NEMECYS

New Medical Cybersecurity and design Solutions

# Policy brief

## From Principles to Practice: Feedback on MDCG 2019-16

*December 2025*

Co-funded by the European Union

The NEMECYS project is co-funded by the European Union under grant agreement ID 101094323, by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee grant numbers 10065802, 10050933 and 10061304, and by the Swiss State Secretariat for Education, Research and Innovation (SERI). The information and views set out in this publication are those of the author(s) only and do not necessarily reflect those of the European Union, HADEA, UKRI or SERI. Neither the European Union nor the granting authorities can be held responsible for them.

## Setting the scene

The increasing complexity of **Connected Medical Devices** (CMDs) and their integration into digital healthcare systems has heightened the urgency for robust cybersecurity practices. To guide stakeholders in this domain, the Medical Device Coordination Group have issued the **MDCG 2019-16 guidelines**, titled "**Guidance on Cybersecurity for Medical Devices**", which outlines key expectations for ensuring cybersecurity throughout the lifecycle of medical devices. Despite being non-binding, these guidelines are now the most widely accepted framework for integrating cybersecurity into the lifecycle of CMDs in the EU and are considered essential for achieving compliance with the cybersecurity and safety requirements in EU's Medical Device Regulation (MDR 2017/745) and In Vitro Diagnostic Regulation (IVDR 2017/746).

Despite being widely used, experts and industry stakeholders have pointed out several limitations and challenges when applying the MDCG 2019-16 guidelines. This was observed by the European Health and Digital Executive Agency (HaDEA), which encouraged the projects funded under the Horizon Europe call "Enhancing cybersecurity of connected medical devices": HORIZON-HLTH-2022-IND-13-01 to analyse the practical usage of the guidelines in diverse CDM scenarios, and to provide recommendations for improvements. Consequently, the **NEMECYS projec**t (2023-2025) applied the guidelines in their **four different case studies** and evaluated their applicability and practical use. In this brief, we summarise the key findings and policy recommendations from the project. The aim is to provide constructive input aimed at enhancing the clarity, completeness, and usability for the next revision of the guidelines.

## Key findings

The evaluation of the practical application of the MDCG 2019-16 guidelines across the four case studies led to the identification of five recurring challenges.

- **Practical Applicability**. While the guidelines provide valuable high-level principles, they currently offer limited concrete implementation guidance, which may present challenges for manufacturers. The level of detail may not sufficiently support stakeholders in addressing all relevant requirements of Annex I of the MDR, potentially leading to gaps in compliance.
- **Terminology**. The guidelines do not explicitly distinguish between cybersecurity, security and safety, while other commonly used terms, such as "layered defence" and "good security hygiene" are left undefined. Roles, such as "integrator" and "operator", are not clearly defined. This may cause uncertainty in interpretation and confusion around responsibility allocation
- **Risk management**. The guidelines lack a clear methodology for balancing cybersecurity with clinical safety and device performance. They provide no examples of effective risk mitigation, offer limited clarity on integrating safety and security risk management, and omit reassessment frequency or measures for evolving threats. The distinction between safety and security within the risk management process is unclear, making it difficult for manufacturers to determine when and how cybersecurity risks should be incorporated into safety assessments. Additionally, the concept of reasonably foreseeable misuse is undefined and misaligned with standards such as ISO 14971:2019 and AAMI TIR57:2016.
- **Verification and validation**. The guidelines on verification and validation are (too) brief and lack actionable cybersecurity verification and validation recommendations, standardized reporting templates, and testing methodologies for CMDs and mobile health software.
- **Defence-in-depth**. The guidelines offer only high-level direction for implementing, configuring, and maintaining a defence-in-depth strategy. It lacks detailed technical steps, configuration guidance, and integration practices necessary for effective execution.

## Policy recommendations

To address the identified key challenges, the NEMECYS project puts forward the following policy 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 labelling, instructions for use, training protocols and validation processes.

- **Clarify terminology, roles and responsibilities.** Key cybersecurity concepts such as security-by-design, security-by-default, defence-in-depth, and good security hygiene should be clearly defined to ensure consistent interpretation across stakeholders. Terminology should be aligned with guidance frameworks such as Postmarket Management of Cybersecurity in Medical Devices, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, ISO 14971:2019, and AAMI TIR57:2016. The guidelines should clearly define and differentiate the roles and responsibilities of manufacturers, integrators, operators.

- **Enhance risk management and threat modelling.** Include requirements for detailed risk assessments based on real-world use case scenarios, including the implementation of specific mitigation measures and controls. Key terms, such as "reasonably foreseeable misuse" should be defined, in alignment with relevant documentation such as ISO 14971:2019 and AAMI TIR57:2016. References on risk management, and best practices and guidance on performing risk-benefit analysis should be provided. A tailored, structured risk management approach for IoMT landscape is needed, including specific methodologies for assessing, prioritising and mitigating risks. A top-adapting to specific infrastructure and domain-specific operational context.

- **Verification & validation.** Include illustrative examples of verification and validation activities applicable to cybersecurity in medical devices. Establishment of verification and validation plans, methods and acceptance criteria. Emphasize the use of standardized processes and templates for documenting verification and validation results to promote consistency across stakeholders.

- **Defence-in-depth.** Incorporate practical examples and real-world scenarios to clarify key concepts such as "layered defence", "depth approach," and "good security hygiene" within medical device cybersecurity contexts, referencing technical ISO standards (e.g., ISO 27000 series). Additionally, offer guidance on creating detailed descriptions, technical specifications, standard processes, and assessments that manufacturers should incorporate to ensure secure design. Finally, 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.

- **Post-market surveillance.** Emphasize structured post-market cybersecurity procedures for gathering user experience information, in order to develop protocols for ongoing support, software maintenance, and mitigation of anticipated security degradation over time.

These recommendations have already been presented to the MDCG New Technologies (NET) Working Group during the spring of 2025, leading to further collaboration, including the submission of suggestions from the project on the draft revision of the MDCG 2019-16 guidelines (Rev. 1).


# NEMECYS: NEw MEdical CYbersecurity assessment and design Solutions

NEMECYS - 101094323

HORIZON-HLTH-2022-IND-13

nemecys.eu info@nemecys.eu nemecys-horizon-eu-project