DOI: 10.1561/9781638285076.ch15

Chapter 15

Connected Medical Devices: The Cybersecurity Nexus of the AI Act and MDR

By Maja Nisevic, Dusko Milojevic, João Rodrigues and Goncalo Cadete

The increasing use of artificial intelligence (AI) in medical devices (CMDs) and their integration in the IoMT environment offers great potential for improving healthcare delivery, but it also brings complex challenges, cybersecurity being one of the most pressing ones. This book chapter delves into how the European Union's AI Act and the Medical Device Regulation (MDR) intersect in addressing the cybersecurity aspects of AI-driven medical devices. While the MDR focuses on ensuring the safety and performance of medical devices, including cybersecurity requirements across the product lifecycle, the Artificial Intelligence Act (AI Act) introduces rigorous measures for regulating high-risk AI systems, particularly in healthcare. Accordingly, the chapter examines the alignment of these frameworks and identifies potential regulatory gaps, particularly in cybersecurity standards, risk assessment, and conformity requirements for AI-enabled CMDs. By analyzing these aspects, the chapter aims to provide insights into how the evolving EU regulatory landscape can effectively ensure the security and safety of CMDs while promoting innovation in AI-driven healthcare technologies. It also offers recommendations for harmonizing regulatory approaches to better address the unique cybersecurity risks associated with AI in medical devices.

15.1 Introduction

In an era of rapid technological advancement, the incorporation of artificial intelligence (AI) into medical devices presents exceptional opportunities alongside complex regulatory challenges. The convergence of AI with medical technology has the potential to revolutionize healthcare delivery through enhanced diagnostics, personalized treatments, and improved patient outcomes. However, this integration also raises significant concerns, cybersecurity being one of the most pressing once, emphasizing the need for a robust regulatory and risk-assessment framework to ensure patient safety and safeguard data protection.

The World Economic Forum's Global Risks Report underlines cyberattacks as a critical global risk, highlighting the increasing severity and impact of these threats [1]. The growing reliance on technology across various sectors has propelled cybersecurity to the forefront of political agendas worldwide [2, 3].

Due to abundance of valuable data and lack of maturity level regarding the cybersecurity, the healthcare sector has emerged as a primary target for cyberattacks. According to the European Union Agency for Cybersecurity (ENISA) Report on the Health Threat Landscape, the health sector ranks third in terms of the number of cybersecurity incidents, with patient data—such as electronic health records—being the most targeted asset between January 2021 and March 2023 [4]. In addition, the FBI Internet Crime Report stresses the vulnerability of the healthcare sector, identifying it as one of the most attacked critical infrastructure sectors in the US in 2023 [5]. Successful attacks on healthcare systems have the potential to disrupt hospital operations, compromise patient safety, and, in severe cases, lead to loss of life.

From the perspective of the European Union, the AI Act (AIA) and the Medical Device Regulation (MDR) are two pivotal legislative instruments addressing distinct aspects of the regulatory landscape. The AIA focuses on establishing a comprehensive framework for the development, deployment, and oversight of AI systems, with an emphasis on risk management and transparency. Contrarily, the MDR governs the safety and performance of medical devices, including those incorporating AI, placing significant emphasis on clinical efficacy and patient safety. The intersection of these regulations presents a unique challenge: *aligning the provisions of the AI Act with the requirements of the MDR to create a cohesive cybersecurity strategy*.

As AI-enabled medical devices become increasingly prevalent, ensuring their security against cyber threats is paramount to maintaining public trust and safeguarding sensitive health information. Case studies highlight the critical intersection of the AI Act and MDR, particularly in instances where AI in medical devices has given rise to compliance issues. For example, AI-driven diagnostic tools such as imaging systems must meet the MDR's General Safety and Performance

Requirements and underwent third-party conformity assessments. However, the AI Act's requirements for transparency and explainability introduce additional complexity, leading to delays in device approval as developers ensure that AI decision-making processes are interpretable by healthcare professionals [6]. Ensuring these systems are resistant to manipulation while satisfying both regulatory frameworks has proven difficult, resulting in delays and compliance issues in the early development stages [7].

This book chapter delves into the broader issue of cybersecurity in connected medical devices (CMDs) amidst the surge of cyberattacks on healthcare sector. Under the MDR, manufacturers must implement cybersecurity measures as part of the General Safety and Performance Requirements, while the AI Act introduces specific provisions on the accuracy, robustness, and cybersecurity of AI systems. Therefore, the objective of this book chapter is to explore the synergies and potential conflicts between the AI Act and the MDR in the context of CMDs cybersecurity. By analyzing the regulatory frameworks of both, it aims to identify how they can be harmonized to address the specific cybersecurity challenges posed by AI-integrated medical devices. Besides, it will delve into importance of risk management strategies and standards in this domain. Through this examination, it seeks to provide actionable insights for policymakers, industry stakeholders, and researchers navigating this complex regulatory terrain, ultimately enhancing the safety and effectiveness of AI-driven medical technologies.

15.2 The Brief Overview of the Advancements in AI and Medical Devices

Many global health systems face a widening gap between demand and capacity. This surge in demand, driven by an aging population, rising chronic conditions, and higher expectations for quality care, is exacerbated by a growing shortage of healthcare professionals. The integration of AI presents a transformative potential to address these challenges. Recent advancements in AI medical devices have greatly impacted healthcare, bringing new possibilities for improved diagnostics, personalized treatments, and enhanced patient care. In 2021, the global AI in healthcare market was valued at over 11 billion U.S. dollars, with projections indicating a significant surge in growth, anticipating the market to expand to approximately 188 billion U.S. dollars by 2030 [8]. However, these advancements also come with new challenges and considerations, particularly in cybersecurity domain.

Further research and innovation hold significant potential in this realm. One crucial focus area is the development of AI-specific cybersecurity tools and risk assessment methodologies. It is essential to investigate potential vulnerabilities of AI models, such as adversarial attacks, and develop strategies to mitigate these

threats in healthcare settings to enhance device security. In addition, there is a growing need for research into explainability in AI systems as regulatory bodies increasingly seek transparent and understandable AI decision-making processes in healthcare contexts. Innovation is key to establishing dynamic regulatory frameworks that can adapt to technological advancements. This includes creating sandbox environments where new AI-enabled medical devices can be rigorously tested in real-world settings under regulatory supervision. These environments would support more effective collaboration between regulators and developers, ensuring that cybersecurity and regulatory compliance progress harmoniously with technological innovation. This section briefly stresses an overview of the recent developments in AI and medical devices.

15.2.1 AI in Medical Diagnostics and Treatment

AI has made substantial steps in medical diagnostics and treatment. Machine learning algorithms, particularly deep learning models, have demonstrated remarkable accuracy in analyzing medical images. For example, AI medical devices can now detect conditions such as diabetic retinopathy, lung cancer, and breast cancer with accuracy comparable to or exceeding that of human radiologists [9, 10]. These AI-driven tools can quickly analyze vast amounts of imaging data, providing valuable support in clinical decision-making.

Another significant advancement is the integration of AI in genomics and personalized medicine. AI algorithms can analyze genetic data to identify genetic markers associated with diseases and predict individual responses to specific treatments. This capability allows for more personalized and effective treatment plans, tailored to the unique genetic profile of each patient [11]. AI-driven platforms like IBM Watson for Oncology have been developed to assist oncologists in selecting appropriate therapies based on the latest research and patient data [12]. Likewise, a recent study highlights the significant strides made in oncology through the use of AI for cancer detection and treatment planning. The researchers developed an AI-based system that integrates genomic data and imaging to improve the accuracy of cancer diagnosis and predict patient responses to various therapies. This system has demonstrated a substantial increase in the precision of tumor classification and the identification of personalized treatment options, leading to more effective and targeted interventions [13].

15.2.2 Innovations in Connected Medical Devices

The Internet of Medical Things (IoMT) has expanded the capabilities of connected medical devices, enhancing their functionality and integration into healthcare

systems. Recent innovations include wearable devices, implantable sensors, and remote monitoring systems. Wearable devices, such as smartwatches and fitness trackers, now offer advanced health monitoring features, including heart rate variability, sleep analysis, and blood oxygen levels [14]. These devices provide real-time data to both patients and healthcare providers, enabling proactive management of chronic conditions and improved patient engagement.

Implantable devices, such as pacemakers and insulin pumps, have also seen significant advancements. Modern pacemakers are now equipped with wireless communication capabilities, allowing for remote monitoring and adjustments by healthcare providers [15]. Similarly, next-generation insulin pumps feature integrated continuous glucose monitoring systems, enabling more precise insulin delivery and better diabetes management [16].

15.2.3 AI-Driven Enhancements in Device Functionality

AI is increasingly being integrated into medical devices to enhance their functionality. For example, AI algorithms are used in automated insulin delivery systems to adjust insulin dosing based on real-time glucose readings, reducing the risk of hypoglycemia and hyperglycemia [17]. AI-powered diagnostic devices, such as handheld ultrasound machines, use machine learning to provide automated image interpretation, making advanced imaging more accessible in remote or underserved areas [18].A recent study explored the use of deep learning algorithms in medical imaging for enhancing the detection and classification of various diseases. The researchers developed an AI model that analyzes chest X-rays with high accuracy, identifying subtle abnormalities indicative of conditions such as pneumonia and tuberculosis [19].

15.2.4 Challenges and Considerations

While these advancements offer substantial benefits, they also present complex challenges. The integration of AI into medical devices raises concerns about data privacy, security, and regulatory compliance. Ensuring that AI algorithms are transparent and interpretable is crucial for maintaining trust in these technologies [20]. Additionally, the interoperability of connected devices and the protection of sensitive health data remain significant concerns as the use of IoMT expands [21].

In conclusion, recent advancements in AI and medical devices are reshaping healthcare by enhancing diagnostic accuracy, personalizing treatments, and improving patient monitoring. However, harnessing these innovations also necessitate careful consideration of privacy, security, and regulatory challenges to fully realize their potential benefits.

15.3 Understanding Cybersecurity and the Cyber Threat Landscape in Healthcare

Before adopting the European Union Cybersecurity Act in 2019, the term "cybersecurity" was often used vaguely, with varying interpretations depending on the context. In both academic literature and policy discussions, cybersecurity lacked a unified definition, making it challenging to develop consistent strategies for addressing cyber threats. As noted by some scholars, cybersecurity was frequently conceptualized differently by governments, organizations, and experts, leading to fragmented approaches across sectors [22]. This ambiguity posed significant challenges to establishing cohesive cybersecurity policies, particularly in critical sectors like healthcare, where the stakes are high.

The European Union Cybersecurity Act marked a turning point by introducing the first definition of cybersecurity within the EU legislative framework. The Act defines cybersecurity as the set of activities aimed at protecting network and information systems, their users, and those affected by cyber threats. This formalization has brought much-needed clarity, enabling a more consistent and structured approach to cyber defence across member states [23]. To understand the healthcare cybersecurity landscape, it is important to explore the motivations behind malicious attacks, the associated risks, and the sector's inherent vulnerabilities.

15.3.1 Motivations and Risks

Cyberattacks on healthcare systems can be driven by a range of motivations, including financial gain, political agendas, and intellectual property theft, to mention just a few [24]. Financial incentives are particularly significant in healthcare due to the value of sensitive data. Electronic Health Records (EHRs), which include comprehensive personal and medical information, are highly sought after on the black market, with stolen records fetching between $10 and $1,000 each, depending on their detail [25, 26]. This data's value extends beyond financial theft, as it can be used for fraudulent activities such as false insurance claims [27]. In addition, ideological motives and espionage also contribute to cybercriminal activities.

15.3.2 Consequences of Cyberattacks

Successful cyberattacks can have severe implications for both healthcare institutions and patients. Financially, the costs of security breaches are substantial. According to the ENISA NIS Investments Report the median cost of significant incidents is 300,000 euros [28]. IBM's Cost of a Data Breach Report highlights that healthcare breaches have been the costliest among industries for over a decade, with costs

increasing by 53.3% since 2020 [29]. Hospitals may face substantial financial burdens from patient compensation claims and regulatory fines [30]. A notable example is the Finnish psychotherapy center Vastaamo, which incurred a penalty of EUR 608,000 due to violations of the GDPR concerning the protection of personal data and the reporting of a data breach [31].

In addition to financial damage, cyberattacks can disrupt healthcare services, leading to potentially life-threatening consequences. The ransomware attack on Brno University Hospital in 2020, which led to postponed surgeries, and the attack on a German hospital that disrupted emergency services and contributed to a patient's death, underscore the critical impact of such breaches [32, 33]. Furthermore, disclosing sensitive health information can have profound and detrimental effects on patients' well-being, including adverse social perceptions, embarrassment, stigmatization, and potential harm to career prospects [34].

It is important to note that information regarding cyberattacks on hospital infrastructure is still scarce and obscured. While there are already examples of the severity of malicious attacks, such as the WannaCry ransomware attack in 2017 [35] and the Conti ransomware attack on Ireland's Health Service Executive in 2021 [36], the more comprehensive picture and information is still unknown and shrouded in mystery. This can be attributed to the reluctance of the provision of such information due to fear of reputational damage, patient compensation claims, and regulatory fines [37].

15.3.3 Physical Harm and Vulnerabilities

Cyberattacks can also result in physical harm. For example, wireless medical devices such as insulin pumps and pacemakers can be hacked to alter settings or dosage, potentially causing fatal outcomes [38]. A study by Allen et al. specifically highlights how vulnerabilities in insulin pumps could be exploited to change dosage levels, leading to severe health complications [39]. The Medtronic recall of insulin pumps due to cybersecurity vulnerabilities exemplifies the risk posed by such devices [40]. Similarly, vulnerabilities in cardiac pacemakers pose significant risks. Scholars such as He and Wu have demonstrated how cyberattacks could alter device settings, resulting in life-threatening arrhythmias or inappropriate shocks [41].

15.3.4 Cyberattack Techniques and Trends

Cybercriminals employ various techniques, including ransomware, distributed denial of service (DDoS) attacks, hijacking, remote code execution, and social engineering. Ransomware remains a prevalent threat in the healthcare sector, as highlighted by ENISA, with an upward trend in attacks [42]. In the Threat Landscape

for Ransomware Attacks Report, ENISA defines ransomware as a type of attack in which threat actors seize control of a target's assets and demand a ransom to restore access to those assets [43]. Furthermore, ENISA has reported a significant increase in Denial of Service (DoS) attacks targeting the availability of systems in 2023, identifying them as one of the most prominent and rapidly growing threats [44].

15.3.5 Healthcare Cybersecurity Challenges

The healthcare sector faces unique cybersecurity challenges. Traditionally focused on patient care, healthcare institutions often lack robust cybersecurity measures. Human error is a significant factor, with many security incidents resulting from inadequate training and awareness among healthcare professionals [45]. The global shortage of cybersecurity professionals has long been recognized as a critical issue (ENISA 2020; NIST 2020), and it now looms as one of the most formidable challenges for the future [46, 47]. This crisis is starkly reflected in the ISC2 Cybersecurity Workforce Study, which reveals a staggering 26.2% increase in the global cybersecurity workforce gap since 2021, amounting to a shortfall of 3.4 million professionals required to adequately safeguard critical assets [48]. This challenge is particularly pronounced in the healthcare sector, where the stakes are immeasurably high [49]. The complexity of securing medical devices magnifies the issue, as cybersecurity specialists in this field need a distinct skill set and expertise in comparison to traditional IT security engineers or architects [50].

Legacy medical devices, which were designed before current cybersecurity threats emerged, present another major challenge. Many of these devices use outdated software and hardware, making them vulnerable to attacks. For example, some devices still operate on unsupported operating systems like Windows XP and even Windows 98 [51]. Financial constraints often prevent the updating or replacement of these devices, leaving them exposed to cyber threats.

15.4 Understanding the Nature of Connected Medical Devices (CMDs)

Modern medical devices, now capable of generating, collecting, analyzing, and transmitting health data, are increasingly connected to the Internet, forming the Internet of Medical Things (IoMT). While IoMT offers benefits such as real-time monitoring and improved patient care, it also expands potential attack surfaces. Each connected device represents a potential entry point for cyber threats, and attacks on one device can compromise the entire system [52]. With the rapid evolution of sophisticated AI-driven cyberattack techniques, the potential for malicious

applications is constrained only by the ingenuity and imagination of the attacker. As these technologies advance, the scope of possible threats will continue to expand, posing unprecedented risks to IoMT environment and hospital infrastructure.

15.5 The Regulatory Framework in Focus: AIA and MDR

The AIA and the MDR pertain to regulating AI-driven medical technologies. Accordingly, the following section enters into the analysis of AIA and MDR by providing a comprehensive overview of the AIA, outlining its objectives, scope, and classification of AI systems based on risk. This will be followed by an analysis of the MDR, focusing on its requirements for the safety, performance, and compliance of medical devices incorporating AI components. In addition, analyzing the interaction between the AIA and MDR is crucial for several reasons. First, the intersection of these two frameworks is essential to ensure that AI systems used in medical devices are both innovative and safe. The AIA introduces a comprehensive framework for the classification and regulation of AI systems based on their risk to fundamental rights and safety. At the same time, the MDR focuses on the safety and performance of medical devices, including those that incorporate AI technologies. Second, AI-driven medical devices have the potential to significantly enhance patient care but also pose unique risks due to their complexity and the potential for unpredictable behaviour. Ensuring that these devices meet stringent safety and performance standards is crucial for patient safety and public trust in healthcare technologies. Therefore, the final subsection will explore the interaction between these two regulatory frameworks, highlighting areas of alignment and potential conflicts, particularly in the context of ensuring the cybersecurity and reliability of connected medical devices.

15.5.1 The AI Act

The AI Act, published in the European Journal on July 12, 2024, represents landmark legislation aimed at regulating artificial intelligence technologies across various sectors. As the world's first comprehensive legal framework dedicated to artificial intelligence, the AI Act seeks to foster the development of human-centered and trustworthy AI technologies. At the same time, it aims to safeguard individuals' health, safety, and fundamental rights from the potentially harmful impacts of AI-powered systems (Article 1(1)). Its primary goal is to mitigate risks to health, safety, and fundamental rights associated with AI systems. Notably, the AI Act adopts a sector-agnostic approach, applying uniformly across various sectors such

as finance, education, transportation, and healthcare. This broad application establishes a coherent set of regulatory principles for AI systems, regardless of the specific field in which they are implemented. With its wide scope of application, the AI Act will have a significant impact on industries, including the medical devices sector, which is already navigated by the complex regulatory framework. However, it is important to acknowledge that AI is not a new player in the healthcare domain.

AI has made notable advancements in healthcare, improving diagnostic accuracy, personalizing treatment plans, and enhancing patient outcomes. AI technologies have already been integrated into medical devices for advanced imaging, predictive analytics, and even robotic surgeries. These AI-driven devices have played a crucial role in transforming medical practices, particularly in diagnosis and treatment [53]. Despite the transformative potential of AI in medical devices, these innovations are subject to strict regulatory oversight. For example, many AI-powered medical devices have been CE-marked under the now-repealed Medical Device Directive (MDD), and now must comply with the more stringent MDR, which became fully applicable in 2021 [54]. Nevertheless, scholars have pointed out that the MDR may not fully address the unique characteristics of AI technologies, particularly their autonomous decision-making capabilities and learning algorithms [55, 56].

The AI Act introduces additional regulatory obligations for medical device manufacturers, who will now be required to comply with both the MDR and the new AI Act. This dual compliance will introduce another layer of complexity to the already intricate regulatory landscape for the medical device industry. Under Article 6(1) of the AI Act, most AI-based medical devices will fall under the category of "high-risk AI systems" because medical device software classified as Class IIa or higher will need to undergo third-party conformity assessments. The Act also introduces new requirements in areas such as data governance (Article 10), record-keeping (Article 12), and human oversight (Article 14), among others, that medical device manufacturers must adhere to in addition to the MDR requirements.

While the AI Act touches upon cybersecurity concerns through several recitals and articles, it does not serve as standalone cybersecurity legislation. In Recital 76, the Act emphasizes the critical role of cybersecurity in ensuring AI systems remain secure against malicious exploitation, alterations, or disruptions that could compromise their safety, behavior, and performance. Article 15 of the Act also integrates cybersecurity with broader considerations of accuracy and robustness, prescribing that high-risk AI systems should be designed to achieve and maintain an appropriate level of cybersecurity throughout their lifecycle (AI Act, Article 15(1)). Nevertheless, some scholars argue that these cybersecurity requirements are vaguely defined and lack specific guidelines for practical implementation [57].

Moreover, the AI Act does not directly reference the cybersecurity definition provided in the Cybersecurity Act (Regulation (EU) 2019/881), a significant omission

noted by experts. By not incorporating the Cybersecurity Act's definition, the AI Act may fall short of fully aligning with established cybersecurity principles, which could have strengthened the link between AI-specific and broader cybersecurity protections [58]. This omission creates further ambiguity regarding the implementation of cybersecurity requirements for high-risk AI systems and leaves open questions about how AI developers and manufacturers should integrate cybersecurity considerations into their development processes.

In conclusion, while the AI Act represents a significant step toward regulating artificial intelligence technologies, its interplay with the MDR, particularly in the context of AI-powered medical devices, raises several practical challenges. Legal uncertainty, overlapping obligations, and cybersecurity ambiguities underscore the need for detailed guidance and clear standards to help manufacturers navigate this complex regulatory landscape. Ongoing standardization efforts, alongside industrial guidelines, will be critical in supporting the practical implementation of these requirements to ensure both regulatory compliance and the safe deployment of AI systems in healthcare.

15.5.2 The Medical Device Regulation (MDR)

The Medical Devices Regulation (MDR) is one of the most critical pieces of legislation in the European Union (EU) governing the cybersecurity of medical devices. Introduced to replace the "outdated" Medical Device Directive (MDD), the MDR addresses the increasing risks posed by rapid technological advancements in healthcare, particularly in the domain of connected and software-driven medical devices. As medical devices become more integrated with digital technologies, they also become more vulnerable to cyberattacks, necessitating stronger regulatory measures. The MDR thus imposes more stringent requirements for ensuring the safety, performance, and cybersecurity of medical devices before they can be placed on the EU market or used within the EU [59].

One of the core elements of the MDR is compliance with cybersecurity rules outlined in its General Safety and Performance Requirements (Annex I). Article 5(2) of the MDR specifically mandates that manufacturers of medical devices, particularly those incorporating electronic programmable systems or software, demonstrate compliance with essential cybersecurity standards. This regulation is designed to mitigate the risks posed by cyber threats that can compromise device safety, performance, and patient data [60]. This is particularly important in light of recent trends in the healthcare sector, where cyberattacks targeting medical devices have increased, leading to potential risks to patient safety [61].

The definition of a medical device under Article 2(1) MDR is broad, encompassing a wide range of instruments, apparatuses, software, implants, and other

materials intended for medical purposes. This includes devices for diagnosis, monitoring, prevention, or treatment, ranging from basic items like disposable gloves and plasters to more complex devices such as pacemakers and radiation systems [62]. This broad definition highlights the importance of cybersecurity measures across the entire spectrum of medical devices, as even seemingly simple devices can pose significant cybersecurity risks if left unprotected.

To assist manufacturers in complying with the cybersecurity requirements of the MDR, the Medical Device Coordination Group (MDCG) endorsed the Guidance on Cybersecurity for Medical Devices (MDCG 2019-16 Rev.1). This guidance provides a comprehensive framework for manufacturers to integrate cybersecurity considerations into the design and development of their devices, marking a significant step forward in implementing the MDR's cybersecurity provisions [63]. However, the dynamic nature of medical device cybersecurity has evolved significantly since the MDCG Guidance was first issued in 2019. Scholars such as Biasin and Kamenjasevic have identified areas where further refinement is necessary, including clarifying the concept of joint responsibility between different stakeholders and improving terminological consistency across the regulatory framework [64].

The introduction of the NIS2 Directive has further complicated the landscape for medical device manufacturers, adding an additional layer of regulatory complexity. NIS2, which focuses on strengthening cybersecurity for critical infrastructure sectors, intersects with the MDR in the realm of medical device cybersecurity, raising questions about how these regulations will work simultaneously (European Commission, 2023). This overlap highlight the importance of aligning various EU cybersecurity frameworks to ensure clarity and ease of compliance for medical device manufacturers. Moreover, it has become evident that updates to the MDCG Guidance will be necessary to reflect the evolving regulatory and technological landscape.

In conclusion, the MDR represents a critical regulatory advancement in ensuring the cybersecurity of medical devices. However, the rapidly changing nature of both technology and the EU's broader cybersecurity framework, such as the introduction of NIS2, presents new challenges. As scholars have noted, it is imperative to continuously refine and update both the MDR and supporting guidance documents like the MDCG Guidance to keep pace with these developments, ensuring that manufacturers can effectively navigate the complex regulatory environment and protect patient safety.

15.5.3 Discussion: The Interplay Between the AIA and MDR

The AI Act and the Medical Devices Regulation (MDR) both aim to ensure the safety, performance, and ethical use of advanced technologies in healthcare, but

their approaches and focus areas reveal significant differences. The common goal of these two regulatory frameworks is to protect public health and safety while fostering innovation. Both the AI Act and the MDR address the integration of complex software systems in medical devices, including artificial intelligence (AI), to ensure that they meet high safety and quality standards.

The MDR, which came into force in 2021, focuses on ensuring the safety and performance of medical devices throughout their lifecycle. It imposes rigorous requirements on manufacturers regarding the design, testing, and post-market surveillance of devices, including those driven by AI. On the other hand, the AI Act, though addressing broader AI applications beyond healthcare, introduces specific regulations to mitigate risks associated with AI systems, especially those classified as "high-risk"—which includes most AI-driven medical devices.

Despite their complementary goals of user protection and trust-building, the AI Act and MDR adopt different approaches to risk, reflecting their distinct regulatory priorities and scopes. The MDR's device-centric framework, which focuses on the physical and technical risks associated with medical devices, is a crucial aspect of ensuring the safety, efficacy, and reliability of these devices. This rigorous approach, which includes pre-market conformity assessments, classification systems, and performance standards, aims to mitigate risks such as device malfunction, improper usage, or potential harm to patients and users. It directly addresses the medical device design and intended purpose, providing a solid foundation for user trust.

In contrast, the AI Act shifts the focus to broader societal and human-centric risks, aligning with a human-rights-based regulatory philosophy. It addresses risks arising from the deployment and operation of AI systems, such as biases in decision-making, threats to data privacy, and the erosion of transparency and accountability. Key provisions, such as those on data governance and human oversight (Article 14), aim to safeguard fundamental rights by ensuring fairness, non-discrimination, and user autonomy. It emphasizes requirements for ensuring AI systems' accuracy, robustness, and cybersecurity (Article 15), which complements but does not directly mirror the MDR's device-centric regulatory framework.

This divergence in focus—device regulation under the MDR versus human rights and societal impacts under the AI Act—creates a complex and often conflicting regulatory landscape. Stakeholders must navigate these frameworks, each with its distinct priorities: the MDR's focus on mitigating tangible risks related to the physical safety and performance of medical devices, and the AI Act's broader, more abstract emphasis on protecting human rights, ensuring fairness, and managing societal impacts of AI systems. While both frameworks aim to ensure safety and trust, the stark difference in their approaches introduces tension, as the MDR's product-centric risk management contrasts sharply with the AI Act's focus on ethical and societal risks that transcend individual devices. This creates additional

challenges for stakeholders tasked with reconciling the two regulatory approaches in practice.

The amalgamation of regulations is expected to lead to increased compliance expenses for manufacturers of medical devices, as they must ensure their products meet the stringent requirements of both legal frameworks. Several scholars have already raised concerns about potential duplication and inconsistencies in the regulatory overlap between the MDR and the AI Act, which could complicate compliance efforts [65]. Moreover, the AI Act's requirements are outlined at a high level, lacking detailed specifications that would clarify their practical implementation. This lack of granularity can lead to legal uncertainty for manufacturers, who may struggle to understand how to fully comply with the overlapping regulations.

Focusing on the potential duplication of regulatory requirements, AI-driven medical devices will likely fall under both the MDR and the AI Act. For example, Article 6(1) of the AI Act classifies medical device software that falls into Class IIa or higher under the MDR as a high-risk AI system, thus triggering additional requirements under the AI Act. These include obligations related to data governance (Article 10), record-keeping (Article 12), and human oversight (Article 14), which overlap with but are distinct from MDR requirements [66]. Navigating this dual compliance could lead to increased complexity and costs for manufacturers, who will need to meet both sets of requirements without clear guidelines on how these obligations interrelate. However, there are also opportunities for harmonization, particularly in the development of industrial standards and guidance documents that bridge the regulatory gap between the MDR and the AI Act. The European Commission's standardization requests to CEN and CENELEC aim to facilitate this alignment, but the process is complex and time-consuming [87]. Moreover, the Medical Device Coordination Group (MDCG) Guidance could be revised to incorporate AI-specific risks and to provide clear direction on how manufacturers can comply with both MDR and AI Act requirements coherently. These opportunities highlight the importance of collaborative efforts between regulators, industry stakeholders, and standards bodies to streamline compliance and reduce the regulatory burden on the MedTech industry.

15.6 AI Risk Management

The purpose of a risk management framework (RMF) is to assist the organization in integrating risk management into significant activities and functions [67]. Risk management refers to the coordinated activities to direct and control an organization with regard to risk [68]. Risk is defined as the effect of uncertainty on objectives and is usually expressed in terms of:

- risk sources, i.e. elements which alone or in combination have the potential to give rise to risk;
- potential events, i.e. occurrences or changes of a particular set of circumstances;
- their consequences (or impacts), i.e. the outcome of an event, affecting objectives;
- and their likelihood, i.e. the chance of something happening [69].

Impact and likelihood can be quantitatively or qualitatively estimated, in order to assist in decision making.

An AI RMF is a framework focused on AI systems that can, for a given set of goals, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments [70].

In order to understand what risks are AI technologies subject to, the characterization of what is desirable and what is not desirable helps guide the further definition of the risks to be mitigated. This characterization can be reflected in general principles for AI systems. The OECD organization defined the Principle for Trustworthy AI [71]. As stated in this document, the objective is to "guide AI actors in their efforts to develop trustworthy AI and provide policymakers with recommendations for effective AI policies". "Countries use the OECD AI Principles and related tools to shape policies and create AI risk frameworks, building a foundation for global interoperability between jurisdictions." These principles are:

- **Inclusive growth, sustainable development and well-being** – "Stakeholders should proactively engage in responsible stewardship of trustworthy AI in pursuit of beneficial outcomes for people and the planet, such as augmenting human capabilities and enhancing creativity, advancing inclusion of underrepresented populations, reducing economic, social, gender and other inequalities, and protecting natural environments, thus invigorating inclusive growth, well-being, sustainable development and environmental sustainability [72]."
- **Human rights and democratic values, including fairness and privacy** – "AI actors should respect the rule of law, human rights, democratic and human-centred values throughout the AI system lifecycle. These include non-discrimination and equality, freedom, dignity, autonomy of individuals, privacy and data protection, diversity, fairness, social justice, and internationally recognised labor rights. This also includes addressing misinformation and disinformation amplified by AI, while respecting freedom of expression and other rights and freedoms protected by applicable international law. To this end, AI actors should implement mechanisms and safeguards, such as capacity for human agency and oversight, including to address risks arising from

uses outside of intended purpose, intentional misuse, or unintentional misuse in a manner appropriate to the context and consistent with the state of the art [73]."

- **Transparency and explainability** – "AI Actors should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art:
  - to foster a general understanding of AI systems, including their capabilities and limitations,
  - to make stakeholders aware of their interactions with AI systems, including in the workplace,
  - where feasible and useful, to provide plain and easy-to-understand information on the sources of data/input, factors, processes and/or logic that led to the prediction, content, recommendation or decision, to enable those affected by an AI system to understand the output, and,
  - to provide information that enable those adversely affected by an AI system to challenge its output [74]."
- **Robustness, security and safety** – "AI systems should be robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose unreasonable safety and/or security risks. Mechanisms should be in place, as appropriate, to ensure that if AI systems risk causing undue harm or exhibit undesired behaviour, they can be overridden, repaired, and/or decommissioned safely as needed. Mechanisms should also, where technically feasible, be in place to bolster information integrity while ensuring respect for freedom of expression [75]."
- **Accountability** – AI actors should be accountable for the proper functioning of AI systems and for the respect of the above principles, based on their roles, the context, and consistent with the state of the art. To this end, AI actors should ensure traceability, including in relation to datasets, processes and decisions made during the AI system lifecycle, to enable analysis of the AI system's outputs and responses to inquiry, appropriate to the context and consistent with the state of the art. AI actors, should, based on their roles, the context, and their ability to act, apply a systematic risk management approach to each phase of the AI system lifecycle on an ongoing basis and adopt responsible business conduct to address risks related to AI systems, including, as appropriate, via co-operation between different AI actors, suppliers of AI knowledge and AI resources, AI system users, and other stakeholders. Risks include those related to harmful bias, human rights including safety, security, and privacy, as well as labor and intellectual property rights.

Also important for risk management of AI systems is understanding how AI systems are designed, built, deployed, updated and finally decommissioned. In another published work from the OECD, the "OECD Framework for the Classification of AI systems", the AI lifecycle activities were defined [76]. In this document, the OECD developed a user-friendly tool to evaluate AI systems in specific contexts, from a policy perspective, to help policy makers, regulators, legislators, among others, to characterize AI systems. The AI lifecycle activities, according to five sociotechnical dimensions, are the following:

- **People and Planet:** this dimension includes several considerations about the implementers of the AI systems, the users of the AI system, the impacted stakeholders, the type of impacts on environment, societal impacts and human rights. For example, consumer protection and product safety considerations lie within this dimension. Stakeholders include all organizations and individuals involved in or affected by the AI systems [77].
- **Economic context:** the context refers to the industrial sector, business function of the organization, and the adequate AI model to be used, scale of use and maturity of the AI system [78]. It also considers the criticality of the AI system, depending on the industry, business function and environment of deployment.
- **AI model:** an AI model "is a computational representation of all or part of the external environment of an AI system – encompassing, for example, processes, objects, ideas, people and/or interactions that take place in that environment". There exists a multitude of AI models. They could be symbolic models (e.g., using human-generated logical representations), Statistical AI models (e.g., identify patterns based on data) or hybrid AI models (e.g., mixing symbolic and statistical AI models) [79].
- **Data and Input:** AI models need information in order to represent the external environment, whether it is data gathered by humans and automated tools, or expert knowledge. Data and Input refers to data that is used for training the AI model, or the input data from the environment that the AI system will process to yield outputs useful for the context of use.
- **Task & Output:** AI systems can perform the following tasks: recognition, prediction, personalization and decision-making. Depending on the level of integration with other systems, the AI system can have different levels of autonomy to perform actions on the environment. The outputs of an AI system could be recommendations, signal outputs for other systems, or even outputs for other AI systems for performing other tasks and/or actions.

This five sociotechnical dimensions were mapped to the AI system's lifecycle [80]. In the NIST AI Risk Management framework, the AI system's lifecycle

were further adapted and reflects the need for risk management coordinated activities to be present throughout the AI systems' lifecycle. The AI system's lifecycle, as per NIST AI Risk Management Framework and OECD Framework for the Classification of AI Systems includes the following phases:

- **Plan and Design:** this phase is dedicated to defining the AI system's concepts, objectives, underlying assumptions, context of use and technical, legal and ethical requirements. This phase will set the path to all the subsequent phases, as the objectives, assumptions and requirements will guide decisions concerning the training of data and AI models to be used, adequate methods of validating and verifying the model training process and the correct outputs of the AI model, and also guide the evaluation of the correct behavior in production environment.
- **Collect and Process Data:** In this phase, having the objectives and requirements in mind, the processes and technologies for selection, gathering, validation and cleaning of data are selected and implemented. These data are of crucial importance since it will be used by the AI model to build a representation of the context or environment defined in the previous phase.
- **Build and Use Model plus Verify and Validate:** With processed training data, the AI model is trained in order to gain the computational representation of the external environment where the AI system will be deployed. This phase will include processes for selecting the training data set and the testing data set, accuracy tests for the trained models, and might even include training and testing several different models and selection of the best fit for the context of use. Accuracy test, comparison of several different models, validation, interpretation of the output results is included in the Verify and Validate phase. Since the two phases are very directly linked, we described them in the same paragraph.
- **Deploy/Task and Output:** In this phase, pilot testing, compatibility check with surrounding systems, verification of regulatory compliance, organizational change management, actual implementation of the system in production, monitoring of user experience and impact to the systems' environment are performed;
- **Operate and Monitor:** Once deployed, the AI system will be part of the business operations and continuous monitoring and assessment is implemented, having in mind the objectives, legal and regulatory requirements, and ethical considerations [81].

Note that the OECD framework places **People and Planet** in the center of the framework.

Some risk examples for the lifecycle phases can be found below:

- **Plan and Design:** in the planning phase, legal, regulatory and ethical requirements must be considered. Social and environmental impacts should also be considered when designing an AI system. If some of these requirements are overlooked, ignored, or even purposely discarded, then the subsequent phases, might lead to a biased AI system.
- **Collect and Process Data:** training data will influence greatly the AI system's functioning. Ultimately, it could lead, for example, to a classification model that might favor certain groups of people in an unfair way. This might be caused by unbalanced data, biased sampling of data, or corrupted/purposely changed data. Training data could include Personal Data that might not have the owner's consent to be used. Data quality plays a key role in training models. If the data has several errors, the resulting trained model might be unreliable or unsafe for use.
- **Build and Use Model:** When training AI models, if the training data is not appropriately fed to the AI model, and if there is not much testing data for evaluating the "correctness of the model", overfitting or underfitting will most certainly lead to wrong AI outputs. AI architecture models could be adequate in certain scenarios, but inappropriate in others. The selection of the wrong architecture model can lead to unintended bias of the system, leading to biased outcomes.
- **Operate and Monitor:** Real-world scenarios always have unexpected situations. These situations could feed some input to the AI system, leading to dangerous behaviors. An AI system must be up-to-date and continuously trained with up-to-date data. Model drift happens when there is no mechanism for monitoring the adequacy of the model with regards to the changing AI system environment. This can lead to erroneous behavior.
- **Build and Use Model plus Verify and Validate, Deploy / Task and Output and Operate and Monitor:** Without explainability, or human understandable reasons for the AI outputs, it would be difficult for humans to interpret the result, and to take corrective actions. With explainability, people can assess better the "correctness" of the AI outputs taking into account other information not present during AI Model training.

Several standards related to AI risk management exists:

- The "ISO/IEC 23894:2023 – Information technology – Artificial intelligence – Guidance on risk management", published in 2023, provide guidance for organizations that develop, produce, deploy or use products, systems and services that utilize AI to manage AI related risks and to integrate risk management into the organization's processes.

- The "ISO/IEC 42001:2023 - Information technology—Artificial intelligence—Management system", published in 2023, provides requirements for setting up and continuously improving the Artificial Intelligence Management System for organizations providing or using AI-based products [82].
- The "ISO/IEC 38507:2022 - Information technology—Governance of IT—Governance implications of the use of artificial intelligence by organizations", published in 2022, this document provides guidance for governing the use of AI technology within an organization, specifically tailored for the organization's governing body [83].
- The NIST AI Risk Management Framework, published in 2023, was designed to enable organizations to increase the trustworthiness of AI systems, and foster responsible design, development, deployment and use of AI systems [84].

Focusing on the Cybersecurity risks of AI systems, Microsoft has released the AI Security Risk Assessment document, where they have suggested a rating scheme for severity, likelihood and impact, stressing the needed alignment with the specific industry and use case. The document also defines a set of control objectives for protecting AI systems against cyber-threats. Controls are any measure, whether procedural, managerial or technical, to mitigate or eliminate risks. Before delving into the controls, the organization must first inventory all the AI systems it is using or planning to use. The organization should assess the current state of AI within the organization, perform gap analysis, define recommendations from the results of the gap analysis, define the roadmap to implement these recommendations and have a progress monitoring process in place. Moreover, the AI systems should be scored based on their criticality for the organization, in order to prioritize protective measures implementation. Then, they must apply the adequate controls to fulfill the following objectives:

1. **Data Collection:** controls and policies for ensuring the integrity of data collected to be used by the AI system. These controls and policies protect the AI system against untrusted data sources, sensitive data misuse, insecure data storage, unauthorized data access and data integrity attacks.
2. **Data Processing:** controls and policies to secure the processing of data that will be used for training the AI model. These controls and policies protect the AI system against data processing pipeline manipulation (altering the intended processing of data) and data subsets reconstruction (recovery of parts of the dataset by an attacker).
3. **Model Training:** controls and policies for reviewing the AI model code. These controls and policies are intended for protecting the AI system from improper model design (which could lead to confidentiality, integrity or

availability breaches), adversarial conditions (e.g., where the AI system is exposed to adversarial attacks), and overfitting (which could lead to unintended behaviors that could be exploited by attackers).

4. **Model Deployment:** controls and policies related to the deployment of models, algorithms, and supporting infrastructure. These controls and policies are intended to protect the AI system against inadequate security testing of the model, and to protect the system from unsecured networks.
5. **System Monitoring:** Controls and policies for ongoing monitoring of AI systems and supporting infrastructure (e.g., securing log data and their infrastructure);
6. **Incident Management:** controls and policies related to securing log data and supporting storing infrastructure. These controls and policies ensure adequate definition of roles and responsibilities, AI systems incident reporting processes/technologies, and the definition of an incident response plan that should be tested regularly. These should guarantee a prompt response in case of AI system's incidents.
7. **Business Continuity Planning:** controls and policies to guarantee that the AI system can recover or can be remediated after an incident. These include the definition of Disaster Recovery Plan, Business Continuity Plan and continuous testing of those plans.

Regarding the data collection, data processing, data training and deployment environments, they could be all in-house for the organization, some parts could reside outside the organization, or all parts could reside outside premises. This would imply the adoption of cybersecurity standards, such as the ISO 27001/27002, CIS Cloud Security Controls, NIST Cybersecurity Framework for IoT (NISTIR 8259), OWASP IoT Security Guidelines, OWASP application security standard, to name a few. In the case of Medical Devices, the ISO 14971 standard must be considered if the AI system is deployed or somehow integrated in the medical device.

The complexity of considerations, standards and regulations, with an ever-changing landscape of the AI technology is posing enormous challenges to organizations. In the case of AI systems or Medical Device using AI systems, when regulation changes, the implications for the AI lifecycle and the whole functioning of an organization can be far-reaching. They can affect organizations' infrastructures (in-premise, cloud, or hybrid), systems integrated with AI (namely applications and sources of information), as well as providers' contracts and services.

Mapping and alignment of laws, regulations, standards, guidelines, and practices remains a challenge for organizations that aim at improving the implementation of compliance requirements and adopt best practices. As the AI landscape evolves, future AI risk management methods and frameworks should aim at being clear and

intuitive, as well as adaptable as part of an organization's broader risk management strategy and processes. Also, they should be outcome-focused and non-prescriptive, by providing requirements and recommendations on outcomes and approaches, rather than prescribe one-size-fits-all requirements [85].

15.7 Outlook: Recommendations and Future Directions

Summarizing above, the integration of AI into medical devices presents unique challenges for ensuring cybersecurity, particularly when considering the regulatory landscape governed by the AI Act and the Medical Devices Regulation (MDR). Addressing these challenges requires strategic alignment of regulations, implementation of best practices, and the adoption of new policy recommendations to safeguard both patients and healthcare systems.

To ensure the cybersecurity of AI-enabled medical devices, it is essential to align the requirements of the AI Act and the MDR. One strategy to achieve this is through the harmonization of standards across both frameworks, with an emphasis on shared definitions of critical concepts such as cybersecurity risks, vulnerabilities, and risk management. One of the solutions could be *development of a unified standard* that addresses both the cybersecurity requirements in the MDR (Annex I) and the robustness and accuracy requirements in the AI Act (Article 15).

Another critical solution is fostering *collaborative guidance documents* between the Medical Device Coordination Group (MDCG) and the European AI regulators to avoid duplication and conflicting requirements. By providing clear guidelines that bridge both frameworks, manufacturers would have a streamlined process for ensuring AI-enabled medical devices comply with both sets of cybersecurity provisions. This would involve identifying overlapping conformity assessments and ensuring that these assessments address both AI functionality and cybersecurity risks.

Given the complexity of AI-driven systems, adopting best practices for cybersecurity in AI-enabled medical devices is essential. One of the solutions could be *the implementation of a secure development lifecycle (SDLC) for AI systems*, where cybersecurity is integrated from the design phase through to post-market surveillance. This approach ensures that manufacturers proactively address cybersecurity vulnerabilities throughout the product lifecycle, aligning with both MDR and AI Act requirements.

In addition, *applying standards such as ISO/IEC 27001 (Information Security Management) and ISO/IEC 62304 (Medical Device Software – Software Life Cycle Processes)* can provide a robust framework for managing cybersecurity risks. These standards should be adapted to address the unique challenges posed by AI, such as ensuring the accuracy and transparency of AI algorithms (AIA Article 10)

while maintaining the integrity and reliability of data used in the device (MDR Annex I). *Risk assessment methodologies*, such as threat modelling and penetration testing, should also be embedded into the development of AI-driven medical devices, ensuring compliance with cybersecurity mandates under both the AI Act and MDR.

To improve regulatory coherence, several policy changes should be considered.

Firstly, *the revision of the MDCG Cybersecurity Guidance* (MDCG 2019-16) should be prioritized, incorporating new risks and challenges specific to AI-driven devices. The updated guidance could provide clear examples of cybersecurity requirements for high-risk AI systems as defined in the AI Act, ensuring that both AI-specific risks and traditional medical device cybersecurity are adequately addressed [86].

A second policy recommendation is *the development of a centralized regulatory body tasked with overseeing AI-enabled medical devices*. This body could facilitate coordination between AI regulators and medical device authorities, ensuring consistent enforcement of cybersecurity standards across both frameworks.

Additionally, *cross-border data-sharing policies should be clarified*, particularly as AI-enabled medical devices often rely on large datasets from different jurisdictions. *Enhancing international cooperation on data governance and cybersecurity standards* would ensure that AI systems are robust and secure across the EU.

As AI continues to evolve, future directions should be tailored to address emerging trends and technologies, ensuring that innovations are effectively integrated and regulated to meet evolving needs and challenges. Accordingly, several emerging trends will reshape the landscape of medical devices and their associated regulatory needs.

Edge AI—where AI computations are performed on-device rather than in centralized data centres—will become increasingly common in medical devices, particularly for real-time diagnostics and monitoring. This shift necessitates new approaches to cybersecurity, as data will no longer be transferred to a central server, thus reducing latency but increasing the risk of local vulnerabilities.

Another emerging trend is the growing use of federated learning in healthcare, which allows AI models to be trained across multiple decentralized devices without sharing sensitive patient data. While this addresses privacy concerns, it presents new cybersecurity challenges related to ensuring the integrity and security of the distributed data used in training models (European Commission, 2023). Regulatory frameworks will need to adapt to address these complexities, particularly around data integrity and model robustness in federated learning environments.

With the advent of these new technologies, regulatory needs will inevitably evolve. As AI systems become more autonomous and capable of decision-making in critical healthcare settings, the demand for explainability and transparency will

increase. The AI Act already highlights the importance of these principles (Article 13), but future iterations of the MDR and AI Act should incorporate stricter requirements for auditability and post-market surveillance specific to autonomous AI systems in medical devices.

Moreover, as medical devices become more connected and integrated into broader Internet of Medical Things (IoMT) ecosystems, interoperability standards will become critical. Regulatory frameworks must address the cybersecurity implications of interconnected devices, ensuring that vulnerabilities in one system do not compromise the entire network. This shift will also necessitate real-time regulatory monitoring and adaptive compliance mechanisms, allowing for faster responses to emerging threats.

15.8 Conclusion

This chapter has delved into the intersection of the AIA and the MDR within the context of cybersecurity for AI-enabled medical devices. We outlined the shared objectives and differing approaches of these regulatory frameworks, demonstrating their mutual aim of ensuring safety and efficacy while highlighting their distinct focus areas. The MDR emphasizes device performance and patient safety, while the AI Act emphasizes algorithmic robustness, transparency, and fairness.

Strategies for aligning the two regulations were discussed, underscoring the need for regulatory harmonization to streamline compliance and reduce complexity for manufacturers. The chapter also presented best practices and standards for securing AI-enabled medical devices, such as implementing a secure development lifecycle (SDLC) and leveraging established cybersecurity frameworks like ISO/IEC standards. Furthermore, policy recommendations were provided, including updating the MDCG Cybersecurity Guidance and establishing a centralized regulatory body to oversee AI-driven medical devices.

For policymakers, the analysis suggests the importance of revising and harmonizing the AI Act and MDR to address the unique cybersecurity challenges posed by AI in medical devices. It is crucial that cybersecurity guidelines remain consistent and avoid regulatory overlap to support innovation while safeguarding patient safety. Additionally, policymakers must consider future-proofing regulations as AI technologies and medical devices continue to evolve.

Declaration of Competing Interest

Authors of the book chapter declare not to have any conflict of interest.

Data Availability

No data was used for the research described in this article.

Acknowledgement

This work was carried out as part of the CYLCOMED [Cyber securitY tooLbox for COnnected MEdical Devices] project, which has received funding from the European Union's (Horizon Europe) research and innovation programme under grant agreement No 101095542.

References

[1] World Economic Forum (WEF). 2024. "The Global Risks Report 2024". Global Risks Report 2024 |World Economic Forum |World Economic Forum (weforum.org)

[2] The White House. 2021. "Executive Order on Improving the Nation's Cybersecurity". https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[3] Ursula von der Leyen. 2021. Speech "State of the Union 2021". September 15 2021, Strasbourg. State of the Union Address by President von der Leyen (europa.eu)

[4] The European Union Agency for Cybersecurity (ENISA). 2023a. "Health Threat Landscape". https://www.enisa.europa.eu/publications/health-threat-landscape.

[5] Federal Bureau of Investigation (FBI). 2023. "Internet Crime Report 2023". 2023_IC3Report.pdf

[6] Choi, D., Malvehy, M., et al. (2022). Artificial Intelligence in Medical Devices: Regulatory Overlap and Challenges in the EU. *European Journal of Medical Technology*, 5(4), 210–224.

[7] Malvehy, J., R. Ginsberg, L. Sampietro-Colom, J. Ficapal, M. Combalia, and P. Svedenhag. 2022. "New regulation of medical devices in the EU: impact in dermatology." Journal of the European Academy of Dermatology and Venereology 36, no. 3: 360–364. https://doi.org/10.1111/jdv.17830.

[8] Conor Stewart. (2024) "AI in healthcare - statistics & facts". Available at https://www.statista.com/topics/10011/ai-in-healthcare/#topicOverview.

[9] Yao, X., Zhang, Y., & Zheng, H. (2021). Deep learning in medical image analysis: A survey. *Neurocomputing*, 453, 1–14.

[10] Esteva, A., Kuprel, B., & Novoa, R. A. (2019). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115–118.
[11] Topol, E. (2019). Deep medicine: How artificial intelligence can make healthcare human again. Basic Books.
[12] Somashekhar, S. P., Mulgund, A., & Babu, S. (2018). Watson for Oncology and the future of clinical decision support in oncology. *Journal of Oncology Practice*, 14(12), 889–897.
[13] Liu, Y., Xu, Y., & Li, J. (2024). AI-driven integration of genomic and imaging data for improved cancer diagnosis and treatment planning. Nature Cancer, 7(1), 78–91. doi: 10.1038/s41571-024-00691-7.
[14] Banaee, H., Ahmed, M. U., & Loutfi, A. (2013). Data mining for wearable sensors in health monitoring systems: A review of the state-of-the-art. Journal of Biomedical Informatics, 46(5), 1–19.
[15] Miller, A., Mullen, A., & Thompson, A. (2020). Advances in pacemaker technology: The role of remote monitoring. Journal of Cardiac Failure, 26(12), 1100–1108.
[16] Battelino, T., Danne, T., & Philip, M. (2019). Clinical targets for continuous glucose monitoring. Diabetes Care, 42(6), 1150–1152.
[17] Beck, R. W., Riddlesworth, T., & Ruedy, K. J. (2017). Continuous glucose monitoring vs usual care in patients with type 2 diabetes receiving insulin: The DIAMOND randomized trial. JAMA, 317(4), 371–378.
[18] Gordon, P. B., Taourel, P., & Deslauriers, J. (2021). Artificial intelligence in ultrasound imaging: A review. Ultrasound in Medicine & Biology, 47(1), 112–122.
[19] Chen, J., Zhang, L., & Wang, X. (2023). Deep learning for automated detection and classification of diseases in chest X-rays. IEEE Transactions on Medical Imaging, 42(4), 1090–1102. doi: 10.1109/TMI.2023.3192378.
[20] Mittelstadt, B. D., Allo, P., & Taddeo, M. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1–21.
[21] Bertolini, R., Morrison, K., & Krause, D. (2021). IoT security challenges and risks in healthcare: A systematic review. IEEE Access, 9, 155621–155635.
[22] Van Eeten, M. J., & Mueller, M. (2013). Where is the governance in Internet governance? New media & society, 15(5), 720–736.
[23] Dunn Cavelty, M. (2018). Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy. European Security, 27(3), 338–355.
[24] Piggin, R. (2017). Motivations behind cyberattacks on healthcare systems. Cybersecurity Review, 9(2), 78–85.
[25] Humer, C., & Finkle, J. (2014). The black market for health data: An analysis of the illicit trade in electronic health records. Health Affairs, 33(12), 2102–2108.

[26] Stack, L. (2017). The black market value of healthcare data. Healthcare Data Security Journal, 11(1), 34–45.
[27] Javaid, M., Haleem, A., & Singh, R. P. (2023). Fraudulent activities and financial implications of healthcare data breaches. Journal of Healthcare Security, 15(2), 25–34.
[28] European Union Agency for Cybersecurity (ENISA). 2022. "NIS Investments 2022". https://www.enisa.europa.eu/publications/nis-investments-2022.
[29] IBM Security. 2023. "Cost of a Data Breach Report 2023". https://www.ibm.com/reports/data-breach.
[30] Silver, Julie K., David S. Binder, Nevena Zubcevik, and Ross D. Zafonte. 2016. "Healthcare hackathons provide educational and innovation opportunities: a case study and best practice recommendations." *Journal of medical systems*. DOI: 10.1007/s10916-016-0532-3.
[31] European Data Protection Board (EDBP). 2022. "Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations. Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations |European Data Protection Board (europa. eu)
[32] Porter, Sophie. "Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak". HealthCare IT News. March 19, 2020. Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak |Healthcare IT News.
[33] Howell, O'Neill Patrick. "Ransomware did not kill a German Hospital patient. 2020". MIT Technology Review. November 12, 2020. https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/.
[34] Waegemann, C. (1996). The impact of data breaches on patient privacy and employment opportunities. Health Information Management Journal, 14(2), 77–88.
[35] Wirth, Axel. 2017. "Hardly ever a dull moment: the ongoing cyberthreats of 2017." Biomedical Instrumentation & Technology 51, no. 5 (2017): 431–433. DOI: 10.2345/0899-8205-51.5.431.
[36] Pattnaik, Nandita, et al. 2023. "It's more than just money: The real-world harms from ransomware attacks." *International Symposium on Human Aspects of Information Security and Assurance*. Cham: Springer Nature Switzerland. 3. https://doi.org/10.1007/978-3-031-38530-8_21.
[37] European Commission: Joint Research Centre, Reina, V. and Griesinger, C., Cyber security in the health and medicine sector – A study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings, Publications Office of the European Union, 2024, https://data.europa.eu/doi/10.2760/693487.

[38] Levy-Loboda, Tamar, Eitam Sheetrit, Idit F. Liberty, Alon Haim, and Nir Nissim. 2022. "Personalized Insulin Dose Manipulation Attack and Its Detection Using Interval-Based Temporal Patterns and Machine Learning Algorithms." Journal of Biomedical Informatics. DOI: 10.1016/j.jbi.2022.104129.
[39] Allen, S. D., Gupta, A., & Wang, Y. (2019). The Risks of Cyberattacks on Medical Devices. Journal of Medical Devices, 13(2), 024501.
[40] Medtronic. "Security Bulletin". June 27, 2019 https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-508-paradigm.html.
[41] He, H., & Wu, D. (2018). Cybersecurity of Medical Devices: A Case Study of the Pacemaker and Implantable Cardioverter Defibrillator Vulnerabilities. *Journal of Biomedical Engineering*, 32(4), 123–135.
[42] The European Union Agency for Cybersecurity (ENISA). 2023. "Health Threat Landscape". https://www.enisa.europa.eu/publications/health-threat-landscape.
[43] European Union Agency for Cybersecurity (ENISA). 2022. "Threat Landscape for Ransomware Attacks 2022". https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks.
[44] European Union Agency for Cybersecurity (ENISA). 2023. "ENISA Threat Landscape 2023". https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
[45] Evans, Mark, Ying He, Leandros Maglaras, and Helge Janicke. 2018. "HEART-IS: A Novel Technique for Evaluating Human Error-related Information Security Incidents." *Computers & Security 80*, 74–89. https://doi.org/10.1016/j.cose.2018.09.002.
[46] National Institute of Standards and Technology (NIST). 2020. "Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future". Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce | CISA.
[47] European Union Agency for Cybersecurity (ENISA). 2023c. "Foresight 2030 Threats". https://www.enisa.europa.eu/publications/foresight-2030-threats.
[48] ISC2. 2023. "Cybersecurity workforce study". Cybersecurity Workforce Study (isc2.org).
[49] Kotz, David, Carl A. Gunter, Santosh Kumar, and Jonathan P. Weiner. 2016. "Privacy and security in mobile health: a research agenda." *Computer* 49, no. 6: 22–30. DOI: 10.1109/MC.2016.185.
[50] Ray, Arnab. 2021. "Introduction to Medical Device Cybersecurity." *Cybersecurity for Connected Medical Devices*, (2021): 1–28. https://doi.org/10.1016/B978-0-12-818262-8.00004-8.
[51] Slabodkin, Greg. "Legacy medical devices, growing hacker threats create perfect storm of cybersecurity risks". MEDTECHDIVE. June 22, 2021. https:

//www.medtechdive.com/news/legacy-medical-devices-growing-hacker-threats-create-medtech-cyber-risks/602157/.
[52] Yaqoob, Tahreem, Haider Abbas, and Mohammed Atiquzzaman. 2019. "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review." *IEEE Communications Surveys & Tutorials* 21, no. 4: 3723–3768. DOI: 10.1109/COMST.2019.2914094.
[53] Ibidem [11].
[54] Ibidem [6].
[55] Mkwashi, A. and I. Brass (2022). "*The Future of Medical Device Regulation and Standards: Dealing with Critical Challenges for Connected, Intelligent Medical Devices*". London: PETRAS National Centre of Excellent in IoT Systems Cybersecurity. DOI: https://zenodo.org/doi/10.5281/zenodo.7054048
[56] Le, S., Brass, R., & Mkwashi, M. (2023). AI and Autonomous Medical Devices: Regulatory Gaps in MDR. *Healthcare Robotics & AI*, 6(2), 76–90.
[57] Biasin, E., Yaşar, B., and Kamenjašević, E. 2023. "New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act ". *Law, Technology and Humans* 5 (2):43–58. https://doi.org/10.5204/lthj.3068.
[58] Biasin, E., Yaşar, B., and Kamenjašević, E. 2023. "New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act ". *Law, Technology and Humans* 5 (2):43–58. https://doi.org/10.5204/lthj.3068.
[59] Biasin, E., E. Kamenjasevic, and R.K. Ludvigsen. 2023. "Cybersecurity of AI Medical Devices: Risks, Legislation, and Challenges." ArXiv. https://doi.org/10.48550/arXiv.2303.03140.
[60] Ibidem [7].
[61] Ibidem [43].
[62] Ibidem [7].
[63] Biasin, Elisabetta, and Erik Kamenjasevic. 2020. "Cybersecurity of medical devices: regulatory challenges in the EU." https://dx.doi.org/10.2139/ssrn.3855491.
[64] Ibidem [63].
[65] Ibidem [6].
[66] Ibidem [6].
[67] ISO 31000:2018, https://www.iso.org/iso-31000-risk-management.html.
[68] ISO 31000:2018, https://www.iso.org/iso-31000-risk-management.html.
[69] ISO 31000:2018, https://www.iso.org/iso-31000-risk-management.html.
[70] NIST AI Risk Management Framework.
[71] https://oecd.ai/en/ai-principles.
[72] Ibidem [72].

[73] Ibidem [72].
[74] Ibidem [72].
[75] Ibidem [72].
[76] OECD Framework for the Classification of AI Systems
[77] Ibidem [77].
[78] Ibidem [77].
[79] Ibidem [77].
[80] Ibidem [77].
[81] NIST AI Risk Management Framework.
[82] https://www.iso.org/standard/81230.html.
[83] https://www.iso.org/standard/56641.html.
[84] Ibidem [68].
[85] Ibidem [68].
[86] Ibidem [59].
[87] European Commission: Joint Research Centre, Soler Garrido, J., Fano Yela, D., Panigutti, C., Junklewitz, H. et al., Analysis of the preliminary AI standardisation work plan in support of the AI Act, Publications Office of the European Union, 2023.