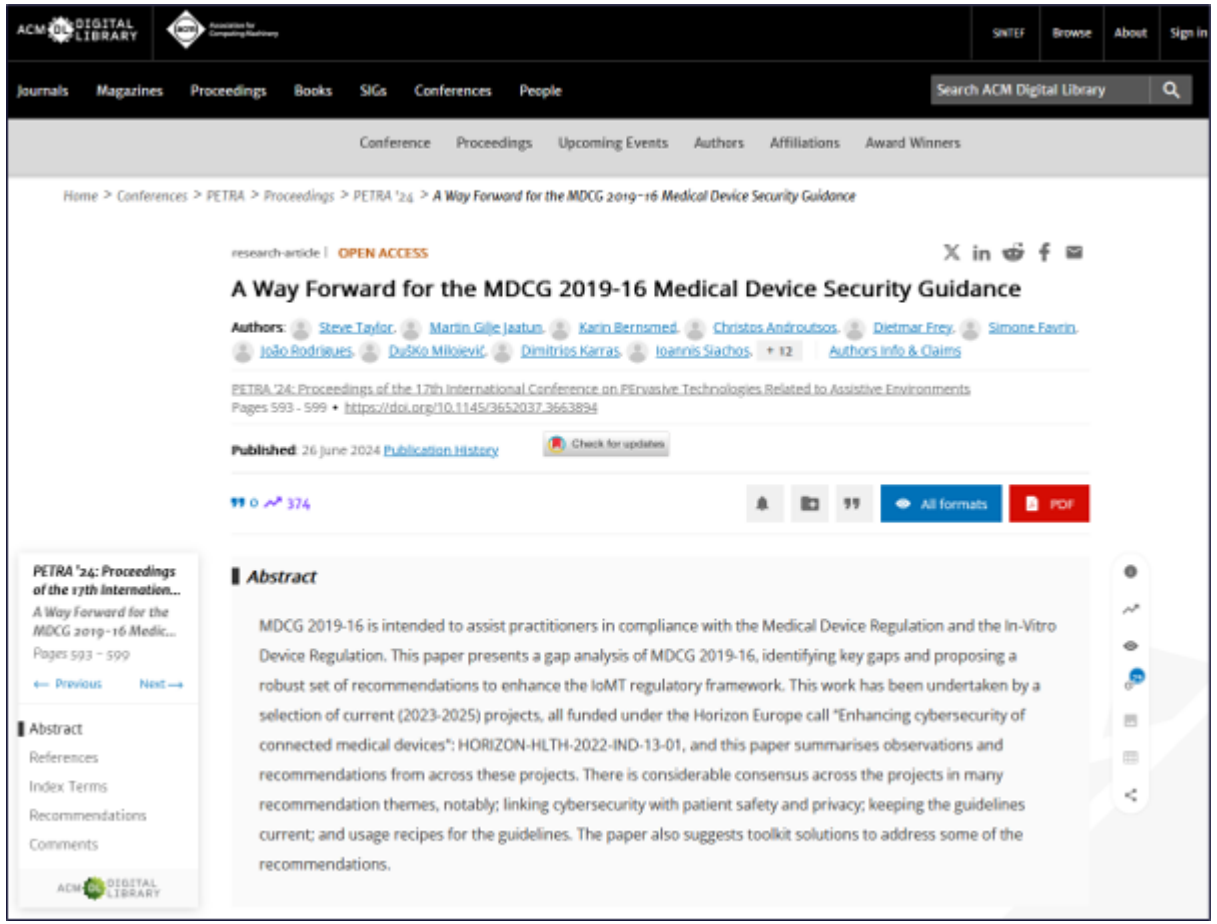
https://www.cylcomed.eu/

Enlightened trust in governance
EnTrust

https://entrust-project.eu/

MedSecurance
Advanced Security-for-safety Assurance for Medical IoT

https://www.medsecurance.org/



Taylor, S., Gilje Jaatun, M., Bernsmed, K., Androutsos, C., Frey, D., Favrin, S., ... & Katzis, K. (2024, June). A way forward for the MDCG 2019-16 medical device security guidance. In Proceedings of the 17th International Conference on PErvasive Technologies Related to Assistive Environments (pp. 593-599).

Funded by the European Union

Nemecys Case Studies

- **Re:Balans Patch Sensor:** A non-invasive wearable for hydration monitoring in dialysis patients, transmitting real-time data to external devices.
- **PDMonitor:** An IoT wearable for continuous monitoring of Parkinson's Disease across home and hospital settings.
- **Diabetes Management App:** A Class IIb mobile SaMD providing insulin dose advice based on patient input.
- **Freestyle Libre 2 CGM:** A continuous glucose monitoring kit integrating wearable sensors, readers, and web-based applications.

Funded by the European Union

SEPTON Case Studies

- **Implantable Medical Devices (IMDs):** Focus on seizure detection and secure data transmission to smartphones.
- **Wearable Devices for RPM:** Gathers health metrics and transmits them to cloud or hospital systems.
- **Hospital Infrastructure Security:** Includes PACS servers, MRI scanners, and critical imaging equipment.Distributed Health Systems: Uses blockchain and IPFS for secure, decentralized medical data sharing.

Funded by the European Union

MEDSECURANCE Case Studies

- **Remote Patient Monitoring (RPM):** Evaluates secure networked transmission of patient data.
- **Portable PCR Testing:** Addresses security in mobile testing under challenging field conditions.
- **Virtual Ward:** Simulates remote hospital ward management using CMDs and IT systems to evaluate integrated risk mitigation.

Funded by the European Union

CYLCOMED Case Studies

- **Hospital Equipment Pilot:** Collaboration with Hospital Niño Jesús to gather feedback on tool performance.
- **Telemedicine in Hospital Settings:** Active involvement of clinicians from hospitals in Rome, Berlin, and Madrid to validate tool usability and protocol alignment with real-world workflows.

Funded by the European Union

ENTRUST Case Studies

- **KardinBLU ECG Monitoring:** Multi-parameter Bluetooth system transmitting cardiological data via mobile or desktop devices.
- **Tellu Personal Health Gateway:** Gateway collecting home-based health data and transmitting it to a cloud-based eHealth platform.
- **Hospital Patient Care:** Demonstrators in smart ambulances and emergency units focus on CMD trustworthiness, especially for legacy systems.
- **Feel Emotion Sensor (FES):** A wearable used in digital mental health monitoring, capturing physiological data for biomarker analysis.

Funded by
the European Union

CYMEDSEC Case Studies

- **CMD Vulnerability Mapping:** Reviews incidents involving vital monitors, pumps, and imaging systems using CVEs and FDA reports.
- **Hospital-at-Home Risk Analysis:** Evaluates MDCG and FDA guidance for adequacy in home-based care settings.
- **Baseline Checklist Comparison:** Independent benchmark created from NIST CSF 2.0, IEC 81001-5, AAMI TIR57, and BSI-03161 to identify regulatory gaps and scope alignment.

Funded by the European Union

Methodology

A structured Excel-based template was designed to enable a consistent and in-depth review of the guidelines and included the following components:

07 - Feedback

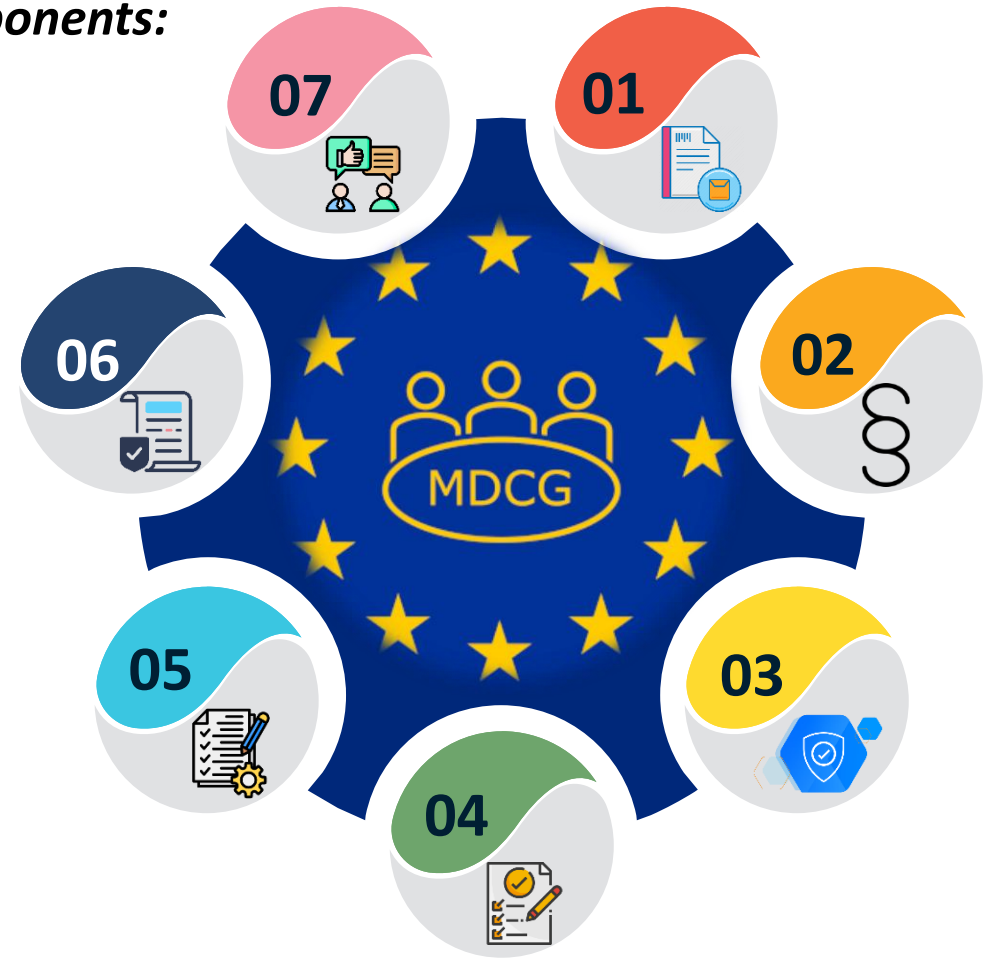
A field was included to collect observations and assessments from the case studies.

06 - Actual Guideline

Each guideline was outlined in detail, ensuring case study owners had the full text for review and analysis.

05 - MDR Requirements:

Alignment with key aspects of the Medical Device Regulation (MDR) was indicated, providing stakeholders with insights into the regulatory objectives the guidelines aim to address.



01 - Unique ID

Each guideline was assigned a unique identifier to enable traceability and simplify reference across the project's documentation and discussions.

02 - MDCG Section

The specific section of the MDCG 2019-16 guidelines from which each recommendation was derived, providing clarity and context for the reviewers.

03 - Defense-in-Depth Strategy

Specific guidelines were categorized based on the principles of defense-in-depth security strategies, reflecting the multi-layered approach required to protect CMDs against cybersecurity risks.

04 - IT Requirements Subcategory

Specific guidelines were further broken down into IT-related subcategories, such as basic principles and general security requirements for operating environments.

Funded by the European Union

Methodology

- Applied a structured stakeholder and case study approach using collaborative workshops and standardized templates.
- Identified MDCG gaps through observed tool limitations in mitigating practical risks.
- Stakeholder engagement in hospital settings through interviews with clinicians, IT staff, and data protection officers pre- and post-dashboard deployment.
- Focused on the impact of MDCG on clinical workflows, patient care, and ethical compliance.

Funded by the European Union

Methodology

- Developed a Trust Assessment Framework (TAF) as outlined in Section 2.4 (Vulnerability Management) of the MDCG 2019-16 guidelines.
- Refined threat lists and control strategies through use-case-specific questionnaires.
- Performed literature-based analysis of real-world Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) using Cybersecurity and Infrastructure Security Agency (CISA) and FDA sources to identify gaps and regulatory inconsistencies .
- Mapped existing cybersecurity incidents against MDCG 2019-16 and FDA guidance.

Funded by the European Union

NEMECYS
New Medical Cybersecurity and design Solutions

MDCG 2019-16 Gap Analysis

01 Guidance Completeness

02 Terminology Clarity and Stakeholders' Responsibilities

03 Risk Management Framework

04 Verification and Validation

05 Defense-in-Depth Strategy

06 Safety vs Security

07 Medical Device Lifecycle Security

08 Post-Market Cybersecurity Maintenance

09 Secure Data Exchange

10 Human Factors in Cybersecurity

Funded by the European Union

MDCG 2019-16 Recommendations

Guidance Completeness

Consider **restructuring the guidance into a clearer and more practical format** that better supports manufacturers aiming for MDR compliance and CE marking.

Suggest **adding more detailed descriptions** on labeling, instructions for use, training protocols and validation processes.

Suggest clarifying how overlapping regulatory frameworks including **GDPR[1], NIS2 Directive[2], AI Act[3], and MDR[4], intersect and apply** within CMD contexts.

Introduce a **process for identifying domain-specific trust sources (e.g., digital twins, anomaly detection, attestation) to support trust assessment** in CMD deployment environments.

Recommend **evaluating available tools and proposing a practical toolkit** to support implementation (e.g., threat modeling, verification, patching, monitoring).

Source Projects
NEMECYS
CYLCOMED
MEDSECURANCE
ENTRUST
CYMEDSEC
SEPTON

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
[2] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[3] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
[4] https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng

Funded by the European Union

MDCG 2019-16 Recommendations

Terminology Clarity and Stakeholders' Responsibilities

Suggest **referencing established frameworks (e.g.,** FDA Post market Management[1], FDA Cybersecurity in Medical Devices Guidance[2], ISO 14971[3], and AAMI TIR[4]) to enhance clarity.

Recommend **including a categorized list of common security requirements** to support manufacturers in drafting effective documentation.

Further clarity on the **distinctions** between **cybersecurity, security, and safety would enhance interpretation**, especially for wearable and IoT-based CMDs.

Definitions for cybersecurity terms such as **"layered defense" and "good security hygiene"** would **improve design consistency and stakeholder alignment.**

Propose incorporating **stakeholder-specific role guidance** for complex environments involving multiple actors (e.g., hospital-cloud systems, home-based monitoring)

Source Projects
NEMECYS
CYLCOMED
CYMEDSEC

[1] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices
[2] https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
[3] https://www.iso.org/standard/72704.html
[4] https://www.aami.org/detail-pages/product/aami-tir572016-r-2023-pdf-a152e000006j60wqaq

Funded by the European Union

MDCG 2019-16 Recommendations

Risk Management Framework

Include **requirements for detailed risk assessments** based on **real-world** use case scenarios, including the implementation of specific **mitigation measures and controls.**

Define **key terms, such as "reasonably foreseeable misuse"** in alignment with recognized standards like ISO 14971[1] and AAMI/TIR57:2016[2].

Provide documentation on **risk management best practices** and guidance on **performing risk-benefit trade-offs** where cybersecurity and clinical utility intersect.

Recommend a **tailored risk management approach for IoMT landscape**, including specific methodologies for assessing and mitigating risks.

Define a **top-down process to threat modeling**, beginning with general threats and adapting to specific infrastructure and domain-specific operational context.

Source Projects
NEMECYS
CYLCOMED
MEDSECURANCE
SEPTON
ENTRUST

[1] https://www.iso.org/standard/72704.html
[2] https://www.aami.org/detail-pages/product/aami-tir572016-r-2023-pdf-a152e000006j60wqaq

Funded by the European Union

MDCG 2019-16 Recommendations

Verification & Validation

Include **illustrative examples of verification and validation testing processes** applicable to cybersecurity in medical devices.

Emphasize the use of **standardized templates for documenting verification and validation results** to promote consistency across stakeholders.

Strengthen **validation and verification processes** for higher-risk software categories.

Incorporate consideration of **human factors** during verification and validation and **align verification efforts** with the Clinical Evaluation Plan and Clinical Evaluation Report.

Source Projects
NEMECYS
MEDSECURANCE

Funded by the European Union

MDCG 2019-16 Recommendations

Defense-in-Depth Strategy

Incorporate **practical examples and real-world scenarios** to clarify key concepts such as "layered defense," "depth approach," and "good security hygiene" within medical device cybersecurity contexts, **referencing certified technical ISO standards (e.g., ISO 27000 series)**

Provide **detailed descriptions**, including technical specifications, rational processes, and assessments that manufacturers should consider for **secure design.**

Explicitly **define requirements** for addressing **generic security-related threats**, with clear guidance on when specific security capabilities are necessary and how they apply to different device types and deployment contexts.

Source Projects
NEMECYS
CYLCOMED

Funded by the European Union

MDCG 2019-16 Recommendations

Safety vs Security

Establish **"safety, security, and effectiveness" requirements** as integrated and measurable outcomes of a **systematic design and risk management process.**

Clearly **explain** the **relationship** between **safety risk assessments** (as addressed by ISO 14971[1]) and **security risk assessments** (e.g., TIR57[2]), especially when **security risks impact safety** and require traceability

Explicitly include **functional and non-functional IT** security requirements, aligned with the general safety and performance expectations outlined in **Annex I of the MDR.**

Establish minimum **cybersecurity baselines for legacy devices.**

Source Projects
NEMECYS
SEPTON

Funded by the European Union

MDCG 2019-16 Recommendations

Medical Device Lifecycle Security

Include **IoMT-specific guidance** on secure coding practices, threat modeling, and continuous testing throughout the **software development lifecycle** to ensure robust cybersecurity for CMDs.

Define **minimum cybersecurity requirements** for mobile platforms that interface with medical wearables.

Emphasize the **need for manufacturer-validated security patches** to prevent unauthorized modifications or tampering during **deployment and maintenance phases.**

Source Projects
MEDSECURANCE
SEPTON

Funded by the European Union

MDCG 2019-16 Recommendations

Post-Market Cybersecurity Maintenance

Emphasize **structured post-market cybersecurity procedures**, including protocols for ongoing support, software maintenance, and mitigation of anticipated security degradation over time.

Define **clear processes** for vulnerability assessment, patch management, and regular security updates.

Introduce **specific protocols for secure over-the-air updates** to minimize the need for invasive procedures.

Provide **frameworks for dynamic trust assessment** in real-world deployment contexts, enabling the **identification of new threats and vulnerabilities** and the enforcement of the appropriate mitigation measures.

Source Projects
NEMECYS
MEDSECURANCE
SEPTON
ENTRUST

Funded by the European Union

MDCG 2019-16 Recommendations

Secure Data Exchange

Broaden the guidance to **include detailed strategies for data privacy management**, covering data consent, minimization, secure storage, and transmission protocols.

Introduce **standardized cybersecurity requirements for secure cross-institutional data sharing.**

Source Projects

MEDSECURANCE

SEPTON

Human Factors in Cybersecurity

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

Source Projects

CYLCOMED

Funded by the European Union

Conclusions

- The outcome of this evaluation reinforces the important role of the MDCG 2019-16 guidelines in supporting cybersecurity assurance for medical device stakeholders.
- Across the participating projects, there is broad consensus that the guidelines are both useful and beneficial.
- These recommendations were presented to the MDCG New Technologies Working Group in Brussels..
- As a follow-up, we were provided with the editable Word version of the MDCG 2019-16 guidelines (Rev.1) to directly integrate our feedback.

Funded by
the European Union

Thank you for your attention

NEMECYS
NEW MEDICAL CYBERSECURITY AND DESIGN SOLUTIONS

This project has received funding from the European Union
HORIZON-HLTH-2022-IND-13-01