Cybersecurity Guidances for Medical Devices: An MDCG and FDA Regulatory Comparison

Andrea Neverdal Skytterholm*, Christos Androutsos†, Adamantios Ntanis‡, and Martin Gilje Jaatun*

*Software Engineering, Safety and Security
SINTEF Digital, Trondheim, Norway
Email: {andrea.skytterholm, martin.g.jaatun}@sintef.no
†University of Ioannina, Ioannina, Greece
Email: xristosandroutsos95@gmail.com
‡PD Neurotechnology Ltd., R&D Department, Ioannina, Greece
Email: a.ntanis@pdneurotechnology.com

***Abstract*—This paper compares the distinct cybersecurity requirements for certifying connected medical devices (CMDs) in the EU and the US, as outlined in the MDCG 2019-16 guidance and the FDA premarket and postmarket guidances, respectively. By examining both the organizational approaches of the MDCG and FDA and their specific guidance documents, this study identifies key differences and areas of convergence. Findings, informed by stakeholder feedback gathered within the Horizon Europe NEMECYS project, reveal a notable disparity, with CMD stakeholders expressing significant dissatisfaction with the current EU regulatory framework, particularly regarding its applicability and clarity. The analysis highlights the strengths and weaknesses of each approach from a practical implementation perspective. Ultimately, the paper emphasizes the critical need for the European regulatory landscape to evolve towards clearer and more actionable guidance, especially in rapidly emerging fields like AI-driven medical devices, to effectively support the secure advancement of CMDs.**

***Index Terms*—Medical Devices; Security-By-Design; Security-By-Default; Cybersecurity; MDCG; FDA**

I. Introduction

The landscape of medical devices has undergone a significant transformation in recent years, marked by the increasing integration of digital infrastructure and Internet of Things (IoT) technologies. This evolution has enabled notable advancements in diagnostics, remote monitoring, and personalized care. However, the same technological progress has also expanded the cybersecurity attack surface, exposing Connected Medical Devices (CMDs) to new threats and vulnerabilities. As CMDs become more interconnected and reliant on networked systems, ensuring their cybersecurity has become a critical component of regulatory compliance and patient safety.

In response to this growing need, the European Union introduced the Medical Device Regulation (MDR) [1], which explicitly incorporates cybersecurity as a regulatory requirement. To support implementation, the Medical Device Coordination Group (MDCG) issued the guidance document "MDCG 2019-16: Guidance on Cybersecurity for medical devices" [2] (latest version 2020), offering recommendations to manufacturers, integrators, and operators on how to satisfy the cybersecurity requirements of the MDR. On the other side of the Atlantic, the FDA published their guidances on cybersecurity for premarket submissions titled "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" [3] (latest version 2023) and postmarket submissions titled "Postmarket Management of Cybersecurity in Medical Devices" [4] (latest version 2016). Despite both the MDCG and FDA documents targeting cybersecurity in the same class of medical devices, notable distinctions exist in their scope, structure, and level of prescriptiveness.

This study presents a detailed evaluation and comparison of the MDCG and FDA cybersecurity guidelines for medical devices, identifying areas of convergence, divergence, and potential improvements, with a specific focus on the applicability and clarity of the MDCG 2019-16 guidance. The findings presented herein are informed by the collaborative interactions of device manufacturers, integrators, and healthcare providers within the NEMECYS research project, a Horizon Europe initiative dedicated to developing cybersecurity-by-design tools and procedures for connected medical and diagnostic devices, thus offering unique stakeholder perspectives.

The remainder of this paper is structured as follows:

- Section II compares the MDCG and FDA approaches to regulating medical device cybersecurity, examining their organizational structures, regulatory authorities, frameworks, and guidance on AI.
- Section III compares the MDCG and FDA cybersecurity guidances, focusing on clarity, applicability, terminology, risk management approaches, and post-market considerations.
- Section IV elaborates on innovation challenges for smaller CMD companies due to unclear regulatory pathways, including difficulties in understanding compliance requirements, unpredictability, lack of awareness regarding MDR documentation, and challenges in demonstrating product safety.
- Section V synthesizes key recommendations for enhancing the MDCG 2019-16 guidelines, including aligning cybersecurity with safety and privacy, enhancing control guidance, updating guidelines, developing a risk assess-

ment framework, strengthening post-market surveillance, improving implementation guidance, and addressing AI.
- Section VI discusses the broader implications of these findings, including the differences between the FDA and MDCG approaches, their impact on manufacturers, the advantages and disadvantages of rule-based versus principle-based systems, and potential areas for future research.
- Section VII concludes the paper with final reflections and potential avenues for future research, emphasizing the need for clearer guidance, particularly for AI-driven devices, and suggests adopting aspects of the FDA's approach.

II. Comparative Analysis of MDCG and FDA Organizations

The following analysis compares the approaches of the Medical Device Coordination Group (MDCG) and the Food and Drug Administration (FDA) in guiding manufacturers, integrators, and healthcare operators on securing medical devices throughout their lifecycle. The comparison examines aspects such as organizational structure, regulatory authority, regulatory frameworks, guidance on emerging areas (like cybersecurity), risk management methodology, and post-market considerations. The differentiating factors identified through a comparison of these key areas (organizational structure, regulatory authority, regulatory frameworks, guidance on emerging areas, risk management methodology, and post-market considerations) will illuminate the distinctions between the MDCG [2] and FDA [3], [4] guidelines, which will be presented subsequently.

A. Organizational Overview

The MDCG is a body composed of representatives from EU Member States. The MDCG's activities cover a broad spectrum of critical areas in the medical device sector, from overseeing Notified Bodies and driving standardization to conducting market surveillance, engaging in international collaboration, addressing new technologies, and managing clinical investigations. One of its functions is to provide guidance and coordination among national competent authorities, ensuring consistent application of the Medical Device Regulation (MDR) [1] and the In Vitro Diagnostic Medical Device Regulation (IVDR) [5]. On the other hand, the FDA is a federal agency of the United States responsible for protecting public health and the primary regulatory authority responsible for ensuring the safety and effectiveness of medical devices, including connected medical devices (CMDs). Operating under the U.S. Department of Health and Human Services, the FDA issues binding guidance and regulations that manufacturers must adhere to for market approval. It regulates a wide range of products, including food, drugs, medical devices, and cosmetics, ensuring their safety and effectiveness.

Factor 1: *FDA is a direct regulatory authority, whereas the MDCG is a coordination group composed of EU member state representatives.*

B. Regulatory Authorities

The FDA's authority includes pre-market approval, post-market surveillance, and enforcement of regulations to safeguard consumers. The MDCG and FDA possess distinct regulatory authorities. In the European Union, the MDCG primarily functions as a coordinating body between member states and lacks direct enforcement power. It plays a supportive role in ensuring harmonization of medical device regulations across the EU but does not have the authority to enforce compliance. Instead, the responsibility for conformity assessment and approval of medical devices lies with notified bodies, which are designated by national health authorities [6]. In contrast, in the United States, the FDA holds extensive authority over both the approval of medical devices and the ongoing monitoring of manufacturer compliance. The FDA has the power to act as both the creator and enforcer of its guidances [6], [7]. Although these guidances are non-binding, the FDA uses them to assess manufacturer compliance with approval requirements, ensuring their effective implementation throughout the approval process and during post-market surveillance. This centralized authority of the FDA contrasts sharply with the role of the MDCG, as the FDA's enforcement power stems from its federal mandate, while the MDCG operates in a more collaborative, less authoritative capacity.

Factor 2: *FDA has the power to issue legally binding regulations and enforce compliance within the United States, whereas the MDCG issues non-binding guidance to ensure consistent application of EU regulations by national authorities.*

C. Regulatory Frameworks

The MDCG and the FDA function within distinct regulatory frameworks. The MDCG operates under a principle-based framework, whereas the FDA follows a rule-based framework [6]. In the EU, the principle-based approach embraces broad guiding concepts and fundamental requirements, emphasizing the establishment of an overarching goal instead of outlining particular compliance measures. This regulatory approach seeks to offer a broad framework that directs regulated entities in comprehending the main objectives of the regulatory framework. This system focuses on broad ideas that are then further developed through harmonized standards, as opposed to creating comprehensive and specific regulations [8]. In contrast, the rule-based framework, exemplified by the US system where regulators like the FDA establish specific and detailed rules for entities such as manufacturers, empowers these regulators to define and elaborate on medical device regulations, necessitating continuous updates to their guidance to accommodate technological advancements. This prescriptive regulatory approach can enhance clarity for regulated entities by simplifying the identification of mandatory compliance measures and expected minimum standards [8].

Factor 3: *The MDCG and FDA operate under regulatory frameworks constructed with distinct methodologies and pursuing different primary goals: the MDCG's principle-based*

framework prioritizes broad objectives and flexible implementation, whereas the FDA's rule-based framework emphasizes specific mandates and clarity in compliance.

D. Guidances on Emerging Areas

Both MDCG and FDA guidances serve as non-binding recommendations, often referred to as "soft law". Such guidances provides valuable frameworks for regulating medical devices and ensuring their safety, performance, and compliance with applicable standards. Compared to the EU, the FDA has been more prolific in issuing guidances on emerging areas. This difference can be attributed to the FDA's rule-based system, which requires specific directives. Conversely, the EU's broader safety principles offer flexibility, lessening the immediate need for regulations on novel technologies [6].

Regarding cybersecurity guidance for medical devices, the FDA initiated its efforts earlier in 2005, demonstrating a longer-standing commitment to clarifying regulatory expectations in response to evolving technological threats. In contrast, the MDCG introduced its first EU-level cybersecurity guidance in 2019, reflecting a later, yet significant, step towards harmonizing regulations within the EU under the MDR [6], [9].

A particularly striking disparity emerges in the treatment of artificial intelligence (AI) within medical devices given its rapid proliferation and potential to introduce novel cybersecurity vulnerabilities. As of April 14, 2025, the FDA is actively establishing a regulatory framework for Artificial Intelligence (AI) and Machine Learning (ML) in medical devices [10]. This effort began with a discussion paper in April 2019 on premarket review for AI/ML software modifications, followed by the "AI/ML SaMD Action Plan" in January 2021, which outlined the FDA's strategy. Subsequently, the FDA issued several guidance documents: "Good Machine Learning Practice for Medical Device Development: Guiding Principles" (October 2021), draft guidance on predetermined change control plans (April 2023), "Predetermined Change Control Plans for Machine Learning-Enabled Medical Devices: Guiding Principles" (October 2023), "Transparency for Machine Learning-Enabled Medical Devices: Guiding Principles" (June 2024), and "Final Guidance: Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions" (December 2024). Additionally, a paper titled "Artificial Intelligence and Medical Products: How CBER, CDER, CDRH, and OCP are Working Together" (March 15, 2024) detailed a coordinated FDA-wide approach to AI in medical products. Most recently, on January 6, 2025, the FDA released a "Draft Guidance: Artificial Intelligence-Enabled Device Software Functions: Lifecycle Management and Marketing Submission Recommendations", which offers lifecycle considerations and marketing submission advice for AI-enabled medical devices, building on prior guidance and addressing AI-specific aspects.

On the other hand, the MDCG documents demonstrate a complete absence of any reference to AI cybersecurity [11], [6]. This disparity further reinforces the observation that the FDA has demonstrated greater proactivity in addressing emerging cybersecurity challenges through the issuance of targeted guidance.

Factor 4: *The FDA has a more extensive and prolific history of issuing guidances compared to the MDCG, especially in rapidly evolving areas.*

III. Comparative Analysis of MDCG and FDA Cybersecurity Guidances

This section provides a comparative analysis of the cybersecurity regulatory approaches between the MDCG [2] and the FDA guidelines [3], [4]. While both documents aim to ensure the security and safety of connected medical devices, they differ in their regulatory scope, language precision, and technical depth.

Throughout the NEMECYS Horizon Europe research project, our discussions with connected medical device (CMD) stakeholders (manufacturers, operators, and integrators) have highlighted several potential challenges associated with the MDCG-2019-16 guidance, corroborating and further elaborating on the issues outlined in [12]. These discussions were also informed by prior findings from five other Horizon Europe projects: MEDSECURANCE, SEPTON, CYLCOMED, ENTRUST, and CYMEDSEC.

A. Clarity and Applicability

Stakeholder feedback pointed to notable issues with the MDCG 2019-16 guidance on cybersecurity [2]. A key worry was that, in the words of one stakeholder, "it makes clear ideas less clear", which complicated understanding the Medical Device Regulation (MDR) and who it applies to. Given the newness of the MDR, some stakeholders thought entirely new guidelines would be required, with one even suggesting the current MDCG 2019-16 guidelines were poorly written and should be discarded. Recognizing these challenges and the wider importance of strong cybersecurity in healthcare, the European Commission launched the European action plan on the cybersecurity of hospitals and healthcare providers on 15 January 2025. This plan aims to improve how the healthcare sector detects threats, prepares for them, and responds to crises. It specifically includes medical equipment and highlights the acknowledged need for guidance on essential cybersecurity practices, suggesting an understanding of the weaknesses identified in existing documents like MDCG 2019-16. In contrast, the FDA guidances were noted for being clear and easy to understand compared to the guidances of MDCG. Stakeholders pointed out that their practical format can help even small companies that make connected medical devices understand the rules without needing as much outside help. The FDA guidances can also serve as useful tools to check for missing cybersecurity information. Their strength lie in providing measurable goals and clear advice, making it a source of good cybersecurity practices even if it doesn't directly apply in Europe. The feeling of stakeholders that it is easier to get approval in the US due to less bureaucracy further highlights the difference in user experience.

B. Technical Terminology

The MDCG-2019-16 guidance presents a notable weakness in its imprecise terminology. The document employs terms and phrases such as "cyber smart behaviour" (a non-standard phrase) and "operator" without sufficient definition. This lack of clarity can lead to misunderstandings and divergent interpretations, ultimately obscuring the allocation of responsibilities under the MDR. This issue of imprecise terminology extends to fundamental concepts within the field, as highlighted by Biasin and Kamenjasevic [9] regarding the lack of proper definitions for terms such as "cybersecurity", "security-by-design", and "security-by-default". Stakeholders emphasize the necessity of practical examples to elucidate the legal requirements. In contrast, the FDA guidances demonstrate strength in their clear and consistent definitions, often grounded in established industry standards, thereby mitigating ambiguity.

C. Cybersecurity Risk Management

Both the MDCG 2019-16 and the FDA Premarket Cybersecurity Guidance adopt a risk-based approach to cybersecurity in CMDs, requiring manufacturers to identify, assess, and mitigate cybersecurity risks throughout the product lifecycle. However, their scope and implementation expectations differ significantly.

The MDCG guidelines position cybersecurity risk management as an extension of ISO 14971–based safety risk management, encouraging manufacturers to treat cybersecurity threats as potential contributors to clinical safety risks. The MDCG guidelines emphasize the bidirectional relationship between safety risks and cybersecurity risks, highlighting that cybersecurity controls may impact patient safety, and conversely, safety controls may introduce cybersecurity vulnerabilities. It recommends that manufacturers ensure traceability between risk assessments, security controls, and residual risks, but offers relatively high-level guidance on how to operationalize these activities.

In contrast, the FDA guidance provides a more prescriptive and structured approach to cybersecurity risk management. It requires manufacturers to: (1) Perform threat modeling as part of design controls. (2) Categorize risks using a security risk assessment (distinct from safety risk assessments). (3) Map threats to specific mitigation strategies, including testing and validation methods. (4) Include a cybersecurity bill of materials (CBOM) and define how security updates will be securely deployed.

While both frameworks align on the importance of cybersecurity-by-design, threat modelling, and post-market surveillance, the FDA provides a more detailed breakdown of cybersecurity measures, whereas the MDCG focuses on harmonizing cybersecurity with patient safety. These differences are further reflected in risk assessment, where the FDA emphasizes transparency in threat modelling and device labelling, while the MDCG provides broader, principle-based guidance on integrating cybersecurity into safety risk analysis.

Another significant divergence between the two guidances lies in their treatment of security capabilities (or cybersecurity control measures). MDCG-2019-16 mentions security capabilities briefly in an early section, with a table that a stakeholder described as random and inconsistent, mixing general categories with specific solutions. In contrast, the FDA guidance discusses security control categories in detail in an appendix. This section provides clear descriptions for each category, along with specific and practical advice on how to implement security controls. This organized approach offers a clearer and less confusing way to understand and implement security measures.

D. Post-Market Cybersecurity Considerations

The FDA has issued distinct guidance documents addressing medical device cybersecurity in both the premarket and postmarket phases. In contrast, the MDCG guidance integrates post-market cybersecurity considerations within the broader lifecycle of the medical device. Notably, the primary post-market cybersecurity aspect addressed by the MDCG is post-market surveillance, which appears to be treated as a mere reference, whereas the FDA extensively covers this area in separate documentation.

IV. Unclear Pathways as an Innovation Barrier

Smaller CMD companies, particularly startups, face the critical need to understand the time and costs associated with regulatory compliance. The inherent unpredictability of the legal and regulatory requirements is often tied to the specific technology and its associated risks. Many startups lack awareness regarding the extensive documentation mandated by the MDR throughout a product's lifecycle, frequently leading to insufficient allocation of funds for essential testing and clinical trials. From the outset, a clear understanding of the product's intended use is paramount. A significant challenge lies in effectively communicating the legal obligations imposed by the MDR. The fundamental goal is to systematically identify, classify, and mitigate risks to a point where the anticipated benefits demonstrably outweigh them. Ultimately, achieving CE marking necessitates documentation that unequivocally demonstrates the minimization of all identified risks and the product's ability to perform as intended.

V. MDCG Guidelines Improvement Recommendations

In our previous work [12], we identified a set of recommendations aimed at strengthening the regulatory framework for cybersecurity in medical devices within the EU. This study, conducted during the NEMECYS Horizon Europe research project, evaluated the applicability, shortcomings, and areas for improvement within the MDCG guidances. Specifically, throughout multiple Horizon Europe projects, stakeholders (medical device manufacturers, integrators, and operators) applied MDCG guidelines to meet MDR requirements in diverse case studies to evaluate the guidelines and provide feedback.

The key recommendations from this evaluation are presented below:

- **Alignment of Cybersecurity, Patient Safety, and Privacy:** We recommend strengthening the alignment between cybersecurity risks and patient safety and privacy concerns. This includes ensuring that security measures do not undermine clinical outcomes or violate data protection regulations, and developing proportionate controls that balance patient risk with minimal disruption to clinical workflows.
- **Enhancement of Cybersecurity Controls Guidance:** The guidance should be expanded to provide more detailed recommendations on cybersecurity controls and threat mitigation strategies, particularly by considering the classification and context of medical devices.
- **Updating and Evaluating Guidelines Frameworks:** To maintain relevance, the MDCG guidelines must be updated regularly to reflect evolving threats, technological advancements, and regulatory developments. Further investigation is needed to evaluate the potential benefits and drawbacks of incorporating more specific, case-by-case guidelines, inspired by rule-based regulatory frameworks, to address specific use cases. Such an approach could offer an easier regulatory pathway to various stakeholders, but may also prove too rigid, potentially impeding innovation.
- **Structured Cybersecurity Risk Assessment:** A structured cybersecurity risk assessment framework should be developed. This framework should address the full lifecycle of a medical device, from design and development to post-market use, and incorporate context-specific recommendations for various operational environments, including hospital networks, home healthcare settings, and distributed systems.
- **Strengthening Post-Market Surveillance:** The post-market surveillance guidance within the European framework is significantly underdeveloped, seemingly serving merely as a reference. Strengthening this aspect is crucial to facilitate effective monitoring, robust incident response, and continuous risk reassessment. Conversely, while the FDA's premarket and postmarket cybersecurity guidances do not directly address post-market surveillance, this domain is comprehensively covered in separate documentation.
- **Post-Market Cybersecurity Management:** The European post-market cybersecurity guidance is integrated within the broader medical device lifecycle management, which differs from the FDA's dedicated guidance document specifically addressing the management of post-market cybersecurity vulnerabilities in marketed and distributed medical devices. This area warrants greater attention and potentially a more distinct focus.
- **Aligh Guidelines With Legal Requirements** Legal alignment with frameworks such as the GDPR and NIS2 is needed to clarify how MDCG cybersecurity obligations interact with broader data governance laws [9]. Currently, the only explicit connection provided is a correspondence table within MDR Annex I and IVDR Annex I, which maps relevant sections to this guidance. This limited mapping does not fully address the complexities of their interaction.
- **Improving Practical Implementation Guidance:** The guidelines would benefit from the inclusion of practical examples and structured implementation guidance to assist manufacturers in achieving conformance.
- **Addressing AI in Medical Devices:** Given the increasing prevalence of artificial intelligence (AI) in medical devices, the guidelines must address this by introducing specific security measures for machine learning models. This should include, but not be limited to, protection against adversarial attacks, validation of model integrity, and secure data handling.

VI. Discussion

This paper has highlighted key differences between the cybersecurity guidance provided by the FDA and the MDCG for connected medical devices (CMDs). While both aim to ensure the safety and security of these devices, their approaches diverge significantly due to their organizational structures, regulatory authorities, and chosen regulatory frameworks.

The analysis reveals that the FDA, as a direct regulatory authority, possesses the power to issue legally binding regulations and enforce compliance within the United States. This contrasts with the MDCG, which operates as a coordinating body composed of EU member state representatives, primarily issuing non-binding guidance to ensure consistent application of EU regulations by national authorities. This fundamental difference shapes the nature of their respective guidance documents. The FDA's guidance tends to be more prescriptive and detailed, reflecting its rule-based framework, whereas the MDCG's guidance adopts a more principle-based approach, prioritizing broad objectives and flexible implementation.

The FDA's proactive approach to emerging areas, such as AI in medical devices, is particularly noteworthy. The agency's early engagement and development of a regulatory framework for AI/ML-based devices demonstrate its commitment to addressing novel cybersecurity vulnerabilities. In contrast, the MDCG's initial EU-level cybersecurity guidance in 2019, while significant, reflects a later step towards harmonizing regulations within the European Union.

These differences have several implications for medical device manufacturers. Companies seeking to market their products in both the US and the EU must navigate two distinct regulatory landscapes, potentially requiring them to implement different cybersecurity measures to meet the specific requirements of each region. This can increase compliance costs and complexity, particularly for smaller manufacturers with limited resources.

Furthermore, the principle-based approach of the MDCG may offer greater flexibility for innovation, as it avoids overly prescriptive rules that could stifle technological advancement.

However, it also introduces the risk of inconsistent interpretation and application, potentially leading to a fragmented regulatory landscape across EU member states. The FDA's rule-based approach, on the other hand, provides greater clarity and consistency but may be less adaptable to rapidly evolving technologies. The regulatory frameworks governing the MDCG and FDA significantly shape the guidance they produce and thus warrant closer examination, with both though offering unique benefits and shortcomings. Future research should focus on: (1) A more in-depth comparison of specific cybersecurity requirements outlined in the FDA and MDCG guidance documents, including areas such as risk management, vulnerability disclosure, and incident response. (2) Assessing how effectively these distinct regulatory guidances influence the actual cybersecurity implementation of CMDs and their capacity to withstand real-world attacks. (3) Exploring the potential for greater harmonization between the FDA and MDCG frameworks could help streamline the regulatory process and improve the overall security of medical devices worldwide, (4) Exploring the impact of regulatory frameworks (rules-based, principle-based) as a whole on the level of progress made within the domains those frameworks are applied on. There is the opinion that rules-based regulation can stifle technological and product innovation, acting as a significant impediment [8].

VII. Conclusion

This study has presented a comparative analysis of the MDCG and FDA approaches to cybersecurity guidances for medical devices, examining both their organizational structures and their respective guidance documents, "MDCG 2019-16: Guidance on Cybersecurity for medical devices" and "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" and "Postmarket Management of Cybersecurity in Medical Devices". Our findings reveal a notable disparity between the two, with feedback from CMDs stakeholders indicating significant dissatisfaction with the current EU regulatory framework. This is particularly pronounced for smaller medical device companies, which often lack the resources to engage external consultants to interpret the perceived vagueness and disjointed nature of the MDCG regulations.

While the EU's principle-based framework is often touted for its potential to foster innovation, our analysis suggests that a lack of specificity may, in fact, create a barrier, rendering the guidance less practically useful, especially for resource-constrained entities. The rapid advancements in artificial intelligence are further compounding this complexity, introducing novel cybersecurity and privacy risks within medical devices. This necessitates proactive and clear Europe-wide regulations that empower stakeholders to bring safe medical devices to market efficiently, rather than reactive measures that struggle to keep pace with technological evolution.

Moving forward, it is crucial for the European regulatory landscape to evolve in a manner that provides clearer pathways and more actionable guidance, particularly in emerging areas like AI-driven medical devices. Addressing the concerns raised by CMD stakeholders and learning from the more prescriptive and detailed approach of the FDA could streamline the regulatory process, reduce uncertainty, and ultimately foster both innovation and the timely availability of secure medical devices within the European Union. Future research could further explore the specific impact of regulatory vagueness on innovation in the medical device sector and investigate optimal strategies for harmonizing principle-based frameworks with the need for practical and readily implementable guidance.

Acknowledgements

This work has been performed in the context of the HEU NEMECYS project, co-funded by the European Union (grant number 101094323), by UK Research and Innovation (10065802, 10050933 and 10061304), and by the Swiss State Secretariat for Education, Research and Innovation.

References

[1] "Medical Device Regulation." 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.), 2025.

[2] Medical Device Coordination Group, "MDCG 2019-16 - Guidance on Cybersecurity for medical devices," 2020.

[3] US Food and Drug Administration, "Cybersecurity in medical devices: Quality system considerations and content of premarket submissions," 2023.

[4] US Food and Drug Administration, "Postmarket management of cybersecurity in medical devices," dec 2016.

[5] "In-vitro Diagnostic Medical Device Regulation." 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.), 2025.

[6] E. Biasin and E. Kamenjašević, "Regulatory approaches towards AI-based medical device cybersecurity: A transatlantic perspective," *European Journal of Risk Regulation*, vol. 15, no. 4, pp. 876–886, 2024.

[7] T. G. Maak and J. D. Wylie, "Medical device regulation: A comparison of the united states and the european union," *JAAOS-Journal of the American Academy of Orthopaedic Surgeons*, vol. 24, no. 8, pp. 537–543, 2016.

[8] Australian Law Reform Commission, "Regulatory theory," 2010.

[9] E. Biasin and E. Kamenjasevic, *Cybersecurity of Medical Devices: Regulatory Challenges in the European Union*, p. 51–62. Cambridge University Press, 2022.

[10] FDA Center for Devices and Radiological Health, "Artificial intelligence and machine learning in software as a medical device," Mar. 2025.

[11] R. Beckers and P. Van Hoydonck, "Impact of the regulatory framework on medical device software manufacturers: Are the guidance documents supporting the practical implementation? comment on" clinical decision support and new regulatory frameworks for medical devices: Are we ready for it?–a viewpoint paper"," *International Journal of Health Policy and Management*, vol. 12, p. 7470, 2023.

[12] S. Taylor, M. G. Jaatun, K. Bernsmed, C. Androutsos, A. Castillo, D. Frey, S. Favrin, J. Rodrigues, D. Milojević, D. S. Karas, I. Siachos, P. Gedeon, G. Epiphaniou, N. Moukafih, C. Maple, S. Messinis, I. Rallis, N. E. Protonotarios, N. Matragkas, R. DeLong, T. Arvanitis, and K. Katzis, "A way forward for the MDCG 2019-16 medical device security guidance," in *Proceedings of PETRA 2024*, 2024.