A Way Forward for the MDCG 2019-16 Medical Device Security Guidance

Steve Taylor, University of Southampton,

Martin Gilje Jaatun, Karin Bernsmed, SINTEF Digital

Christos Androutsos, University of Ioannina

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

Dietmar Frey, Charité Universitaetsmedizin Berlin

Simone Favrin, MediaClinics Italia

João Rodrigues, INOV

Duško Milojević, KU Leuven

Dimitrios S. Karras, Ioannis Siachos, UBITECH

Paul Gedeon, Red Alert Labs

Gregory Epiphaniou, Nabil Moukafih, Carsten Maple, WMG, University of Warwick, Coventry, UK

Sotiris Messinis, Ioannis Rallis, Institute of Communication and Computer Systems

Nicholas E. Protonotarios , Academy of Athens, Greece

Nikolaos Matragkas, CEA Saclay Nano-INNOV - Institut CARNOT CEA LIST, DILS/LSEA

Rance DeLong, The Open Group

Theodoros Arvanitis, University of Birmingham

Konstantinos Katzis European University Cyprus

NEMECYS New Medical Cybersecurity and design Solutions

CYLCOMED

MedSecurance Advanced Security-for-safety Assurance for Medical IoT

Septon

Enlightened trust in governance EnTrust

PETRA24, Crete, 29 June 2024

NEMECYS New Medical Cybersecurity and design Solutions

Co-funded by the European Union

The NEMECYS project is co-funded by the European Union, by UK Research and Innovation (UKRI) and by the Swiss State Secretariat for Education, Research and Innovation (SERI).

Introduction

- MDCG 2019-16 aims to assist practitioners in compliance with the Medical Device Regulation (MDR) and the In-Vitro Device Regulation (IVDR)
- This paper presents an analysis of MDCG 2019-16, identifying key gaps and proposing recommendations to enhance the IoMT regulatory framework
- This work has been undertaken by a selection of current (2023-2025) projects, all funded under the Horizon Europe call *"Enhancing cybersecurity of connected medical devices": HORIZON-HLTH-2022-IND-13-01*

Co-funded by the European Union

Recommendations

- **Linking Cybersecurity Risks, Patient Safety & Privacy Risks (NEMECYS, CYLCOMED, MEDSECURANCE)**
  - It is not clear how cybersecurity techniques and privacy measures relate to patients' safety
  - Need to consider relationships between **cybersecurity consequences** (*"A security violation that results from a threat action"* (ISO/IEC 27001:2022)) and **patient harms** (*"injury or damage to the health of people, or damage to property or the environment"* (ISO 14971:2019))
  - A key integration point is via **data**, where a widely accepted set of risks is related to the CIA triad – Confidentiality, Integrity and Availability
    - E.g., compromises in the availability or integrity of MD sensor data can lead to late or inaccurate diagnosis, leading to potential patient harm

Co-funded by the European Union

Recommendations

- **Guidance on Cybersecurity Controls (NEMECYS)**
  - Absence of guidance in the MDCG on security-related controls with respect to device classes
    - Causes difficulties in identifying security control criteria for types of MD
  - Recommend that reference to **relevant cybersecurity risk management standards** such as ISO 27002 are recommended by MDCG

- **Balancing Different Types of Patient Risk (NEMECYS)**
  - Recommend that the MDCG provide guidance on resolution of conflicts
    - E.g. between privacy requirements, cybersecurity and medical needs
  - Advice on **methods to evaluate balances between conflicting needs** will enable decision maker to determine clear policy on acceptable balance between patient healthcare and privacy

Co-funded by the European Union

NEMECYS
New Medical Cybersecurity and design Solutions

Recommendations

- **Keep MDCG 2019-16 Guidelines Current (NEMECYS, MEDSECURANCE)**
  - Recommended that MDCG guidelines are **periodically updated** with respect to evolving standards and state of the art
  - Also to keep pace with evolutions of MDR / IVDR

- **MD Lifecycle & Risk Assessment (NEMECYS)**
- Recommended that the MDCG guidelines map guidance to the **different stages of the whole MD lifecycle**:
  - Design and manufacturing, deployment in (many different) scenarios, operation of the device in those scenarios and decommissioning / disposal.
  - Different lifecycle stages of a medical device may give rise to differing priorities for cybersecurity or patient harm

Co-funded by the European Union

Recommendations

- **Operational Environment (NEMECYS)**
  - Recommended that MDCG guidelines advocate a system-wide approach when assessing harms & threats, related to **intended usage scenarios and environments**
  - Many situations where the environment has multiple domains of control - i.e. controlled by different legal entities.
- **Processes, Recipes & Education for MDCG Guidelines (NEMECYS, MEDSECURANCE)**
  - Recommended that MDCG provide "**recipes**" describing different cases of compliance, processes and objectives to achieving them for identified user types
  - Recommend that a **training and education resource** be developed based on the MDCG guidance, forming a knowledge base that supports manufacturers in meeting regulatory demands

Co-funded by
the European Union

Recommendations

- **Multiple Nomenclatures (CYLCOMED)**
  - Cyber security concerns involve different aspects depending on the stakeholder role, and it is **difficult to provide a common language** and mutual understanding between clinical practice and technology solution providers
  - Recommend MDCG provides a chart to navigate this complexity
- **Need for Specificity (MEDSECURANCE)**
  - The MDCG's generic guidelines often lack specificity for advanced technologies, leading to an overreliance on guidance documents rather than legislative texts, thus introducing potential subjectivity into the regulatory assessment process
  - Recommend **tailored guidance** that addresses the unique verification, validation, and transparency of these technologies

Co-funded by
the European Union

Recommendations

- **Post-market surveillance (SEPTON)**
  - Recommend guidance to address key gaps in the post-market phase:
    - **Adaptability** of post-market surveillance practices to rapidly evolving technologies
    - **Information sharing** between manufacturers, competent authorities, and other stakeholders to collectively address emerging cybersecurity threats.
  - Recommend guidelines detail a standardized methodology for systematically categorising and analysing **root causes of incidents**
    - Investigation of the factors that contributed to incidents, considering both technical and contextual aspects.
    - Using standardized frameworks and International Medical Device Regulators Forum (IMDRF) codes

Co-funded by the European Union

Recommendations

- **Legal Perspective (CYLCOMED)**
  - MDCG operates in a complex legal space with multiple regulations applicable, e.g. GDPR, NIS Directive, Cyber Security Act, and the proposed Cyber Resilience Act and the AI Act
  - Well-acknowledged overlapping and conflicting issues that arise in practical implementation
  - **Proper guidance is crucial to facilitate compliance with the myriad legal requirements dispersed across various regulations**
  - Wider in scope than MDCG but additional guidance in section 6 would be highly appreciated

Co-funded by the European Union

Recommendations

- **Vulnerability Management (ENTRUST)**
  - Vulnerability management is a critical aspect of providing cybersecurity assurance to medical devices, and entails the organization, and evaluation of the identified vulnerabilities affecting a medical device throughout its operational lifecycle, in order to determine the most appropriate actions to be taken in order to address and mitigate those vulnerabilities, considering their criticality and prevalence.
  - Recommendations:
    - Guidance for **prioritisation of vulnerability patch creation**
    - Guidance for **monitoring of vulnerabilities** in the operational environment
    - Guidance for **delivering patches in the field** in a secure, timely and efficient manner
    - Guidance on **assessing "reasonably foreseeable misuse"** in operational environments

Co-funded by the European Union

Conclusions

- We have presented 12 recommendations from five Horizon Europe projects towards providing feedback to the MDCG guidance represented in MDCG 2019-16
- Considerable consensus across the projects in many recommendation themes, notably:
  - linking cybersecurity with patient safety and privacy;
  - keeping the guidelines current; and
  - usage recipes for the guidelines.
- These projects are approaching the halfway point, and subsequent papers will describe further recommendations to the MDCG 2019-16 guidelines as appropriate

Co-funded by the European Union