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

Steve Taylor*
University of Southampton
s.j.taylor@soton.ac.uk

Martin Gilje Jaatun, Karin Bernsmed
SINTEF Digital,
Martin.G.Jaatun@sintef.no
Karin.Bernsmed@sintef.no

Christos Androutsos
University of Ioannina
xristosandroutsos95@gmail.com

Andres Castillo
Fundación Para La Investigación Biomédica Hospital Infantil Universitario Niño Jesús
Andres.Castillo@salud.madrid.org

Dietmar Frey
Charité Universitaetsmedizin Berlin
dietmar.frey@charite.de

Simone Favrin
MediaClinics Italia
s.favrin@mediaclinics.it

João Rodrigues
INOV
joao.rodrigues@inov.pt

Duško Milojević
KU Leuven
dusko.milojevic@kuleuven.be

Dimitrios S. Karras, Ioannis Siachos
UBITECH, dkarras@ubitech.eu
isiachos@ubitech.eu

Paul Gedeon
Red Alert Labs
paul.gedeon@redalertlabs.com

Gregory Epiphaniou, Nabil Moukafih, Carsten Maple
WMG, University of Warwick, Coventry, UK.
gregory.epiphaniou@warwick.ac.uk,
CM@warwick.ac.uk
nabil.moukafih@warwick.ac.uk

Sotiris Messinis, Ioannis Rallis
Institute of Communication and Computer Systems,
irallis@mail.ntua.gr
smessinis@mail.ntua.gr

Nicholas E. Protonotarios
Academy of Athens, Greece
nprotonotarios@academyofathens.gr

Nikolaos Matragkas
CEA Saclay Nano-INNOV - Institut CARNOT CEA LIST, DILS/LSEA
nikolaos.mzatragkas@cea.fr

Rance Delong
The Open Group
r.delong@opengroup.org

Theodoros Arvanitis
University of Birmingham
t.arvanitis@bham.ac.uk

Konstantinos Katzis
European University Cyprus
k.katzis@euc.ac.cy

ABSTRACT

MDCG 2019-16 is intended to assist practitioners in compliance with the Medical Device Regulation and the In-Vitro Device Regulation. This paper presents a gap analysis of MDCG 2019-16, identifying key gaps and proposing a robust set of 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, and this paper summarises observations and recommendations from across these projects. There is 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. The paper also suggests toolkit solutions to address some of the recommendations.

*Corresponding author.

PETRA '24, June 26–28, 2024, Crete, Greece

ACM ISBN 979-8-4007-1760-4/24/06
https://doi.org/10.1145/3652037.3663894

CCS CONCEPTS

• **Applied computing** → Life and medical sciences; • **Security and privacy** → Systems security; Distributed systems security; Software and application security; Domain-specific security and privacy architectures.

KEYWORDS

Medical Devices, MDCG, Cybersecurity, Risk Management, Clinical Benefit, Regulation, Guidelines, Recommendations

ACM Reference Format:

Steve Taylor, Martin Gilje Jaatun, Karin Bernsmed, Christos Androutsos, Andres Castillo, Dietmar Frey, Simone Favrin, João Rodrigues, Duško Milojević, Dimitrios S. Karras, Ioannis Siachos, Paul Gedeon, Gregory Epiphaniou, Nabil Moukafih, Carsten Maple, Sotiris Messinis, Ioannis Rallis, Nicholas E. Protonotarios, Nikolaos Matragkas, Rance Delong, Theodoros Arvanitis, and Konstantinos Katzis. 2024. A Way Forward for the MDCG 2019-16 Medical Device Security Guidance. In *The PErvasive Technologies Related to Assistive Environments (PETRA) conference (PETRA '24), June 26–28, 2024, Crete, Greece*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3652037.3663894

1 INTRODUCTION

The European health care system is moving toward personalised, distributed, and home-based services where an application spans from remote patient monitoring to virtual consultations for chronic illnesses. This is made possible via new and improved connected medical devices (MDs) and in vitro diagnostic devices connected to the internet (together, Connected Medical Devices – CMDs or Networked Medical Devices - NMDs), and will benefit health care providers in terms of reduced cost (fewer hospital beds) and improved service. However, for these benefits to be fully realised, the cybersecurity of CMDs needs to be ensured. The Medical Device Coordination Group (MDCG) is instrumental in addressing critical aspects of the medical device sector. MDCG is tasked with enhancing the understanding and implementation of guidance across various stakeholders, including regulatory bodies, notified bodies, and manufacturers, thereby facilitating the overall regulatory approval process for medical devices. The MDCG 2019-16 - Guidance on Cybersecurity for medical devices [1] is intended to assist practitioners in compliance with the Medical Device Regulation (MDR, [2]) and the In-Vitro Device Regulation (IVDR, [3]). This paper presents a gap analysis of MDCG 2019-16, identifying key gaps and proposing a robust set of recommendations to enhance the IoMT regulatory framework. This work has been undertaken by a set of current (2023-2025) projects, all funded under the Horizon Europe call "Enhancing cybersecurity of connected medical devices": HORIZON-HLTH-2022-IND-13-01 [4], which requested feedback to MDCG 2019-16, and this paper summarises observations and recommendations from across these projects to contribute to answering this request. Each of the projects is briefly described, then recommendations for improvements and enhancements to the MDCG guidance are presented. Suggested tools from the projects follow to address some of the recommendations, and the paper concludes with a brief summary of consensus amongst recommendations.

2 PROJECTS

2.1 NEMECYS [5]

NEMECYS benefits practitioners such as cybersecurity communities, MD manufacturers, CMD scenario system integrators and CMD scenario operators (e.g. health care providers) to (1) comply with MD regulations by providing recommendations for best practice and guidelines for MD cybersecurity by design, along with compliance assurance tooling; (2) to be able to apply proportionate MD cybersecurity (too little security risks exposure, too much is costly and can obstruct clinical care) by providing a risk-benefit scheme to address cybersecurity risk balanced with clinical benefit; and (3) build in cybersecurity by design for both MDs and the connected scenarios they operate in by providing a set of specific tools to address MD cybersecurity by design and their deployment in connected scenarios.

2.2 CYLCOMED [6]

CYLCOMED strengthens the cybersecurity of connected, in vitro diagnostic and software as medical devices (CMDs, IVDs, SaMD), maintaining their performance and safety for patients and preserving or enhancing the confidentiality, integrity and availability of private data they exchange or allow to be remotely accessed and focusing on humans operating the technology as the weakest link in the chain for security and privacy, with training and awareness measures tailored to healthcare staff needs. It does so by enabling adoption by all ecosystem stakeholders of technologically sovereign and trustworthy cybersecurity methodologies and toolboxes for connected medical devices and the environments in which they are managed and operate (platforms), complemented with fit-for-purpose guidance covering identified risks and gaps.

2.3 MEDSECURANCE [7]

MEDSECURANCE conceives novel methodologies, infrastructures, and technologies that enable an effective, harmonious and continuous development and evolution of secure system engineering management activities in Internet of Medical Things (IoMT). Its objective is to advance knowledge and basic understanding of decision making in diverse IoMT threat landscapes based on different system and component level interactions. This is accomplished via the development of a novel holistic strategy that considers the interdependence of several IoMT subsystems, information exchange, risk thresholds, and regulatory ramifications. We provide scalable and verifiable secure system engineering management solution(s) that capture, communicate, and act on these complexities in order to improve decision-making in cyber defence while automating cybersecurity assurance.

2.4 SEPTON [8]

SEPTON has a holistic approach towards reinforcing networked medical devices (NMD) security. It advances cutting-edge solutions in healthcare cybersecurity targeting health providers and focusing on NMDs. The SEPTON approach will result in a comprehensive cybersecurity toolkit providing tools and mechanisms to be used in hospitals and care centres for a) the protection of networked medical devices, including wearable and implantable devices, and using techniques such as polymorphism b) the secure and privacy preserving data exchanges between NMDs, utilising techniques such as blockchain, differential privacy and encryption c) behavioural anomaly detection, utilising a cybersecurity analytics framework coupled with machine learning techniques and hardware acceleration for increased performance and d) NMD vulnerability assessment. The usability of the proposed solutions will

be tested in a realistic setup via extensive pilot trials, facilitated by the participation of two healthcare organisations.

2.5 ENTRUST [9]

Aligned with the guidelines of the Cybersecurity Act and the existing guidance on cybersecurity for medical devices, ENTRUST envisions a Trust Management Architecture intended to dynamically and holistically manage the lifecycle of connected medical devices, strengthening trust and privacy in the entire medical ecosystem. ENTRUST will introduce a novel remote attestation mechanism to ensure the device's correct operation at runtime regardless of its computational power. This will be accompanied by dynamic trust assessment models capable of identifying the Required Level of Trustworthiness (RTL) per device and function (service) that will then be verified through a new breed of efficient, attestation mechanisms to be deployed and executed during runtime. The motivation behind ENTRUST is to ensure end-to-end trust management of medical devices including formally verified trust models, risk assessment process, secure lifecycle procedures, security policies, technical recommendations, and the first-ever real-time Conformity Certificates to safeguard connected medical devices.

3 RECOMMENDATIONS

This section contains brief statements regarding recommendations to improve, enhance or widen the benefits of the MDCG 2019-16 guidelines. Each project was canvassed for recommendations and the responses were collated into thematic groups presented here, and the theme heading refers to the projects that advocated the recommendation, which in some cases is a single project and in other cases multiple projects.

3.1 Linking Cybersecurity Risks, Patient Safety & Privacy Risks (NEMECYS [5], CYLCOMED [6], MEDSECURANCE [7])

Although cybersecurity techniques and privacy measures are often considered together, it is not clear how they relate to patients' safety. Many cybersecurity risk management frameworks and standards exist nowadays, including ISO/IEC 27001 [10], ISO 27005 [11], NIST Risk Management Framework [12] and the NIST Cybersecurity Framework [13]. ISO/IEC 27701 [15] was introduced to tackle privacy information management, as well as the NIST Privacy Framework [14]. When it comes to safety of medical devices, the ISO 14971 standard [16] describes the process by which manufactures can manage the safety risks of their MD throughout its life cycle. It outlines how to structure the risk management process and what activities should be performed to guarantee MD safety for medical use.

There is a need to consider relationships between cybersecurity consequences ("A security violation that results from a threat action" [10]) 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 [16]). 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. Investigations so far have shown that a key integration point between cybersecurity and patient safety is via data, where a widely accepted set of risks is related to the CIA triad – Confidentiality, Integrity and Availability. Guidance for identification of these risks and how they affect patient safety is recommended. As an example, compromises in the availability or integrity of MD sensor data can lead to late or inaccurate diagnosis, leading to potential patient harm or reduction in the quality of treatment.

3.2 Guidance on Cybersecurity Controls (NEMECYS [5])

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 [17] are recommended by MDCG.

3.3 Balancing Different Types of Patient Risk (NEMECYS [5])

It is recommended that the MDCG guidelines provide guidance on resolution of conflicts, for example between privacy requirements (when need to comply with privacy regulations such as GDPR [22]) and medical needs. It is clear that efforts towards personal data protection should not hamper medical care, but contrasted against this is a need to minimise privacy-related risks associated with medical devices and provide guidelines addressing their privacy concerns. Advice on methods to evaluate balances between these conflicts will enable the decision maker to determine clear policy on an acceptable balance between patient healthcare and their privacy.

3.4 Keep MDCG 2019-16 Guidelines Current (NEMECYS [5], MEDSECURANCE [7])

Rapid technological evolution necessitates regular updates and amendments to guidance, ensuring relevance. 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. It is also recommended that new versions of the MDCG guidelines be periodically released resulting from state-of-the-art surveys to ensure that the MDCG provides relevant and up to date guidance on how to meet relevant security standards and ongoing monitoring regarding cybersecurity protocols and controls.

3.5 MD Lifecycle & Risk Assessment (NEMECYS [5])

It is recommended that the MDCG guidelines map guidance to the different stages of the whole MD lifecycle – from design and manufacturing, deployment in (many different) scenarios, operation of the device in those scenarios and eventual decommissioning

/ disposal. There is a many-to-many relationship between these phases - i.e., one device can be used in different contexts (and indeed the same scenario can have varying environments for devices), and so the lifecycle is complex. Each use of a device should be assessed for cybersecurity and the responsible party (i.e. who should assess it and ensure risk is acceptable) needs to be clear. Further, different lifecycle stages of a medical device may give rise to differing priorities for cybersecurity or patient harm, so lifecycle stage should be taken into consideration when assessing the importance of consequences / harms.

3.6 Operational Environment (NEMECYS [5])

It is recommended that the MDCG guidelines advocate a system-wide approach when assessing harms, threats, vulnerabilities and controls, related to valid intended usage scenarios. The manufacturer already needs to describe intended use, which will very likely involve a device's operation in an environment connected with other devices, networks, people and places and will thus be exposed to threats resulting from connection with these other entities and actors. Further, there are likely to be many situations where the environment has multiple domains of control - i.e. controlled by different legal entities (an example being a medical device in a patient's house connects to a 3rd party cloud service that is also accessed by a hospital - three legal entities). Therefore, there are multiple sources of threats and risks, and it is unlikely that one entity will be able to exercise total control, so cooperation between entities will be required to address the threats and risks, and guidance on assessment and control of threats and risks in such multi-party situations would greatly assist practitioners.

3.7 Processes, Recipes & Education for MDCG Guidelines (NEMECYS [5], MEDSECURANCE [7])

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. For higher-risk medical device software, detailed guidance on validation and verification processes is crucial to ensure safety and performance. It is recommended that MDCG guidelines be organised into "recipes" describing different cases of compliance, processes and objectives to achieving them for identified user types, e.g. a device manufacturer wishing to acquire compliance with the MDR, or a system integrator wishing to ensure their usage scenario is compliant, and the recipes organise the MDCG guidance into step-by-step guides. The provision of practical case studies and examples will facilitate the application of MDCG 2019-16, aiding manufacturers in regulatory compliance. A comprehensive training and education resource could also be developed based on the MDCG guidance, forming a knowledge base that supports manufacturers in meeting regulatory demands cohesively and coherently.

3.8 Multiple Nomenclatures (CYLCOMED [6])

Cyber security concerns involve different aspects depending on the stakeholder role, and perception misalignment can be challenging to address. A specific point emerging from CYLCOMED is that it is extremely difficult to provide a common language and mutual understanding between clinical practice and technology solution providers. This difference in perception leads to increased complexity, particularly when introducing new technology solutions in a pre-existing context. For example, the process of introducing a new medical device (specifically - telemonitoring) needs to take into account a broad range of concerns (ethical aspects, state-of-the-art infrastructure), which are difficult, if not impossible, to be foreseen by the technological providers alone. Providing a chart to navigate this complexity would be highly beneficial for all stakeholders.

3.9 Need for Specificity (MEDSECURANCE [7])

The transition to the full application of the MDR and IVDR has created a climate of uncertainty, affecting market access and compliance strategies. Enhanced surveillance obligations require ongoing monitoring of device performance, implicating further resource allocations. Additionally, the redefined roles of economic operators and rigorous clinical investigation prerequisites present new complexities. The detailed device classification system under the new regulations may result in reclassification challenges, demanding precise interpretation and application of guidance. 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. This highlights the imperative for iterative guidance refinement to facilitate compliance within the dynamic regulatory milieu. Given the rise of Artificial Intelligence and Machine Learning in medical devices, tailored guidance that addresses the unique verification, validation, and transparency of these technologies is essential. This should be integrated with continuous monitoring protocols.

3.10 Post-market surveillance (SEPTON [8])

The evaluation of incidents in the post-market surveillance phase is a delicate process that requires a prudent assessment of their severity and potential impact. Manufacturers distinguish between serious and non-serious incidents, a classification crucial for assessing the urgency and scope of subsequent actions. Under the MDCG 2019-16, the assessment of the need to report serious or non-serious incidents and the subsequent implementation of Field Safety Corrective Actions (FSCA) is a cornerstone of post-market surveillance of medical devices [19]. FSCA includes corrective actions taken by manufacturers to prevent or mitigate serious incidents. This multi-layered assessment process is consistent with regulatory requirements and ensures that the appropriate level of action is taken in response to identified incidents to ensure the safety and effectiveness of medical devices on the market. However, there exist gaps in terms of defining clear and enforceable timelines for reporting these incidents. Delays in reporting may hinder the ability to take prompt corrective actions. The MDCG 2019-16 encourages manufacturers to take a forward-thinking stance by investing in research and development efforts aimed at incorporating advanced encryption mechanisms, enhanced access controls and the latest threat intelligence. While there is a focus on incorporating advanced encryption mechanisms, there might be gaps in the guidelines regarding the

adaptability of post-market surveillance practices to rapidly evolving technologies. Furthermore, potential gaps may exist in terms of guidelines for communication and information sharing between manufacturers, competent authorities, and other stakeholders to collectively address emerging cybersecurity threats. In addition, given the international nature of the medical device market, aligning post-market surveillance requirements globally may enhance consistency and effectiveness in addressing cybersecurity concerns. To this end, improving further the security capabilities in the post-market phase is essential to address emerging vulnerabilities and protect devices against potential risks [20].

Understanding the root causes of cybersecurity incidents is the basis for effective risk mitigation and prevention strategies. Post-launch monitoring requires a thorough investigation of the factors that contributed to the incidents, considering both technical and contextual aspects. Root cause analysis aims to identify the underlying issues that lead to vulnerabilities and incidents and provides a basis for targeted corrective actions. The taxonomy of root causes covers various dimensions, such as software vulnerabilities, unauthorized access and systemic weaknesses. By using standardized frameworks and the International Medical Device Regulators Forum (IMDRF) codes, manufacturers can systematically categorize and analyze root causes of incidents [21]. It is recommended that the guidelines detail a standardized approach or methodology for conducting root cause analyses. The iterative nature of this analysis contributes to the continuous improvement of post-market cybersecurity strategies and promotes the sustained safety and effectiveness of medical devices.

3.11 Legal Perspective (CYLCOMED [6])

MDCG 2019-16 Section 6 provides an overview of legislative intersections with different legal frameworks that might apply in parallel with MDR, particularly GDPR [22] and NIS Directive [23]. It briefly touches upon the overall purposes of these legal frameworks in a descriptive manner. However, due to well-acknowledged overlapping and conflicting issues that arise in practical implementation, there is an overarching necessity for addressing these issues more substantially, such as clarification of the concept of "joint responsibility" and "improvement of terminological coherence" [24], to mention just a few that would be of help to all stakeholders concerned. Next, the MDCG guidelines also briefly acknowledges the Cyber Security Act (CSA)[24], which introduces an EU-wide cybersecurity certification framework, without establishing a closer connection between the MDR and CSA in any sense, neither terminological nor substantial. Such a connection would be immensely beneficial, particularly in clarifying the interplay between MDR and CSA regarding cybersecurity certification[25]. Many scholars emphasize the centrality of ethical considerations in cybersecurity practices, but the MDCG guidelines do not contain any reference to ethics, so shedding more light on ethical principles and values would enhance understanding of the risks at stake and foster the implementation of ethical principles throughout the entire life cycle of medical devices. While medical device stakeholders operate in an already complex legal environment, new legislative initiatives, such as the AI Act Proposal [26] and the Cyber Resilience Act Proposal, [27] bring additional layers of complexity and uncertainty. While proper guidance is crucial to facilitate compliance with the myriad legal requirements dispersed across various regulations, it would be unrealistic to expect that the MDCG guidelines should serve as the "silver bullet" for untangling the medical device cybersecurity legal ecosystem. Nevertheless, additional guidance in section 6 would be highly appreciated.

3.12 Vulnerability Management (ENTRUST [9])

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. Vulnerability management (discussed in Section 2.4 of MDCG 2019-16) has been explored very little with regard to medical devices. In this regard, ENTRUST provides the following recommendations:

- *Which vulnerabilities should be patched?* The MDCG guildelines state that it is best to assume that any vulnerability which is deemed to be exploitable for a given implementation of software might be discovered and exploited over time, and as such should be regarded as an enabler for reasonably foreseeable misuse. This recommendation might be viewed as too restrictive where other types of devices are concerned, since end users will often agree with a manufacturer that a particular vulnerability is not worth patching in the device (e.g., because of a low CVSS or EPSS score). However, it is possible that most users of medical devices – i.e., hospitals – will agree that every vulnerability that has been verified to be exploitable in the device should be patched.
- *Infield monitoring of vulnerabilities.* The MDCG guidelines state that medical device manufacturers should ensure that a medical device is designed and manufactured in a way that ensures that the risks associated with reasonably foreseeable environmental conditions are removed or minimized. In this regard, we note that in most cases it will not be possible for the manufacturer to perform this monitoring, but it is possible (and hopefully already widely practiced) for the organizations utilizing these devices (e.g., hospitals) to do so.
- *Delivering patches.* The MDCG guidelines highlight the possibility to perform a device update (outside the context of a field safety corrective action) through, for example, delivering patches to ensure the continued security of the device. However, we argue that many device manufacturers have infrequent software updates on their devices, thus leaving users vulnerable to attacks that exploit the vulnerability before it is patched during the next update. Thus, we highlight the need to deploy security measures that are able to address such critical vulnerabilities in a more timely and efficient manner. These may include the remote attestation enablers provided by the ENTRUST framework, the AI-based Misbehaviour Detection module, and the identification of attacks via simulation in the Digital Twin of the device.

- *Reasonably foreseeable misuse.* The MDCG guidelines recommend that, during the risk management process, the manufacturer should foresee or evaluate the potential exploitation of the vulnerabilities which may be the result of a reasonably foreseeable misuse. However, in this regard, the ENTRUST consortium notes that this may depend on the specific situation. For example, using an insecure memory stick to enter data into a medical IT system can be considered reasonably foreseeable misuse, but may have major security implications as it is possible that it inadvertently introduces malware into the device. Therefore, while it is not possible to draw an unambiguous distinction, it is necessary to introduce security measures that are able to act as continuous security monitors for the provision of operational assurance in medical devices.

4 SUGGESTED TOOLKIT SOLUTIONS (SEPTON [8], NEMECYS [5], MEDSECURANCE [7], CYLCOMED [4], ENTRUST [9])

To strengthen security capabilities in line with the MDCG 2019-16, it is recommended that the MDCG evaluate tools and propose a toolkit solution. The toolkit may include threat intelligence collection tools, penetration testing frameworks, continuous monitoring mechanisms, risk assessment and solutions for encryption key management, secure coding policies and automatic security updates to strengthen devices against new threats. Collaboration platforms within the toolkit can enable knowledge sharing, in line with the collaborative ethos emphasized in the guidelines. In addition, visualization tools, such as interactive dashboards, can help understand incident complexities. In this direction, several recent initiatives aim to develop state-of-the-art toolkits with certain functionalities that contribute to the post-market surveillance phase. To this end, recent research projects deal with the development of specific state-of the art toolkits that enhance the cybersecurity of connected medical devices and systems.

NEMECYS [5] contributes to enhancing the cybersecurity of connected medical and diagnostic devices (CMDs) with its innovative toolkit, which guides CMD manufacturers, integrators, and healthcare providers in adhering to medical device regulations, providing recommendations, guidelines, and compliance assurance tools. It addresses the delicate balance between cybersecurity measures and clinical benefits through a risk-benefit scheme and tailored risk assessment tools. The toolkit supports CMD manufacturers during design, CMD system integrators during integration, and operators in connected scenarios. The MEDSECURANCE [7] toolkit offers resources for enhancing security and safety in healthcare systems. It includes tools for standards compilation, gap analysis, and risk assessments, featuring an assurance automation system and interoperability software implementation toolkit. SEPTON [8] focuses on networked medical device security, delivering a comprehensive cybersecurity toolkit for safeguarding devices and ensuring secure data exchanges. Incorporating blockchain, differential privacy, and encryption techniques, it also includes behavioral anomaly detection using a cybersecurity analytics framework and vulnerability assessment. CYLCOMED [6] provides a risk assessment framework with risk benefit analyses schemes and a toolbox addressing cybersecurity risks and gaps in connected medical devices; (iii) assessment and extension of baseline standards, best practices and guidelines covering challenges for CMDs including SW, making them suitable for purpose when used in conjunction with novel technologies. ENTRUST [9] provides dynamic trust assessment models capable of identifying the required level of trustworthiness (RTL) per device and function (service) that will then be verified through a new breed of efficient, attestation mechanisms (to be deployed and executed during runtime). This will also enable us to align with the existing standards on defining appropriate protection profiles per device, especially considering the heterogeneous types of medical devices provided by different vendors with different requirements, including targets of validation properties to be attested during runtime.

5 CONCLUDING REMARKS

This paper has presented recommendations from five Horizon Europe projects towards providing feedback to the MDCG guidance represented in MDCG 2019-16. There is 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. The paper has also suggested toolkit solutions from the projects. The status of the projects at the time of writing (Feb 2024) is that they are approaching the halfway point, and subsequent papers will describe further feedback and recommendation to the MDCG 2019-16 guidelines as appropriate.

ACKNOWLEDGMENTS

This work was funded by the European Commission under the following projects and grant IDs. NEMECYS: 101094323, CYLCOMED: 101095542, MEDSECURANCE: 101095448, SEPTON: 101094901, ENTRUST: 101095634.

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] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri$=$CELEX%3A32017R0745

[3] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.) https://eur-lex.europa.eu/eli/reg/2017/746/oj

[4] Enhancing cybersecurity of connected medical devices. HORIZON-HLTH-2022-IND-13-01 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-hlth-2022-ind-13-01

[5] NEw MEdical CYbersecurity assessment and design Solutions (NEMECYS) Project ID: 101094323, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/org-details/999999999/project/101094323/program/43108390/details

[6] Cyber securitY tooLbox for COnnected MEdical Devices (CYLCOMED) Project ID: 101095542, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/org-details/999999999/project/101095542/program/43108390/details

[7] Advanced Security-for-safety Assurance for Medical Device IoT (MEDSECURANCE) Project ID: 101095448, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/org-details/999999999/project/101095448/program/43108390/details

[8] SECURITY PROTECTION TOOLS FOR NETWORKED MEDICAL DEVICES (SEPTON) Project ID: 101094901, https://ec.europa.eu/info/funding-

tenders/opportunities/portal/screen/how-to-participate/org-details/999999999/project/101094901/program/43108390/details
[9] ENsuring Secure and Safe CMD Design with Zero TRUST Principles (ENTRUST) Project ID: 101095634, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/org-details/999999999/project/101095634/program/43108390/details
[10] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems: Requirements. https://www.iso.org/standard/iso-iec-27001-2022-v1
[11] ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Guidance on managing information security risks. https://www.iso.org/standard/80585.html
[12] NIST Risk Management Framework (RMF) https://csrc.nist.gov/projects/risk-management/about-rmf
[13] NIST Cybersecurity Framework https://www.nist.gov/cyberframework
[14] NIST Privacy Framework https://www.nist.gov/privacy-framework
[15] ISO/IEC 27701:2019. Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines. https://www.iso.org/standard/71670.html
[16] ISO 14971:2019. Medical devices: Application of risk management to medical devices. https://www.iso.org/standard/72704.html
[17] ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection: Information security controls. https://www.iso.org/standard/75652.html
[18] R. Shirey, Network Working Group, Request for Comments: 4949. Internet Security Glossary, Version 2. August 2007
[19] Ben-Menahem, S. M., Nistor-Gallo, R., Macia, G., von Krogh, G., & Goldhahn, J. (2020). How the new European regulation on medical devices will affect innovation. Nature biomedical engineering, 4(6), 585-590.
[20] Sigmund, W., Pracyk, J., Karchmer, T., Dias, J., Hoerauf, K., Beer, I., ... & Silverman, R. (2024). Medical Affairs in MedTech. In Medical Affairs (pp. 231-242). CRC Press.
[21] Jelić, L. (2023). Cybersecurity, Data Protection, and Artificial Intelligence in Medical Devices. In Inspection of Medical Devices: For Regulatory Purposes (pp. 417-445). Cham: Springer Nature Switzerland.
[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing 24. Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj
[23] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555
[24] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at: Directive - 2016/1148 - EN - EUR-Lex (europa.eu)
[25] Biasin, Elisabetta and Kamenjasevic, Erik, Cybersecurity of Medical Devices: Regulatory Challenges in the EU (September 30, 2020). The Future of Medical Device Regulation: Innovation and Protection, Cambridge University Press, 2020, Available at SSRN: https://ssrn.com/abstract$=$3855491
[26] European Union. 2019. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). EUR-Lex - 32019R0881 - EN - EUR-Lex (europa.eu)
[27] Milojevic, Dusko. "Is it time to update the Medical Device Coordination Group's Guidance on Cybersecurity for Medical Devices?" Blog Post, 14 NOVEMBER 2023. Available at: Is it time to update the Medical Device Coordination Group's Guidance on Cybersecurity for Medical Devices? - CiTiP blog (kuleuven.be)
[28] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)
[29] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. EUR-Lex - 52022PC0454 - EN - EUR-Lex (europa.eu).