HEALTH AND WELLBEING

White Paper

The Future of Medical Device Regulation and Standards: Dealing with Critical Challenges for Connected, Intelligent Medical Devices

PETRAS in partnership with BSI

Authors

Andrew Mkwashi and Irina Brass

UCL Department of Science, Technology, Engineering and Public Policy

Acknowledgements

We would like to thank our project partners at BSI who provided invaluable expertise, guidance, and input at various stages of this report, especially to Rob Turpin (Head of Healthcare Sector), Paul Sim (Medical Devices Knowledge Manager), Emma Glass (University Partnership Manager) and Matthew Chiles (Educational Development Manager). This report does not represent their views and any errors or omissions remain those of the authors.

We would also like to express our utmost appreciation to all stakeholders representing regulatory bodies, software developers, device manufacturers, clinicians, and academic researchers who kindly provided their time and expertise at various stages of our research.

Special thanks go to the PETRAS Communications Team, especially Sarah Hardy (Communications Lead) and Katerina Papakyriakopoulou (Marketing and Communications Officer) for their invaluable support with the design and promotion of this White Paper.

Please cite this White Paper as

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. Publication available at: https://petras-iot.org/wp-content/uploads/2021/06/White-Paper-The-Future-of-Medical-Device-Regulation-and-Standards.pdf. DOI: 10.5281/zenodo.7054049

White Paper graphics and design by Katerina Papakyriakopoulou.

About the Authors

Dr Andrew Mkwashi is a Research Fellow at UCL Department of Science, Technology, Engineering and Public Policy, working on the Regulation and Standardization of Connected, Intelligent Medical Devices (Reg-MedTech) project, funded by the PETRAS National Centre of Excellence in IoT Systems Cybersecurity (EPSRC grant number EP/S035362/1).

Dr Irina Brass is an Associate Professor in Regulation, Innovation and Public Policy at UCL Department of Science, Technology, Engineering and Public Policy. She leads the Regulation and Standardization of Connected, Intelligent Medical Devices (Reg-MedTech) project, funded by the PETRAS National Centre of Excellence in IoT Systems Cybersecurity (EPSRC grant number EP/S035362/1). Dr Brass is a member of the BSI Standards, Policy and Strategy Committee (SPSC), as well as a member and former chair of the BSI IoT-1 Technical Committee.

The Reg-MedTech project has received UCL Research Ethics approval 22137.001.

Contents

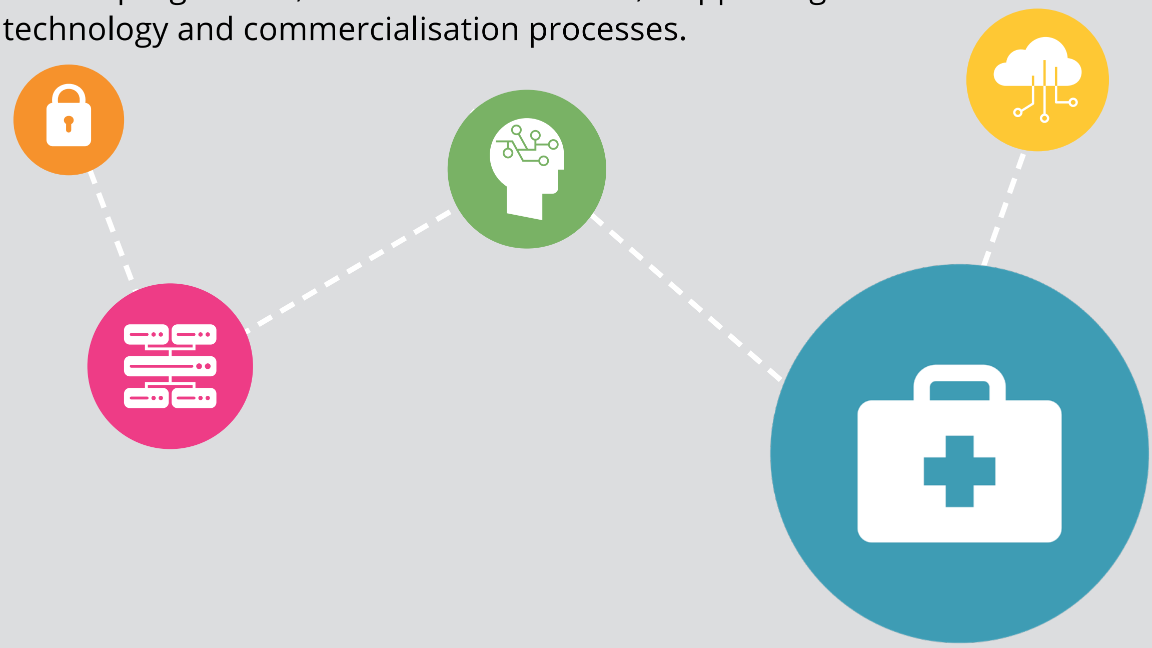
About PETRAS

The PETRAS National Centre of Excellence for IoT Systems Cybersecurity exists to ensure that technological advances in the Internet of Things (IoT) are developed and applied in consumer and business contexts, safely and securely. This is done by considering social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

To achieve our objectives, PETRAS works in collaboration with academia, industry and government partners to ensure our research can be directly applied to benefit society, business and the economy.

The Centre is a consortium of 23 research institutions and the world's largest socio-technical research centre focused on the future implementation of the Internet of Things. The research institutions are: UCL, Imperial College London, University of Bristol, Cardiff University, Coventry University, University of Edinburgh, University of Glasgow, Lancaster University, Newcastle University, Northumbria University, University of Nottingham, University of Oxford, University of Southampton, University of Surrey, Tate, the University of Warwick and Keele University.

As part of UKRI's Security of Digital Technologies at the Periphery (SDTaP) programme, PETRAS runs open, national level funding calls which enable us to undertake cutting edge basic and applied research. We also support the early adoption of new technologies through close work with other members of the SDTaP programme, such as InnovateUK, supporting demonstrations of new technology and commercialisation processes.



Executive Summary

New digital technologies and systems, such as the Internet of Things (IoT) or Artificial Intelligence (AI) tools that are typically implemented as software in medical devices or as medical devices themselves, are fuelling the digital healthcare sector's ongoing quest for better ways to diagnose and treat conditions proactively. When medical devices are connected to digital infrastructures such as the Internet, they can support the real-time transfer of important diagnostic data to information technology systems, where machine learning and AI can be used to quickly identify patient health patterns and anomalies. Despite the significant benefits that Connected, Intelligent Medical Devices (CIMDs) bring to the healthcare sector, different stakeholders such as manufacturers, software developers, clinicians, regulators and global standards organizations are facing several challenges around patient safety, effectiveness, transparency, accountability, and explainability of software and AI-based medical devices, as well as increased cybersecurity breaches and limited sectoral data governance frameworks necessary to ensure the safety, quality, and integrity of medical services, and ultimately patient trust. CIMDs are integrated in existing digital healthcare infrastructures in hospitals, general practice surgeries, patient care homes, and related health system services, generating new requirements to transfer, manage, store, and analyse health data. CIMDs can be wearable or implantable, acquiring physiological patient data or providing therapy outside the hospital setting, which brings new challenges for monitoring the performance, accuracy, and safety of these devices.

This White Paper reviews the main trends in the existing standards and regulatory landscape applicable to CIMDs. While the paper brings important information from several jurisdictions (UK, EU, USA) and highlights issues that are transnational in nature, affecting the healthcare sector as a whole, it has a predominant focus on UK and EU legislation and initiatives.

Based on interviews and a roundtable with key experts and practitioners in the field, the White Paper identifies several critical challenges that should inform the future development of standards and guidelines applicable to CIMDs, with a specific focus on artificial intelligence, cybersecurity, and data governance issues. The Paper provides valuable insights to regulators, standards-making bodies, notified bodies, manufacturers, software developers, clinicians, and researchers regarding present gaps and potential loopholes that CIMDs create in current regulatory frameworks, concluding with recommendations for standards development and initiatives in the context of widespread adoption of CIMDs in the healthcare sector.

Key Findings

This White Paper summarizes research that was carried out in the Reg-MedTech Project [1] based at UCL, between October 2021 and July 2022. Reg-MedTech investigates critical regulatory and standardization challenges for CIMDs. It is funded by the PETRAS National Centre of Excellence in IoT Systems Cybersecurity (EPSRC grant number EP/S035362/1).

We acknowledge that the current regulatory landscape for connected, intelligent medical devices is being redesigned in several key jurisdictions, including the UK where the Medicines and Healthcare products Regulatory Agency (MHRA) is updating its medical device regulations [2] and working on a forefront initiative called the “Software and AI as a Medical Device Change Programme” [3]. Due to these changes, our paper doesn’t comment directly on the clarity of the regulatory process for CIMDs. However, based on our extensive research with practitioners and experts in the field, we identify several critical areas that require further regulatory and legal clarity, where both standards and regulatory guidelines can be developed to support stakeholders through the development, implementation, testing, and post-market surveillance of connected, intelligent medical devices:

- **Liability concerns** resulting from the complexity of devices, their changing characteristics through updates and algorithmic learning, and questions about the distributed responsibility of several parties including software developers, device manufacturers, clinical staff operating the technology, patients or other end users.
- **Risk classification challenges**, especially resulting in modifications in the characteristics of medical devices, arising from potential exploitation of cybersecurity vulnerabilities or the limited predictability of their machine learning component.
- **Detecting and managing cybersecurity vulnerabilities**, especially in connected devices that do not have a clear vulnerability reporting, maintenance, and software update policy.
- **Interaction between new medical devices and legacy components** in the digital healthcare system, which can affect the performance of new devices and expose them to vulnerabilities and security attacks.
- **Assessing and communicating the transparency and explainability** of dynamic and deep learning-based medical devices.
- **Understanding and assessing types of bias** in training data and algorithmic learning in AI-based medical devices or AI as a Medical Device (AIaMDs).
- **Responsible and accountable data management across the lifecycle of a**

medical device, covering input, output, transfer, storage, and analytics. These measures should include **data quality and integrity controls** for software and AI-based medical devices, which are largely missing from standards and regulatory guidelines at the moment.

Recommendations

Based on the key findings above, **we make the following recommendations** for action by national and international standards-making bodies, regulators, and international harmonisation bodies such as the International Medical Device Regulators Forum (IMDRF):

1. National standards-making bodies can work closely with regulators to formalise an agenda for new standards and regulatory guidance development for connected, intelligent medical devices, especially AIaMDs. Priority areas for standards and guidance development include: addressing **software lifecycle management** issues for locked and adaptive algorithms used in or as medical devices, as well as **explainability and transparency** of AI as a component in medical devices or a standalone medical device.

2. National standards-making bodies can work jointly and in collaboration with international harmonisation bodies such as IMDRF to develop a new work programme that addresses **data governance** issues in medical devices, including data quality, data integrity, management, oversight, and audit processes in line with emerging regulatory frameworks such as Art 10 in the proposed EU AI Act.

3. International standards-making bodies can prioritise the development of a single standard addressing **cybersecurity of connected medical devices**, which should include legacy device cybersecurity, in order to avoid duplication of device cybersecurity standards and address the critical need to update general health informatics standards.

4. Regulators can provide further guidance on **the responsibilities and obligations of critical stakeholders** in the development, deployment, use and monitoring of connected, intelligent medical devices, so that their integrity, safety, and performance can be ensured.

5. National and international guidance needs to be provided to support **clinical and administrative staff** in hospitals and other healthcare facilities to understand and monitor the performance of connected, intelligent medical devices deployed and used on their premises, and how to record and report incidents triggered by cybersecurity, algorithmic, or data integrity breaches or failures.

List of abbreviations

AI	Artificial Intelligence
AIaMD	AI as Medical Device
AIMDD	Active Implantable Medical Device Directive (90/385/EEC)
ANSI	American National Standards Institute
BSI	British Standards Institution
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CIMDs	Connected, Intelligent Medical Devices
GDPR	General Data Protection Regulation
EC	European Commission
ETSI	European Telecommunications Standards Institute
EU	European Union
FDA	United States Food and Drug Administration
IMDRF	International Medical Device Regulators Forum
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IVDMDD	EU In-vitro Diagnostic Medical Device Directive (98/79/EC)
IVDR	EU In-vitro Diagnostic Medical Devices Regulation (2017/746)
JTC 1	Joint Technical Committee 1 (joint ISO and IEC Committee)
MDD	EU Medical Device Directive (93/42/EEC)
MDR	EU Medical Device Regulation (2017/745)
MEDDEV	Medical Device Guidance Documents
MHRA	UK Medicines and Healthcare products Regulatory Agency
ML	Machine Learning
NIST	National Institute for Standards & Technology
SaMD	Software as Medical Device

Glossary

Artificial Intelligence: refers to "the design and study of machines that can perform tasks that would have previously required human (or other biological) brainpower to complete" [4]. "AI is a branch of computer science, statistics, and engineering that uses algorithms or models to perform tasks and exhibit behaviours such as learning, making decisions, and making predictions" [5].

Connected, Intelligent Medical Devices: medical devices that are or incorporate software and artificial intelligence tools, and use communication technologies, networks, and cloud services to transfer, manage, store, and analyse health data.

Cybersecurity: "the protection of devices, services and networks – and the information on them – from theft or damage" [6].

Machine Learning (ML): is "an artificial intelligence technique that can be used to design and train software algorithms to learn from and act on data. Software developers can use machine learning to create an algorithm that is 'locked' so that its function does not change, or 'adaptive' so its behaviour can change over time based on new data" [7].

AI-based medical devices: medical devices that employ artificial intelligence or machine learning software as a component of the device, generally used to perform a specific task based on performance and outcome measures. "AI, and specifically ML, are techniques used to design and train software algorithms to learn from and act on data" [8]. Some AI/ML-based medical devices are locked beyond the original market authorization, while others can adapt over time.

AI as Medical Device (AIaMD): Artificial Intelligence as a medical device (AIaMD) refers to a type of software as a medical device (SaMD) [9].

Software-based medical devices: "are medical devices that incorporate software or are software, including software as a medical device, or software that relies on particular hardware to function as intended" 10].

Software as Medical Device (SaMD): The term Software as a Medical Device is defined as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device" [11].

Internet of Things (IoT): is defined as "an infrastructure of interconnected entities, people, systems and information resources together with services, which processes and reacts to information from the physical world and from the virtual world" [12]. The IoT infrastructure generally comprises of sensors performing data collection functions, transferring data via communication networks, cloud data processing, and some actuation where IoT devices change the properties of a physical entity or system in response to an input.

Internet of Medical Things (IoMT): "the collection of medical devices and applications that connect to healthcare IT systems through information and communication technologies to collect, store, exchange and process information" [13, pg.4]. Medical devices that have the ability to connect to networks for example via Wi-Fi, GPRS or cable based connectivity allow the machine-to-machine communication that is the basis of IoMT [13].

1. Introduction

The application of artificial intelligence (AI) in connected medical devices is on an exponential growth trajectory and is already leading to improvements in patient outcomes on a mass scale, as well as fundamental changes in the way that healthcare is delivered.

Connected, Intelligent Medical Devices (CIMDs) are medical devices that incorporate software, artificial intelligence tools, and use communication technologies, networks, and cloud services to transfer, manage, store, and analyse health data. These devices can be wearable or implantable, collect physiological patient data and/or provide therapeutic options. They can be software-based medical devices or standalone Software as Medical Device (SaMD) or AI as Medical Device (AIaMD). Some examples of such AI-based medical devices include imaging systems with significantly enhanced capabilities that use algorithms to detect lung cancer [14], devices that give diagnostic information for skin cancer, or an electrocardiogram (ECG) device that can be used to check one's heart rhythm and electrical activity or estimate the probability of a heart attack [15]. The devices themselves, the digital infrastructure that supports them, and the data collected are "creating the Internet of Medical Things (IoMT) – a connected infrastructure of medical devices, software applications, and digital healthcare systems and services" [16, pg.1].

However, with all the promise CIMDs offer, these powerful new technologies also introduce a number of critical vulnerabilities and significant risks to patient safety, their security, and fundamental rights, while also having the potential to disrupt the resilience of healthcare systems and continuity of service. Amidst the growing risk landscape applicable to CIMDs, regulators and policymakers in major jurisdictions are faced with substantial challenges including the need to provide the industry with clearer regulations, guidance, and standards to ensure that such devices work effectively and safely.

What is a Connected, Intelligent Medical Device (CIMD)?

CIMDs are medical devices that incorporate software, artificial intelligence tools, and use communication technologies and networks to transfer, manage, store, and analyse health data. These devices can be wearable or implantable, collect physiological patient data and/or provide therapeutic options. They can be software-based medical devices or standalone Software as Medical Device (SaMD) or AI as Medical Device (AIaMD). The devices themselves, the digital infrastructure that supports them, and the data collected are creating the Internet of Medical Things (IoMT) – a connected infrastructure of medical devices, software applications, and digital health systems and services.

1.1 Background: Emerging Risk and Policy Change

In an attempt to keep pace with rapidly evolving healthcare technologies, two new EU regulations on Medical Devices (MDR) and In Vitro Diagnostic Medical Devices (IVDR) were adopted in April 2017 [17, 18]. The new set of regulations raised the certification requirements for the production and distribution of medical products in the European Economic Area (EEA) [17] and had a staggered transition period. The MDR entered into force in May 2021 and the IVDR in May 2022, following the transition period. In brief, the classification requirements of medical devices under the MDR are based on a risk-based approach that “takes into account the vulnerability of a human body and the potential risks associated with the devices” [19, pg.4]. However, it has been noted that one of the challenges with these two new EU regulations is that they were not developed for (adaptive) AI or Machine Learning (ML) technologies, which have the potential to learn continuously and can potentially modify device performance in real time or near real time [8]. As noted in the specialist literature: “The distinctive characteristics of AIaMDs such as adaptive learning algorithms require a regulatory approach that spans the lifecycle of these technologies, allowing necessary steps to improve treatment while assuring safety outcomes” [20, pg 14].

In addition, the MDR does not provide comprehensive reference to cybersecurity in its main text. However, it provides some vital information security-related obligations that manufacturers have to comply with when placing medical devices on the market or putting them into service [21]. A critical cybersecurity concern is that all medical devices connected in the IoMT environment are directly or indirectly connected to each other and the Internet. The risk is therefore 'the weakest link in the chain'. The weakest link may be the hardware, the software, the communication interface, the use, or even the user(s). While IoT device security vulnerabilities are generally low-hanging fruit exploits [22], where the vulnerability lies is sometimes unknown, especially in more complex and interdependent clinical or medical settings [23].

Emerging policy and regulatory initiatives

Policymakers and regulators at global, regional, and national level have recognized the importance of regulation and the need for standards in emerging technologies such as artificial intelligence or machine learning, which have wide societal impact when applied across sectors. Some of the recent initiatives include the International Medical Device Regulators Forum (IMDRF)'s 2020 "Principles and Practices for Medical Device Cybersecurity" [24]; the World Health Organization's 2021 framework on "Generating Evidence for Artificial Intelligence-based Medical Devices" [25]; the FDA's 2021 "Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan"[7]; the European Union's 2018 "Declaration of Cooperation on Artificial Intelligence" that puts forward a pan-European approach to the governance and standardisation of AI technologies [26]; the European Commission's 2021 "Artificial Intelligence Act", which is a proposal that lays down harmonised rules for the governance of AI applications in the European Economic Area (EEA) [27]; the MHRA's 2021 "Software and AI as a Medical Device Change Programme" [3] (see Section 2.1 for a detailed review of the latest regulatory initiatives). However, the translation and applicability of these policy and regulatory advancements to the healthcare sector, and CIMDs in particular, remains unclear. This raises several questions such as: How will policy and regulatory requirements be translated into sector-specific guidelines? What standards and guidelines support these new regulatory changes? What AI, cybersecurity, or data governance standards or guidance documents are available for use in CIMDs, and are they adequate? What should organizations do to show conformity and compliance with current and forthcoming regulatory requirements?

Our study raised several questions: How will emerging digital technology policy and regulatory requirements be translated into sector-specific guidelines? What standards and guidelines support these new regulatory changes? What AI, cybersecurity, or data governance standards or guidance documents are available for use in CIMDs, and are they adequate? What should organizations do to show conformity and compliance with current and forthcoming regulatory requirements?

In addition, regulation has evolved to tackle critical cybersecurity threats, but the implementation of best practices in the development and management of connected devices remains challenging [28]. Yet, an adequate level of CIMDs cybersecurity is one of the most crucial elements that ensures patient safety and data protection in the daily provision of healthcare services and it is pivotal to mitigating risks that can potentially have a negative impact on healthcare or clinical outcomes [15]. The European Parliament noted that “the regulatory framework for AI must be developed with full respect for the rights enshrined in the Charter of Fundamental Rights, and in particular with respect to the principles of data protection, privacy and security” [29, para.L]. One of the ways to demonstrate and ensure that medical devices are designed and manufactured in a way that makes them safe to use, suitable for their intended purpose, and compliant with regulatory requirements is through the application of standards that represent the current state of the art. However, there are currently few standards that address cybersecurity, algorithmic integrity, and data governance issues – including input, output, communication, storage, and data analytics – at device level and also within the wider digital infrastructure that connects medical devices to each other and the healthcare system.

Thus, we are currently at an important junction in the regulation and standardization of CIMDs. On the one hand, we are seeing promising initiatives and debates on the evolution of overarching regulatory frameworks for cybersecurity and artificial intelligence, as well as several exciting initiatives about how medical device regulation and standards should adapt and evolve to this new reality, highlighting an increased level of awareness amongst critical stakeholders. On the other hand, this White Paper shows that more standards development and regulatory guidance work needs to be done to respond to the emerging challenges raised by CIMDs and to provide procedural clarity for critical stakeholders such as device manufacturers, software developers, and clinicians operating these devices on a day-to-day basis.

1.2 White Paper Objectives

This paper examines the regulation and standardization of CIMDs, as well as the critical challenges and risks faced by different stakeholders in the pre-market and post-market phases of the medical device product lifecycle. This is a pressing, yet under-researched area, at the intersection of cybersecurity and algorithmic governance in IoMT ecosystems, law and regulation, and digital healthcare. In order to paint an accurate picture of the status quo in this domain, the paper provides a comprehensive overview of the main published and in development standards and guidelines that apply to CIMDs, focusing mainly on initiatives from the UK, EU, and the US. The regulatory initiatives and standards are split into three categories pertaining to artificial intelligence, cybersecurity, and data governance. The research focuses on these three critical issue areas because they are key pillars of digital healthcare transformation.

The main question guiding this study is: *How and to what extent do current regulatory frameworks and standards address the critical challenges and unique risks posed by Connected, Intelligent Medical Devices (CIMDs)?*

In the paper, we identify seven areas highlighted by the stakeholders and the specialist literature consulted in this study as critical for further standards and guidance development, in order to provide clarity to current and emerging regulatory initiatives and to support stakeholders through the development, implementation, testing, and post-market surveillance of connected, intelligent medical devices (Section 4). These findings form the basis to our recommendations, which identify priority areas in the short and medium-term development of standards and guidelines for CIMDs.

1.3 Research Methodology

This White Paper summarizes research findings that were carried out in the Reg-MedTech Project at UCL between October 2021 and June 2022. Reg-MedTech is funded by the PETRAS National Centre of Excellence in IoT Systems Cybersecurity (EPSRC no EP/S035362/1). The research comprised of the following:

- Academic and grey literature review, including review of policy documents, legislation, and regulation;
- Expert commentary from members of the British Standards Institution (BSI),

especially representatives of the BSI Healthcare Sector;

- Interviews with 12 stakeholders including software developers, device manufacturers, clinicians, security practitioners, lawyers, standards-makers and regulators (Appendix A);
- A roundtable entitled "The Future of Medical Device Regulation and Standards: Dealing with Software Challenges", held on 27 April 2022, organized in collaboration with BSI and MHRA, with participation from key stakeholders across the IoMT ecosystem (Figure 1). The event offered attendees from the healthcare sector, regulatory agencies, standards-making organizations, professional associations, and academia an opportunity to convene and collectively discuss the critical opportunities and challenges arising from the deployment of CIMDs (Appendix B).

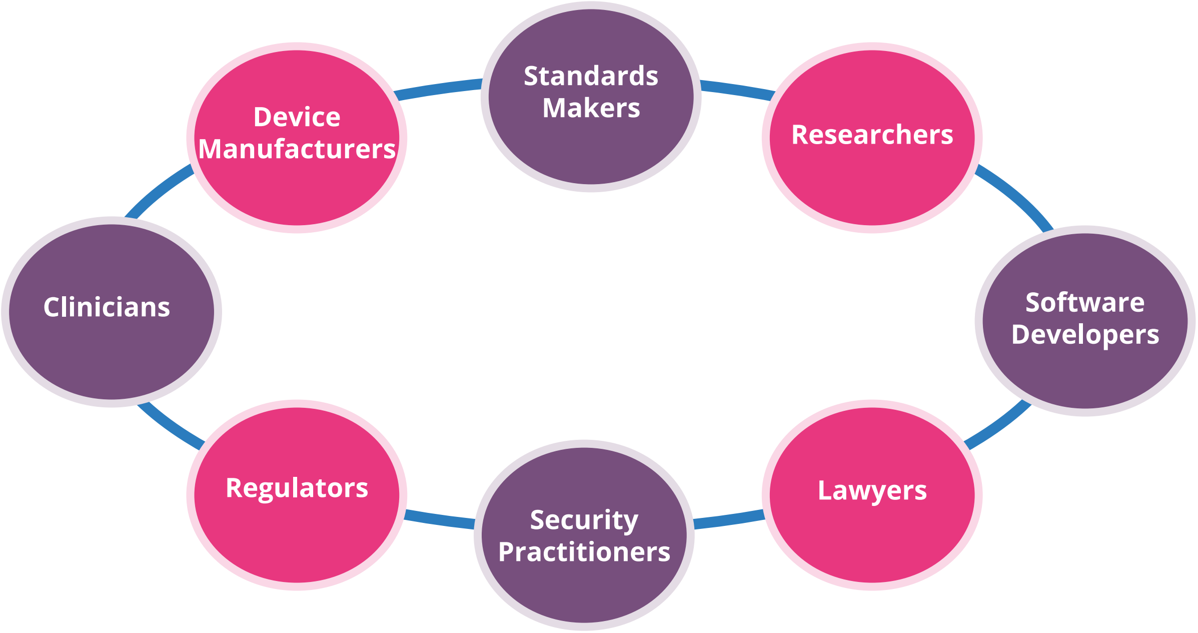


Figure 1: Representation of participants in the roundtable "The Future of Medical Device Regulation and Standards: Dealing with Software Challenges"

The roundtable opened with a plenary session featuring keynote talks from Johan Ordish (Head of Software and AI, Innovative Devices Division, MHRA) and Rob Turpin (Head of Healthcare Sector, BSI) covering the latest regulatory responses to software-based medical devices and how standards can best support these regulatory developments. The keynotes were followed by small group discussions addressing the main hurdles that software developers and device manufacturers face pre- and post-market to demonstrate conformity and ensure an appropriate level of cybersecurity, data governance, and integrity of algorithmic tools. Critical considerations about the deployment, use and monitoring of these devices in clinical settings were also addressed. Participants reflected on current gaps in regulatory guidelines and standards and discussed priority areas for future standards development.

We provide several expert and practitioner quotes derived from our interviews and the roundtable in this White Paper, which are captured in text boxes below.

2. Setting the Regulatory and Standards Landscape

Recognizing the potential of CIMDs to transform healthcare, public bodies in different jurisdictions have been taking policy and regulatory steps in the last few years towards advancing the development and uptake of safe and effective new healthcare technologies. However, the regulatory landscape applicable to CIMDs remains complicated and exhibits variation in scope across jurisdictions. Overall, in the last years, we have seen a variety of general framework regulations for cybersecurity and AI, as well as several principles, guidelines, and initiatives to support the uptake of digital solutions such as IoT or AI in healthcare, yet we continue to struggle to put all the pieces together and assess whether and how these initiatives fill current gaps in the implementation of medical devices regulation.

> *“The regulation of the AI space is very complicated and also overlaps in a lot of different regulatory authorities. This is a really challenging area, because there are so many different stakeholder interests, different regulatory policies and so many applications of AI. As such, having one regulation to rule them all will be very difficult because there will be individual challenges to different uses of AI”* (Manufacturer, interview-004, 2022).

2.1 Latest regulatory responses to connected, intelligent medical devices

Existing and emerging medical device regulations

To be lawfully marketed and put into service within the European Union, all medical devices and in vitro diagnostic medical devices must meet the CE marking requirements and comply with the relevant EU regulatory frameworks. In 2017, two major regulations were adopted, which are highly relevant for medical device "economic operators" such as manufacturers, authorized representatives, distributors or importers [30]. The two new regulations (EU Regulation 2017/745 on medical devices (MDR) and EU Regulation 2017/746 on in vitro diagnostic medical devices (IVDR)) are binding in their entirety and are directly applicable in all Member States [17, 18]. Prior to placing a medical device on the market and putting it into service, the device must undergo an assessment of conformity, in accordance with the procedures set out in Article 52 and Annexes IX to XI of the MDR, to demonstrate that it has fulfilled the requirements specified in the regulation and ensure that the safety and performance of the device is as intended [17, 30]. The conformity assessment followed is dependent on the classification of the device in accordance with Annex VIII of the MDR and its inherent risk type: by way of illustration, the higher the risk, the higher level of regulatory requirements and scrutiny [17]. The conformity assessment involves an audit of the manufacturer's quality system and, depending on the type of device, an assessment of technical documentation of at least one representative device per generic group as specified in Chapters 1 and 111 of Annex IX [30]. The MDR, which applies from May 2021, introduced more stringent requirements for medical device software. Any software providing prediction or prognosis of a disease or medical condition falls under the scope of the MDR. As a result, manufacturers must address more explicit and stringent requirements before and after placing their software on the market. However, because the two major regulatory changes that entered into force in 2017 were drafted at a time when the use of ML or AI in healthcare was in its inception, many aspects pertaining to these technologies were not explicitly considered, such as the continuous or lifelong learning of AI tools or the detection of biases in AI algorithms. In addition, there is still a need for clear guidelines on what specifically constitutes a 'device' when it comes to the use of software, which may lead to an increased number of "combination products" or "borderline" devices that are confusing the existing product classification scheme [30].

> Software with a medical purpose of "prediction and prognosis" falls within the scope of the MDR and IVDR.

In the UK, the regulatory landscape for medical devices is changing. Currently, medical devices are regulated under the Medical Device Regulation 2002 (UK MDR 2002). The route to market and UKCA marking requirements are derived from EU legislation prior to the implementation of the 2017 EU MDR, specifically Directive 90/385/EEC on active implantable medical devices (EU AIMDD), Directive 93/42/EEC on medical devices (EU MDD) and Directive 98/79/EC on in vitro diagnostic medical devices (EU IVDD) [31]. Recently, the MHRA consulted on a new proposal for medical device regulation following the UK's departure from the EU. In its response to the consultation, the MHRA recognises that "current medical device regulations contain few provisions specifically aimed at regulating SaMD or AIaMD" and makes several proposals for amendments to the definition of SAMDs and the classification rules for these devices [32].

In the USA, the FDA is responsible for regulating medical devices and radiation emitting products [33]. The FDA "controls all procedures for the admission of a medical device to the market" [30, pg.59] and evaluates device safety and effectiveness before and after it has reached the market [34]. Similar to the EU MDR, the FDA classifies medical devices using a risk-based approach whereby the device classification will generally indicate the regulatory pathway: Class I being the lowest risk, Class II moderate risk and Class III highest risk [15]. The intended use and reasons for using the device determines the risk profile of the device [35]. As the class of a device increases from I-III, the degree of risk also increases and, in turn, the regulatory controls and scrutiny are simultaneously intensified [36]. If a device is identified as Class I or II, and there are no exemptions present, a 510(k) application can be pursued [36]. A 510(k) provides a market access pathway "based on a new device being substantially equivalent to an already existing FDA-cleared device, known as the predicate device" [37, pg.193]. For class III devices, a premarket approval (PMA) application is needed, which is a much more stringent process that does not compare a device to existing ones, but relies heavily on device-specific data to determine its safety and performance, often generated through clinical trials [36].

Latest AI initiatives

Recently, several initiatives have been proposed to address the regulatory challenges posed by software as standalone medical device and, increasingly, the use of AI in or as a medical device. In 2021, the FDA issued the "Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan" [7]. The plan outlines necessary measures to update processes to keep pace with the needs of the ever evolving digital health technology market (including adaptive algorithms) and proposes initiatives for real-world device performance monitoring to manufactures and developers [7].

In 2021, the European Commission issued a proposal for an AI regulation (Artificial Intelligence Act), which lays down harmonised rules to govern AI applications in the European Economic Area (EEA) [27]. The proposal emerged in response to a considerable concern over the increasing use of "algorithmic decision-making systems" that are affecting social, economic, and fundamental rights [38, pg.1]. The aim of this proposal is to give users (professionals or individuals) and affected persons the confidence to adopt safe AI-based solutions, while encouraging businesses to develop them [27]. A dominant feature of the proposal is that it takes a risk-based approach and sets three main categories of risk (unacceptable risk, high risk, and low or minimal risk), which are relevant to AI systems that are within its scope [39]. The risk categories are fundamental in determining the regulatory consequences for different AI tools and systems. The AI Act proposal is "applicable for all AI application areas, and does not reflect the specificities and risks of AI in the healthcare domain" [40, p.iii]. Article 10 of the proposed AI Act provides for the governance of training, validation and testing data sets, using appropriate data governance and management practises to ensure that data used in high-risk AI systems satisfy the quality criteria laid down in paragraphs 2 to 5 of the Article [41].

In March 2022, the European Parliament published a "draft opinion" on the AI Act proposal [42]. The draft opinion places its focus mainly on issues pertaining to the European Parliament' Committee on Industry, Research and Energy (ITRE) competences but also broader issues related to enhancing innovation, competitiveness, research, sustainability and future changes in industry [42]. The draft opinion highlighted the need to lay out clearer guidelines for AI companies and the need to provide simpler tools and more efficient resources to economic operators to cope with the AI Act proposal [42]. The draft opinion called for the development and uptake of high but realistic AI standards for accuracy, robustness, cybersecurity, and data governance as they play a pivotal role in the development of safe AI applications that protect fundamental rights.

Due to the lack of globally recognised frameworks that assess evidence generated in the use of AI-based medical devices, in 2021, the World Health Organization (WHO) published a framework called "Generating Evidence for Artificial Intelligence-based Medical devices: A Framework for Training, Validation and Evaluation" [25]. The WHO framework is designed to provide several essential considerations used in the evaluation of clinical evidence regarding AIaMD, with the aim to assist in the formulation of a general agreement for guiding validation, evidence generation, and reporting across the total product lifecycle (TPL) within a global health context [25]. The framework is intended for current and future software developers, researchers, policy-makers and, other critical stakeholders involved in the development and deployment of AIaMD.

In May 2022, IMDRF published guidance N67 "Machine Learning-enabled Medical

Devices (MLMD): Key Terms and Definitions". The purpose of this guidance document is to raise awareness of key terms and definitions covering the Total Product Life Cycle (TPLC) to promote consistency, provide support for harmonization efforts at global level, and a foundation for the development of future guidelines related to MLMD [43]. This guidance document contains a reference to the BSI-AAMI "White Paper for Medical Device AI" [44], demonstrating how standards development organisations can connect standards thought leadership to regulatory thinking at an early stage.

To address some gaps in regulatory standards regarding software and AI as a medical device, the UK's Medicines and Healthcare products Regulatory Agency (MHRA) is currently working on a programme to develop a framework that seeks to lay out a high degree of patients and public protection, and at the same time provide an exciting opportunity to advance UK stakeholders' knowledge of responsible innovation for medical device software [3]. This initiative is called "Software and AI as a Medical Device Change Programme" and it includes eleven work packages across two workstreams, including packages focusing on AI rigour, interpretability, and adaptivity [3]. The scope of the programme activity so far consists of eleven work packages structured in two workstreams. The first aims to make fundamental reforms across the software as a medical device (SaMD) lifecycle. The second workstream reviews the critical challenges that AI can pose to current medical device regulatory frameworks and is made up of three work packages that operate in tandem with those described for software in general, focusing on AI rigour, interpretability, and adaptivity [3].

Similarly, in May 2022, Australia's Therapeutics Goods Administration (TGA) issued a draft guidance document on "Regulation of software based medical devices", which provides important "information on the regulation of software that meet the legislated definition of a medical device" [10]. This guidance is designed to assist manufacturers and sponsors to better understand how the TGA interprets requirements, and thus indicates how best sectoral economic operators can meet regulatory requirements.

Latest cybersecurity initiatives

In the USA, the FDA's Centre for Devices and Radiological Health (CDRH) published the following guidance documents that are relevant for CIMDs cybersecurity:

- 2018 Draft Guidance: "Content of Premarket Submissions for Management of

Cybersecurity in Medical Devices” [45]. The guidance outlines some beneficial industry recommendations regarding cybersecurity device design, device labelling, and technical documentation to be included in premarket submissions for devices with cybersecurity risk.

- 2022 Draft Guidance: “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions” [46]. This draft guidance supersedes the 2018 draft and indicates the significance of ensuring that medical devices are designed securely, enabling emerging cybersecurity risks to be mitigated throughout the Total Product Life Cycle (TPLC), and to outline the FDA’s recommendations more clearly for premarket submission content to address cybersecurity concerns [46]. Taken together, the recommendations are intended to support “security by design” principles.

In April 2019, the “EU Cybersecurity Act” presented “a cybersecurity certification framework for ICT products, services and processes”, which would also include connected devices [47]. The framework was designed with the aim to establish “a unified standard for cybersecurity certification and avoid a disjointed approach to product cybersecurity across different EU member states” [47]. The Act is one component in the EU’s strategic actions to upsurge information systems and data security. Soon after, the Medical Device Coordination Group (MDCG) published MDCG 2019-16 (July 2020) “Guidance on Cybersecurity for Medical Devices” [48]. The guidance provides manufacturers, distributors, and other key stakeholders with guidance on how to meet the relevant essential requirements of Annex 1 to the MDR and IVDR with regards to cybersecurity.

In 2021, Australia’s TGA put in place the “Medical Device Cyber Security Guidance for Industry” [49]. The guidance was created with the aim to assist Australia’s medical device cybersecurity capability, and incorporate improved cybersecurity practices throughout the medical device industry [49].

Worldwide, in 2020, the IMDRF’s Medical Device Cybersecurity Working Group published guidance on “Principles and Practices for Medical Device Cybersecurity” [24]. A foundational concept of this document is to ensure security is incorporated into the end-to-end lifecycle of a medical device. Currently, the working group is consulting on “Principles and Practices for the Cybersecurity of Legacy Medical Devices” [50]. The main aim of this important piece of work is to foster a harmonized approach to medical device cybersecurity at a global level and to provide medical device cybersecurity guidance for stakeholders throughout the device lifecycle [50].

Latest data governance initiatives

In 2020, the European Commission published "A European Strategy for Data", motivated by finding ways to ensure that society can make better decisions with "greater agency over data" [51]. There is also an emphasis on ensuring that Europe is competitive as a key player in the data economy by developing its connectivity capacities and cybersecurity. Furthermore, it stresses that there should remain strict protections and controls to ensure that the legal framework prioritizes data protection, fundamental rights, safety, and security [41]. The strategy formulates four vital principles: 1) a cross-sectoral governance framework for data access and use; 2) investments in data, capabilities, infrastructures, and interoperability; 3) building competences and skills; and 4) establishing common European data spaces. It also provides an international approach to making data available for European firms.

In November 2020, the European Commission issued a proposal regulation on European data governance ("Data Governance Act") as part of its 2020 Data Strategy [52]. The proposal puts forward the basis for the reuse of certain data types held by public sector bodies, such as confidential data or personal data in public databases. The primary aim of this draft legislation is to build a competitive landscape that facilitates data sharing, while ensuring a level-playing field for different actors and networks in the data economy [41]. It further proposes setting up a board that will take the responsibility of creating best practices throughout different sectors and ensuring standardization, for instance, on matters of security and access procedures [41].

In February 2022, the European Commission published its "Proposal for a Regulation on harmonized rules on fair access to and use of data" (Data Act) [53]. The proposed Act is seen as a central pillar of the data strategy. The ambition behind the proposal is to create a cross-sectoral governance framework for data access and use, and to generate incentives for horizontal data sharing across sectors [53]. The Data Act "leaves room for vertical legislation to set more detailed rules for the achievement of sector-specific regulatory objectives, including in the healthcare sector" [53, para.2]. Under Article 4, the draft Data Act proposes the rights of users to access and use data generated as a result of using products and their related services [53]. This particular proposition translates into a requirement for manufacturers or software developers to design their products in a way that enables the data produced to be easily accessible and transparent [41]. Furthermore, the Data Act proposal encourages the formulation of interoperability provisions in the European data governance framework [41]. The proposal was open for feedback from interested stakeholders from March to May 2022 and the feedback will be presented to both the European Parliament and Council with the aim of feeding into the legislative discussion. While the proposed 2020 Data Governance Act forms the processes and structures required to facilitate data exchanges, the 2022 Data Act proposal clarifies who can create value from data and under which conditions. A potential consequence of the Data Act is setting up clearer rules regarding the use of data generated by Internet of Things (IoT) devices [54].

In May 2022, the European Commission released a "Proposal for a regulation – The European Health Data Space" (EHDS). This proposal aims to facilitate reuse and sharing of data by third parties and "builds on the requirements that have or will be imposed on software through the Medical Devices Regulation (MDR) and the proposed Artificial Intelligence Act (AIA)" [55, para.9]. The reported objectives of the EHDS are to: (i) enable individuals to easily access and control their electronic health data; and (ii) allow various actors to use electronic health data in a lawful and secure way that preserves privacy and the fundamental rights of patients. Besides these framework legislative proposals and existing data protection regulations around the world, we note that data governance legislation has not developed to the extent of cybersecurity and AI regulations at the moment. This is a critical area for future legislative and regulatory development given the importance of data to the integrity of artificial intelligence systems, cybersecurity, and patient protection.

Overall, the legislative and regulatory landscape applicable to CIMDs is rapidly changing, with the development of both framework initiatives tackling AI, cybersecurity, and data governance risks, as well as more activity on how to translate and apply some of their principles in medical device regulations and guidance. However, as reported by several stakeholders in our research, legislative and regulatory initiatives provide only the first step in the management of disruptive emerging technologies and their associated risks, requiring further development of guidance and standards to help critical stakeholders such as device manufacturers and clinical users develop, deploy, and monitor the safety and performance of these devices in a responsible manner.

Another major challenge faced by regulators and standards-making organisations is to ensure that their interventions remain relevant and fit-for-purpose. This is made more challenging by the pace of innovation and the evolving needs in healthcare. An example of this is the emergence of AIaMDs, which can evolve independently of the manufacturer or user, and have the potential to adapt and change device performance and outcomes in real time, with limited understanding from the human supervising the process. Procedural clarity is paramount in this case, in terms of obligations for device manufacturers at each stage of development and post-market monitoring, as well as requirements for suppliers, users, and even patients regarding the maintenance of these devices, from deployment to the end of their lifecycle.

3. Research Overview

3.1 Areas of focus: artificial intelligence, cybersecurity, and data governance

Artificial Intelligence (AI)

Artificial Intelligence use in connected medical devices is rapidly growing and is one of the most promising areas of health innovation. AI is significantly impacting people's lives in different ways and plays a pivotal role in digital transformation through its automated decision-making capabilities [5]. Yet, AI in the domain of medical devices comes with its specific benefits and risks, requiring standards and guidelines that provide clarity of regulatory requirements, from classification to conformity assessment and post-market surveillance. As more AI innovation occurs, regulators and standards makers must consider different "approaches for addressing the safety and effectiveness of AI in the healthcare sector, including how international standards and other best practices are currently used to support the regulation" [44, pg.11]. AI is not one technology, but a constellation of techniques and processes, as depicted in Figure 2.

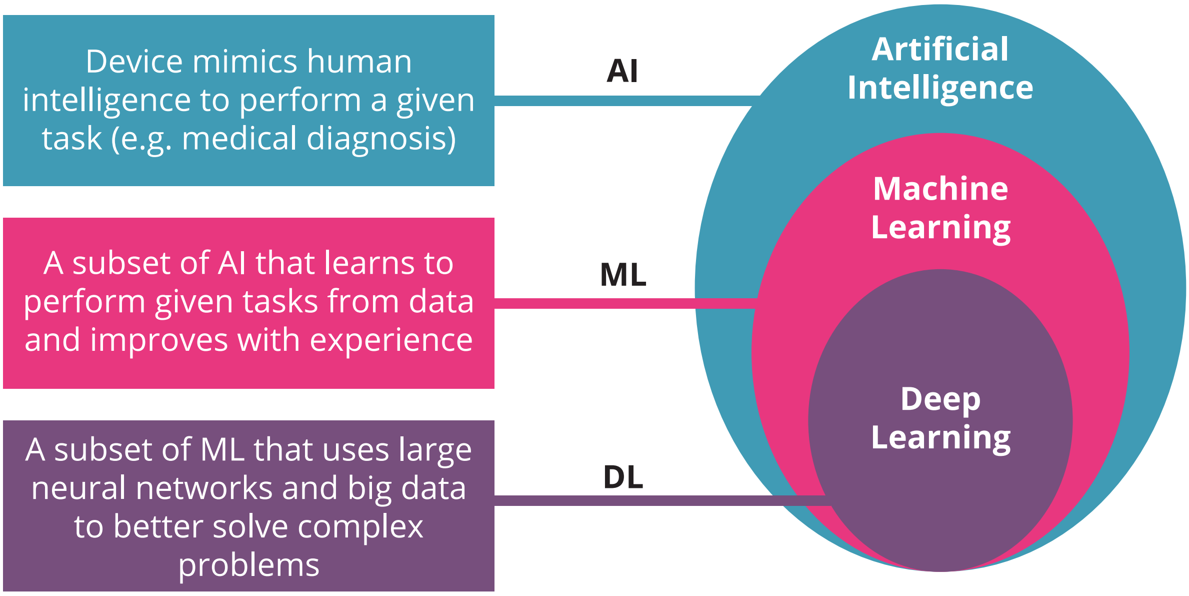

Device mimics human intelligence to perform a given task (e.g. medical diagnosis)
AI
A subset of AI that learns to perform given tasks from data and improves with experience
ML
A subset of ML that uses large neural networks and big data to better solve complex problems
DL
Artificial Intelligence
Machine Learning
Deep Learning

Figure 2: Overview of AI and associated subtypes , adapted from [56]

As shown in Figure 2, “the subset of AI known as Machine Learning (ML) allows ML models to be developed by training algorithms through analysis of data, without models being explicitly programmed” [43, pg.4]. AI and its subtypes can be further divided into ‘locked’ systems whereby the system function does not change, or ‘adaptive’ in which the system performs continual learning [44]. Deep learning is a subset of ML that uses large neural network structures along with considerable data training to better solve complex problems [57]. Deep learning technologies are also in a stage of rapid development, which in turn challenges existing regulatory frameworks. In particular, the use of these new data-driven technologies in CIMDs present new challenges to existing methods for ensuring medical device safety and effectiveness, such as: how can device manufacturers demonstrate equivalence with software already on the market for AIaMDs with highly adaptive learning; what verification and validation methods should be performed pre-market to ensure clinical safety and performance; what monitoring and assurance processes should be implemented post-market to ensure the an AIaMD maintains its originally declared characteristics and risk classification; what should be done if the risk profile of the device changes and when should regulators be notified?

Cybersecurity

CIMDs have been shown to have poor security specifications, which makes them “open to manipulation that can result in outcomes such as administering fatal doses of drugs, compromising patient data, or otherwise malfunctioning, putting users’ health at risk” [58, pg.53]. The accelerated adoption and use of IoMT within the healthcare sector has enabled real-time updates and created positive health outcomes for both patients and clinicians, but also embedded critical security vulnerabilities into an already old digital infrastructure, potentially leading to data loss or identity and information theft [58]. Within the EU regulatory space, “both the MDR and IVDR mandate consideration of medical device cybersecurity, and the Medical Device Coordination Group (MDCG) in its guidance directs manufacturers on how to fulfil the relevant essential requirements of Annex I to the MDR and IVDR with regard to cybersecurity” [48, 59]. However, cybersecurity remains a challenge for standard-setting and certifying organisations on several grounds: what should be the baseline for ensuring a connected medical device is developed with security from the onset and its security is maintained throughout its lifecycle; how should security updates be performed; are there secure interoperability protocols when interacting with other devices within the network; what should manufacturers and users such as clinicians do if a device is compromised? These are only some of the critical questions not yet answered by current standards and guidelines for cybersecurity of CIMDs.

Data Governance

IoMT and AI systems deployed in healthcare cannot realise their full potential without data. AI enabled medical devices in general need a considerable amount of data, both personal and non-personal, to perform their expected functions [60]. Combining IoMT and AI require constant data collection, transfer, and cloud storage where a lot of data processing and analytics occurs. While discussions about the quality and integrity of this data are on the rise, there is still considerable opaqueness about how organisations govern and manage risks associated with data use in digital healthcare, especially for CIMDs. There are several critical data governance considerations that remain unclear, ranging from data collection practices and data quality at the input level, how data used for algorithmic processing is audited, how securely data is stored, to name but a few. Thus, in the IoMT world, it is critical to have adequate, clear, and comprehensive data governance guidelines and standards that help organisations implement appropriate levels of risk management and protection for their data-reliant medical devices.

3.2 Key Research Output: Standards Map for CIMDs

To support the achievement of regulatory objectives, medical device standards have been developed and used to demonstrate conformity to medical device regulations. In the European Economic Area (EEA), harmonised standards are developed and agreed by the three officially recognized European Standardization Organizations: the European Committee for Standardization (CEN), the European Committee for Electro technical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI). “They are created following a request from the European Commission to one of these organisations. Medical device manufacturers, other economic operators, or conformity assessment bodies can use harmonised standards to demonstrate that products, services, or processes comply with relevant EU legislation” [30, pg.6].

Examples of harmonised standards include: the *ISO 13485: 2016 – Quality management systems* that provides the comprehensive quality management system framework for the design and manufacture of medical devices, *ISO 14791:2019 – Application of risk management to medical devices* that provides fundamental guidance on a product’s intended use, determination of potential hazards, risk mitigation, and post-marketing surveillance methods, and the *IEC 62304:2006/AMD1: 2015 Medical device software - Software life cycle processes* that lays out a software lifecycle process for medical devices and refers to ISO 14971 in matters of risk management. Alongside these harmonised standards, there are several supporting standards, such as guidance documents, that help several stakeholders adopt best practice [30]. The Medical Device Guidance Documents (MEDDEV) published by the European Commission are "the most used guidelines by manufacturers of medical devices, promoting a common approach to the implementation of the procedures. They are not legally binding, but they have been written in cooperation with regulators, notified bodies, industry representatives and many other expert organizations. Many standards need to be taken into account when developing a medical device, especially when software is included and each of them tackles a particular issue" [30, pg.35]. Medical device standards can be vertical (address all safety requirements for an individual product group), but more commonly are horizontal (one safety requirement for multiple devices) or process standards (quality, risk, software lifecycle). There are also other general standards covering software safety, security, and performance, developed by health informatics or even general artificial intelligence or information security standards committees.

Evidence from our interviews and roundtable shows that stakeholders are not always clear about the standards, best practice, and regulatory guidance available for them in the process of developing, deploying, and monitoring the performance of CIMDs. In order to have a picture of the standards status quo addressing medical device cybersecurity, algorithmic integrity, and data governance, the Reg-MedTech project developed an interactive, free access mapping tool of existing and in progress standards that apply for CIMDs [1]. A screen shot of the tool is presented in Figure 3.

The mapping tool comprises of the main published and in development standards that apply to CIMDs (Figure 3). The standards are split in three categories pertaining to artificial intelligence, cybersecurity, and data governance. For each of the categories, our research has identified three types of standards:

- **Regulatory standards and guidance documents.** These are documents that further specify regulatory requirements for medical devices and digital healthcare. They are generally used to demonstrate conformity to regulatory requirements (e.g. EU harmonized, UK designated). Medical device standards can be vertical (e.g. address all safety requirements for an individual product group) but more commonly are horizontal (e.g. address one safety requirement for multiple devices) or process standards (e.g. address quality, risk, device lifecycle management).
- **Principles and guidelines.** These are supporting documents that set principles and guidelines pertaining to medical devices and digital healthcare. They are generally voluntary.

- **General standards.** These are documents that provide baseline good practice and/or guidance on how to implement, test, or assess digital technologies and systems pertaining to the integrity of AI systems, cybersecurity, and data governance in general and specifically in the healthcare sector. They are mostly horizontal standards.

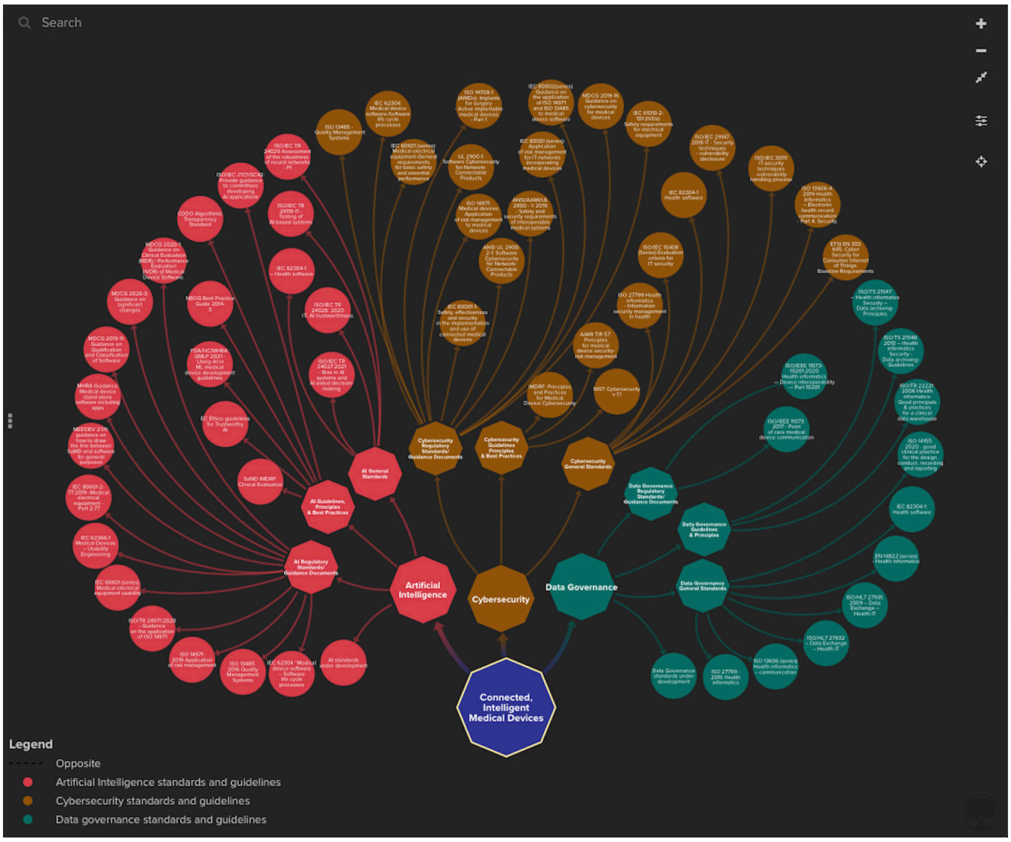

Search
Connected, Intelligent Medical Devices
Artificial Intelligence
Cybersecurity
Data Governance
AI General Standards
AI Guidelines, Principles & Best Practices
AI Regulatory Standards/ Guidance Documents
Cybersecurity Regulatory Standards/ Guidance Documents
Cybersecurity Guidelines Principles & Best Practices
Cybersecurity General Standards
Data Governance Regulatory Standards/ Guidance Documents
Data Governance Guidelines & Principles
Data Governance General Standards
ISO/IEC TR 24029 Assessment of the robustness of neural networks - P1
ISO/IEC JTC1/SC42: Provide guidance to committees developing AI applications
CDDO Algorithmic Transparency Standard
ISO/IEC TR 29119-11 - Testing of AI-based systems
MDCG 2020-1 Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software
IEC 82304-1 – Health software
MDCG 2020-3: Guidance on significant changes
NBOG Best Practice Guide 2014-3
ISO/IEC TR 24028: 2020 IT- AI trustworthiness
MDCG 2019-11: Guidance on Qualification and Classification of Software
FDA/HC/MHRA: GMLP 2021 - Using AI or ML medical device development guidelines
ISO/IEC TR 24027:2021 - Bias in AI systems and AI aided decision making
MHRA Guidance: Medical device stand-alone software including apps
EC Ethics guidelines for Trustworthy AI
MEDDEV 2.1/6: guidance on how to draw the line between SaMD and software for general purposes
SaMD IMDRF: Clinical Evaluation
IEC 80601-2-77:2019 -Medical electrical equipment - Part 2-77
IEC 62366-1 Medical Devices – Usability Engineering
IEC 60601 (series): Medical electrical equipment usability
ISO/TR 24971:2020 - Guidance on the application of ISO 14971
ISO 14971: 2019 Application of risk management
ISO 13485 2016 Quality Management Systems
IEC 62304 "Medical device software – Software life cycle processes
AI standards under development
ISO 13485 - Quality Management Systems
IEC 62304 Medical device software-Software life cycle processes
ISO 14708-1 (AIMDs): Implants for surgery - Active implantable medical devices - Part 1
IEC 80002(series): Guidance on the application of ISO 14971 and ISO 13485 to medical device software
MDCG 2019-16 Guidance on cybersecurity for medical devices
IEC 61010-2-101 (IVDs): Safety requirements for electrical equipment
IEC 60601 (series): Medical electrical equipment-General requirements for basic safety and essential performance
UL 2900-1: Software Cybersecurity for Network-Connectable Products
IEC 80001 (series): Application of risk management for IT-networks incorporating medical devices
ISO/IEC 29147: 2018 IT - Security techniques - vulnerability disclosure
ISO/IEC 30111 IT-security techniques -vulnerability handling process
ISO 14971: Medical devices Application of risk management to medical devices
ANSI/AAMI/UL 2800 - 1: 2019 - Safety and security requirements of interoperable medical systems
IEC 82304-1 Health software
ISO 13606-4: 2019 Health informatics – Electronic health record communication - Part 4: Security
ANSI UL 2900-2-1: Software Cybersecurity for Network-Connectable Products
ISO/IEC 15408 (Series) Evaluation criteria for IT security
ETSI EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements
IEC 80001-1: Safety, effectiveness and security in the implementation and use of connected medical devices
ISO 27799 Health informatics - Information security management in health
AAMI TIR 57 Principles for medical device security-risk management
IMDRF: Principles and Practices for Medical Device Cybersecurity
NIST Cybersecurity v 1.1
ISO/TS 21547 – Health informatics Security – Data archiving-Principles
ISO/TS 21548: 2010 – Health informatics Security - Data archiving-Guidelines
ISO/IEEE 11073-10201 2020 Health informatics — Device interoperability — Part 10201
ISO/TR 22221: 2006 Health informatics- Good principals & practices for a clinical data warehouse
ISO/IEEE 11073 2017 - Point of care medical device communication
ISO 14155: 2020 - good clinical practice for the design, conduct, recording and reporting
IEC 82304-1: Health software
EN 14822 (series) - Health informatics
ISO/HL7 27931: 2009 – Data Exchange – Health IT
ISO/HL7 27932 – Data Exchange – Health IT
ISO 13606 (series) Health informatics – communication
ISO 27799 : 2016 Health informatics
Data Governance standards under development
Legend
Opposite
● Artificial Intelligence standards and guidelines
● Cybersecurity standards and guidelines
● Data governance standards and guidelines

Figure 3: Standards Map for CIMDs: overview of standards by area of focus

Our findings from the development of the Standards Map for CIMDs show that there are several standards and guidelines that currently apply to medical devices and, in some cases, help developers demonstrate conformity with regulatory requirements and inform their risk management and lifecycle monitoring processes. However, some of these standards have been in place for a while and require updates to better capture the critical cybersecurity, algorithmic, and data governance challenges presented above. For example, *ISO 13485: 2016 – Quality management systems* for medical devices mentions software explicitly, following the categorisation of SaMD guidance published by the IMDRF [11]. However, ISO 13485 does not mention AIaMD, leading to the need to interpret the requirements for this particular application. Moreover, *ISO/IEC TR 29119-11: 2020 – Software and systems engineering - Software testing - Part 11: Guidelines on the testing of AI-based systems* states in paragraph 4.3.3.2.3: "AI-specific requirements for safety-related AI-based systems are currently [in 2020] poorly covered by standards and in most domains are reliant on pre-existing standards written for conventional (non-AI) systems" [61]. Some of these standards (e.g. *IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements and ISO 26262 Road vehicles - Functional safety - Part 4: Product development at the system level*) actually specify that AI-based systems which are non-deterministic should not be used for higher-integrity systems [61].

At the other end of the spectrum, general cybersecurity, artificial intelligence, and data governance standards and guidelines are starting to emerge, but it is not yet clear the extent to which they can be used in conjunction with existing medical device standards or they will need to be translated and adapted to align to sector-specific regulatory requirements. For example, *IEC 80001-1:2021 - Application of Risk Management for IT-Networks Incorporating Medical Devices: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software* has recently changed. Among the new specifications, it provides for the provision of accompanying documentation relating to the connectivity of the device. Unfortunately, not all chapters are clearly explained; for example, the security categorization or security requirements of the system are not explained.

Finally, our review of existing standards relevant to CIMDs also demonstrates a clear gap in data governance standards, spanning from how data quality and integrity are assessed, how data are used in algorithmic training, how datasets and databases are audited and maintained. Thus, most horizontal standards identified in the data governance cluster of the CIMDs standards map focus on health informatics and information security management in healthcare pertaining to the confidentiality, integrity and availability of personal health data (e.g. *ISO 27799: 2016 – Health informatics*).

Below, we provide further details of the main findings that have arisen from our analysis of the existing standards landscape relevant to CIMDs:

3.2.1 Need to update horizontal standards for medical devices

The current regulatory and standards landscape for CIMDs pertaining to AI and cybersecurity is multi-layered and complex. Transposing horizontal standards into sector-specific or clinical application standards could lessen this complexity. A very good example of such an initiative would be the development of a single standard for connected medical device cybersecurity, which could borrow from the baseline security measures introduced in the *ESTI EN 3030645: Cybersecurity* *for consumer IoT: baseline requirements* standard and the sector-specific guidance highlighted in the IMDRF's *Principles and Practices for Medical Device Cybersecurity*. Similar standards-development initiatives could be achieved in relation to managing data and algorithmic bias in medical devices, translating existing and emerging standards such as *ISO/ IEC TR 24027:2021 – Bias in AI Systems and AI aided decision-making* into sector specific ones.

We also highlight the need to update current horizontal standards in the healthcare sector to reflect issues pertaining to continuous connectivity, compromise management and reporting, and data governance issues. Examples of general standards that could be updated to fill in this gap include:

- *ISO/HL7 27931: 2009 - Health Level Seven Version 2.5* which is a data exchange standard in healthcare IT environments that can also be used in the medical device sector.

- *ISO/IEC TR 24028: 2020 IT - Information technology - Artificial intelligence - Overview of trustworthiness in artificial intelligence.* This standard "is not specific to any particular domain, but it provides examples from the healthcare sector. The standard summarizes important hazards and threats as well as common risk minimization measures" [62].

3.2.2 Gap in software-based medical device lifecycle standards and organizational processes

Under most regulatory frameworks currently in place, medical device manufacturers are broadly responsible for the safety and effectiveness of their products throughout their entire lifecycle, from its development to its post-market surveillance. "The concept of a lifecycle for medical devices is adopted from the broader idea of a product lifecycle (PLC). Like all products, medical devices begin their lives in a manufacturing plant, then sold to the end user and may be used until the natural end of their lifecycle" [63]. As such, this creates "a need for rigorous pre-market trials and post-market surveillance activities to monitor the performance of medical devices" [63]. The effective management of medical devices throughout their lifecycle is a crucial process that provides value for the manufacturer and the end user. As medical devices transition through each stage of their lifecycle, they are subject to new types of processes, testing, and regulatory requirements [64].

For SaMDs, the lifecycle process covers all stages in a software's life including product idea, development, installation, maintenance, problem management, all the way to the deinstallation and the end of the product's life [64]. All software related standards such as *IEC 62304:2006/AMD1: 2015 Medical device software - Software life cycle processes* and the FDA software validation guidance document [65] stipulate that medical device manufacturers follow these lifecycle processes. However, we still see a gap in software-based medical device lifecycle standards and organizational processes.

For example, harmonized standard *IEC 62304:2006/AMD1: 2015 Medical device software - Software life cycle processes* contains a number of processes for medical device software development and maintenance that firms follow in order to implement medical device software best practices and to streamline the process of achieving regulatory approval [30]. However, this standard does not provide full guidance on all the necessary processes required or system level activities such as validation and release. *IEC 62304: 2006* states: "This standard does not cover validation and final release of the medical device, even when the medical device consists entirely of software" [66, pg.17]. Since validation is one of the requirements under most of the regulatory frameworks and is performed in order to ensure the quality of the software and confirm that the software is working in its intended use, another validation method is required. "As a result, *IEC 62304* roles off system processes to aligned standards such as *ISO 13485: 2016 – Quality management systems*, which provides the comprehensive quality management system framework for the design and manufacture of medical devices and *ISO 14971:2019 – Application of risk management to medical devices* which provides fundamental guidance on a product's intended use, determination of potential hazards, risk mitigation, and post marketing surveillance methods" [30, pg.108].

3.2.3 Gap in data governance standards

Supporting the development and deployment of connected AIaMDs is dependent on transparent, reliable, and fair data governance and management practices. This aspect is also recognised in the EU AI Act proposal, which introduces a requirement for data governance of high-risk AI systems (Art 10) [27]. To ensure data integrity, adequate data governance rules, processes, and standards must be applied throughout the entire data lifespan. Data governance is also strictly linked to data ownership and accountability, and "should consider the design, operation, and monitoring of processes/systems in order to comply with data integrity requirements, including control over all changes to data. Data governance systems should also ensure that data are readily available and accessible for review" [67, pg.17].

> *“Essential to ensuring integrity of algorithms (and this isn’t captured in standards) is the diversity of clinical data we have access to; organizations internally have to grapple with the algorithms that are over fitting the datasets that they have.”* (Manufacturer, Roundtable, 2022).

At the moment, there are very few standards that address the data component of CIMDs – from input, output, communication, storage, and analytics – at the device level and also at the wider digital infrastructure that connects medical devices to each other and wider systems. One of the few standards that address the data component of CIMDs is *ISO/IEEE 11073-10201:2020 Health informatics - Device interoperability - Part 10201: Point-of-care medical device communication*. This standard covers communication between different medical devices and between medical devices and other IT systems for information and for command and control. The standard was designed to provide “real-time plug-and-play interoperability” for patient-connected medical devices and facilitate the efficient exchange of patient-related data and medical device related data, acquired at the point-of-care (POC), in all healthcare environments [68].

Another example is *IEEE 11073-10207-2017 Point-of-care medical device communication Part 10207: Domain Information and Service Model for Service-Oriented Point-of-Care Medical Device Communication* standard. This standard provides support of the exchange of medical information between medical devices and external computer systems [69].

Yet, we are still missing data governance standards that directly address data quality management requirements and data quality process frameworks for AIaMDs. Roundtable participants involved in our research also pointed out the need for clear guidance on data collection and creation for AI development. This challenge is recognised more broadly, because building an AI system “requires substantial amounts of data and the process is highly iterative” [70, pg.29]. This process is complex and “may require several rounds of training, testing, and evaluation until the desired outcome is achieved, with data playing an important role at each step” [71, pg.9].

> *“We are also faced with lack or the challenge of clarity on data to be collected post-implementation in a real intended use environment in the case of dynamic AI algorithm.”* (Start-up, Roundtable, 2022).

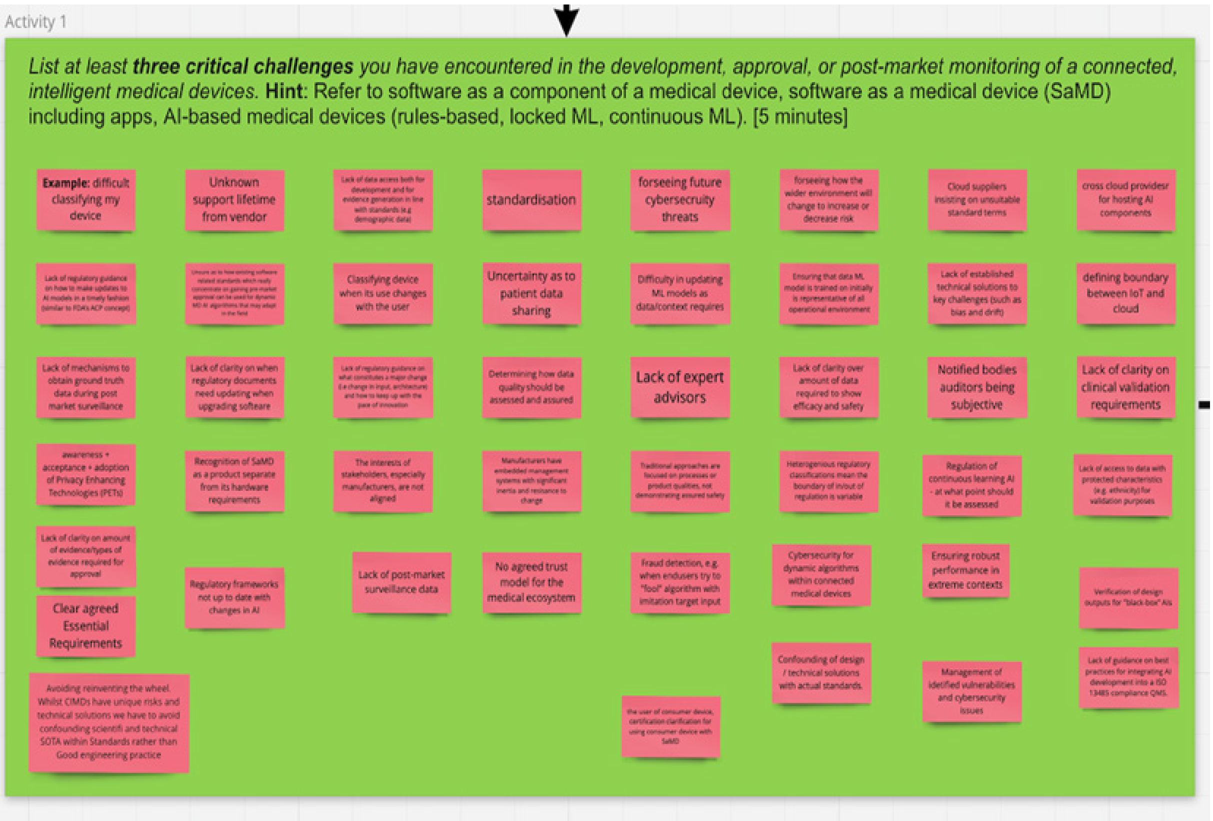
3.2.4 Gap in data quality standards for AI-based medical devices and AIaMDs

The European Council acknowledged that "high-quality data are essential for the development of Artificial Intelligence" [72, para.20]. Data quality is crucial in determining performance of AIaMD. However, it is recognised that "there are many aspects that contribute to data quality, including the completeness, correctness, and appropriateness of the data, annotation, bias, and consistency in labelling of the data" [73, para.3]. Our standards mapping exercise identified that there is need for additional information regarding factors that affect data quality in AI-based systems. We also found that the standards addressing data quality in the development and use of AIaMD are largely missing.

> *"Data quality is the greatest obstacle for AI-based MDs and IVD-MDs and this is derived from the fact that ML-based devices require vast amounts of data to deliver safe and effective outcomes."* (Software Developer, interview-008, 2022).

3.3 Key Research Output: "The Future of Medical Device Regulation and Standards: Dealing with Software Challenges" Roundtable

On 27 April 2022, the Reg-MedTech project held a roundtable with over 45 participants from across all critical stakeholder groups in the CIMD space, including device manufacturers, software developers, clinicians, and regulators (among others). The event aimed to elicit expert guidance on what is critically missing in the current regulation and standards landscape for CIMDs. Figure 4 show one of the data gathering exercises conducted during the event to identify the main challenges encountered during the development, approval or post-marketing monitoring of CIMDs.



Activity 1

List at least ***three critical challenges*** *you have encountered in the development, approval, or post-market monitoring of a connected, intelligent medical devices.* **Hint**: Refer to software as a component of a medical device, software as a medical device (SaMD) including apps, AI-based medical devices (rules-based, locked ML, continuous ML). [5 minutes]

Example: difficult classifying my device

Lack of regulatory guidance on how to make updates to AI models in a timely fashion (similar to FDA's ACP concept)

Lack of mechanisms to obtain ground truth data during post market surveillance

awareness + acceptance + adoption of Privacy Enhancing Technologies (PETs)

Lack of clarity on amount of evidence/types of evidence required for approval

Clear agreed Essential Requirements

Avoiding reinventing the wheel. Whilst CIMDs have unique risks and technical solutions we have to avoid confounding scientifi and technical SOTA within Standards rather than Good engineering practice

Unknown support lifetime from vendor

Unsure as to how existing software related standards which really concentrate on gaining pre-market approval can be used for dynamic MD AI algorithms that may adapt in the field

Lack of clarity on when regulatory documents need updating when upgrading softeare

Recognition of SaMD as a product separate from its hardware requirements

Regulatory frameworks not up to date with changes in AI

Lack of data access both for development and for evidence generation in line with standards (e.g demographic data)

Classifying device when its use changes with the user

Lack of regulatory guidance on what constitutes a major change (i.e change in input, architecture) and how to keep up with the pace of innovation

The interests of stakeholders, especially manufacturers, are not aligned

Lack of post-market surveillance data

standardisation

Uncertainty as to patient data sharing

Determining how data quality should be assessed and assured

Manufacturers have embedded management systems with significant inertia and resistance to change

No agreed trust model for the medical ecosystem

forseeing future cybersecruity threats

Difficulty in updating ML models as data/context requires

Lack of expert advisors

Traditional approaches are focused on processes or product qualities, not demonstrating assured safety

Fraud detection, e.g when endusers try to "fool" algorithm with imitation target input

the user of consumer device, certification clarification for using consumer device with SaMD

forseeing how the wider environment will change to increase or decrease risk

Ensuring that data ML model is trained on initially is representative of all operational environment

Lack of clarity over amount of data required to show efficacy and safety

Heterogenious regulatory classifications mean the boundary of in/out of regulation is variable

Cybersecurity for dynamic algorithms within connected medical devices

Confounding of design / technical solutions with actual standards.

Cloud suppliers insisting on unsuitable standard terms

Lack of established technical solutions to key challenges (such as bias and drift)

Notified bodies auditors being subjective

Regulation of continuous learning AI - at what point should it be assessed

Ensuring robust performance in extreme contexts

Management of idetified vulnerabilities and cybersecurity issues

cross cloud providesr for hosting AI components

defining boundary between IoT and cloud

Lack of clarity on clinical validation requirements

Lack of access to data with protected characteristics (e.g. ethnicity) for validation purposes

Verification of design outputs for "black-box" AIs

Lack of guidance on best practices for integrating AI development into a ISO 13485 compliance QMS.

Figure 4. Activity 1 (data gathering exercise using Miro board) at "The Future of Medical Device Regulation and Standards: Dealing with Software Challenges" Roundtable

We received 38 responses that highlighted different challenges across the three research focus areas of our study – artificial intelligence, cybersecurity, and data governance. Among them, what stood out the most are: limited AI guidance and best practices, lack of cybersecurity standards for dynamic algorithms within the IoMT ecosystem, and determining how data quality should be assessed and assured. The findings from this roundtable activity validated some of the initial findings derived from the development of the Standards Map for CIMDs (Table 1).

Table 1: Challenges faced by CIMD stakeholders – Summary of responses to Activities 1-3 at "The Future of Medical Device Regulation and Standards: Dealing with Software Challenges" Roundtable" (See Appendix C)

Artificial Intelligence	Cybersecurity	Data Governance
Lack of regulatory guidance on how to make updates to AI models in a timely fashion (similar to FDA's ACP concept)	Foreseeing future cybersecurity threats	Lack of data access, both for de-velopment and for evidence gener-ation in line with standards (e.g. demographic data)
Unsure as to how existing soft-ware-related standards, which concentrate on gaining pre-market approval, can be used for dynamic medical device algorithms that may adapt once deployed	Fraud detection (e.g. when end users try to "fool" an algorithm with imitation target input)	Cloud suppliers standards
Difficulty in updating ML models as data or context requires	Cybersecurity for dynamic algo-rithms within connected medical devices	Uncertainty as to patient data sharing
Ensuring that the data the ML model is initially trained on is representative of the operational environment	Awareness, acceptance, and adop-tion of Privacy Enhancing Tech-nologies (PETs)	Lack of established technical solu-tions to key challenges (such as bias and drift)
Lack of regulatory guidance on what constitutes a major change (i.e. change in input, architecture) and how to keep up with the pace of innovation	Management of identified vulner-abilities and cybersecurity issues	Lack of mechanisms to obtain ground truth data during post market surveillance
Regulatory frameworks not up to date with changes in AI	Clear communication and aware-ness of software update period	Determining how data quality should be assessed and assured
Verification of design outputs for black box AIaMD	Lack of clarity for when regulatory documents need updating if up-grading software	Limited clarity over amount of data required to show efficacy and safety
Lack of guidance on best practices for integrating AI development into an ISO 13485 compliance quality management system (QMS)	Cybersecurity training for device users, such as clinicians	Limited post market surveillance data

Crosscutting challenges

- Unknown support from vendor over the lifetime of the device
- Classifying device when its use changes with the user
- Defining boundary between IoT and the cloud
- Lack of clarity on clinical validation requirements
- Recognition of SaMD as a product separate from its hardware requirements
- Ensuring robust performance in extreme contexts
- Clear, agreed essential requirements
- No agreed trust model for the medical ecosystem
- Limited clarity on amount of evidence/type of evidence required for approval
- Confounding of design/ technical solutions with actual standards

4. Findings: Critical Challenges with Connected, Intelligent Medical Devices

Based on the research and engagement underpinning this White Paper, we now highlight seven critical areas where further standards, guidelines, and regulatory guidance can be created to support stakeholders through the development, implementation, testing, post-market surveillance, and use of connected, intelligent medical devices. Our analysis has shed light on some of the critical challenges faced by different stakeholders in relation to existing regulations and standards applicable to CIMDs, summarised here:

- The fast pace of digital innovation we see in CIMDs, especially in AI, is challenging the medical devices field, which is a strictly regulated domain and one where standards have been critical in providing guidelines for how to comply with regulatory requirements. This gap between technological advancements and existing obligations or best practices presents many challenges to the industry stakeholders such as software developers or medical device manufacturers seeking to place their devices on the market, while potentially putting patients at risk. Dynamic learning AI-based medical devices or AIaMDs raise particularly serious concerns about how established risk and lifecycle management processes specified in current medical device standards and guidance can be used to ensure the integrity, safety, and performance of these devices.
- The expanding use of CIMDs in the delivery of healthcare services also introduces a number of potentially significant cybersecurity risks. Cybersecurity risks are relatively well known, but these can be difficult to assess in situations

where devices are in constant use, when it comes to both the type of threat and the extent of possible consequences. Some medical devices have poor security specifications such as default passwords, unclear software update policies, no specified coverage over the device lifecycle, and an unclear incident or vulnerability reporting policy. Moreover, there is a considerable divergence within the industry on the best ways to effectively address cybersecurity issues specific to CIMDs. Standards for incident reporting are key to making reporting clear and to understanding the cause of the incident.

- We currently have a critical gap in standards and regulatory guidelines development pertaining to data management and governance as an underpinning and crosscutting issue that can ultimately either undermine or enable the responsible, safe, and equitable development and deployment of CIMDs.

> *“There is a need to make sure that regulation is able to keep up with innovation, but regulation must not hinder innovation. I think there is definitely room for regulatory innovation”* (Manufacturer, interview-003, 2022).

4.1 The chain of responsibility and liability

The issues of responsibility and liability in case of a security breach or the malfunctioning of a device due to input or output errors caused by AI software are complex. Current product liability legislation was not written with software in mind. When cybersecurity breaches or algorithmic failures occur, identifying the source or cause of the failure is not straightforward and, in several cases, does not constitute a product “defect” as understood thus far. Consequently, the question of responsibility between software developers, manufacturers, vendors, users, and other stakeholders within the supply chain arise. In this study, we highlight a critical gap in current legislation and emerging regulation setting clearer responsibility lines and liability rules for AI-based tools, especially in safety-critical sectors such as healthcare.

> *“A challenge continues to exist in current national and international regulations concerning who should be held accountable or liable for errors or failures of AI systems, especially in medical AI.”* (Lawyer, interview-002, 2022).

Sector-specific regulatory guidelines and standards can help clarify software lifecycle quality controls and risk management processes, which can help organisations achieve more clarity regarding their responsibility and accountability for the outcomes of AI-based medical devices and human oversight of AI systems.

> *"I think sector specific standards are needed to assign and bolster responsibility and accountability adequately to all actors in the AI workflow in medical practice, including the manufacturers, thus providing incentives for applying all measures and best practices to minimise errors and harm to the patients."* (Manufacturer, Roundtable, 2022).

This need is also supported by the European Parliament Resolution on 'civil liability for AI, which states that liability rules should cover all operations of AI systems, "irrespective of where the operation takes place and whether it happens physically or virtually" [74, para.11].

The accountability or responsibility challenge is also compounded by the fact that CIMDs are open to software extensions, updates, and patches after they have been placed on the market. Any change to the software of the device may affect its functionality, operational risk profile, and ultimately its capacity to operate as expected or cause harm. As shown in the specialist literature, "a brain stimulation device's software could be remotely updated or given automated direction by an algorithm. If the data are changed in an unauthorized manner, AI software instructions could increase the electrical stimulus beyond its typical thresholds, causing brain damage" [75, pg.1566]. The need for a preventative approach by way of setting or updating relevant sector specific standards is especially important given the speed and scale at which these technologies now operate.

Most stakeholders that participated in our roundtable highlighted that, when cybersecurity breaches occur, multiple failures at various levels are involved. Consequently, we may need to look at shared responsibility models that can be applied across the medical device supply and use chain including software developers, manufacturers, suppliers, authorized representatives, sub-contractors, importer, distributors, and vendors in order to address the software liability issue. As highlighted by the Scientific Foresight Unit of the European Parliament, "AI regulation could include the notion of emergent harms by including post-deployment monitoring and (re)assessment in order to take account of the divergent paths AI systems and models often take after their initial conception, and how they pose different problems to oversight depending on the use" [41, pg.60].

4.2 Risk and classification of medical devices

A striking observation that has emerged from our review of the standards and regulatory space for CIMDs is the absence of compliance tools for assessing AI-based medical devices against approved European Standards. Currently the medical device industry does not have harmonised standards that specifically address the unique performance aspects of AI technologies [76]. For example, the "*ISO 14971 - Application of risk management to medical devices* has consistently demonstrated its usefulness in assessing the safety of medical technologies that function in the same manner and do not change with use over time" [76, pg.5]. However, data-driven medical technologies with adaptive algorithms may well present one risk profile during the initial product development process and a different risk profile after the device has been deployed for use with patients. The validation of adaptive algorithms could be harmonised and strengthened to assess and identify these multi-faceted risks and limitation [76].

The draft EU AI Act proposes the adoption of a risk-based approach to classifying AI tools and their application and it is likely that most AI tools that are either part of a medical device or a medical device themselves will fall under the "high risk" classification. However, at this point in time, it is unclear how emerging regulations addressing general AI or cybersecurity risks will align with existing medical device regulations. Furthermore, sector and clinical application-specific guidelines and standards for AI-based medical devices are needed to further understand, qualify, and manage emerging risks, especially if these can introduce substantial risks and uncertainties. AI-based medical device lifecycle management standards are also lacking, though critical in this space.

> *"In the early stages of our small start-up, it was the lack of clarity on clinical validation requirements. Connected with that, lack of access to certain data with protected characteristics, it is challenging to discuss. Lack of clarity and clinical validation and linking in with risk classification devices and what clinical data is required to validate changes made to the device, adding in different indications."* (Start-up, Roundtable, 2022).

> *"It would be ideal to have a more robust standardisation and regulatory framework to define basics, such as classification; there should be more specific classification for AI."* (Product Assessor, Roundtable, 2022).

In CIMDs, the potential risks and critical challenges associated with AI are multi-dimensional and occur at different levels, depending on the type of algorithm being developed and deployed. For example, locked algorithm risks would be different from those posed by an adaptive algorithm (also referred to as continuous learning). Equally, supervised algorithms present a different set of challenges and requirements to those based on unsupervised learning. As highlighted in the specialist literature, this "raises the question: how do we regulate software that is continuously learning or changing its output in response to new data? Over time, these kinds of changes might introduce unknown risks, overriding existing risk profiles originally envisioned by developers and regulator" [77, pg.7]. In addition, some ML models can be sensitive to small changes in their data, thus it could become problematic to quantify the risks associated with these incremental changes [58]. The complexities of these new AI technologies and the challenges of deploying them have put a spotlight on the lack of AI standards across many sectors, including the healthcare sector, in different jurisdictions. To address these issues, the UK's National Institution for Health and Care Excellence (NICE) "recommends developing a separate standard for artificial intelligence with adaptive algorithm" [77]. As pointed out in the NICE recommendation, it is also pivotal to ensure that new regulatory requirements and standards do not hamper innovation or become new restrictions to stakeholders' ambitions to develop and market new technologies but rather help contribute towards business growth and opportunities. CIMDs with embedded self-learning algorithms and adaptive nature capability warrant new regulatory approaches that would ensure patient safety and improve patient care [77]. Existing standards and guidance such as *IEC 62304:2006/ AMD 1: 2015 – Medical device software – Software life cycle processes*, *MDCG-2020-3 – Guidance on significant changes and even ISO 13485 2016 – Quality management systems for medical devices* may be insufficient for some of CIMDs with dynamic algorithms in demonstrating conformity to the IVDR and MDR.

As with all medical devices, AI-based healthcare technologies are subject to regulatory scrutiny based on the risk they pose to patients [20, 78]. This translates into a requirement on manufacturers to provide a risk classification for medical devices. In the USA, for instance, "Class I devices, such as software that solely displays readings from a continuous glucose monitor pose the lowest risk. Class II devices are considered to be moderate to high risk, and may include AI software tools that analyse medical images such as mammograms and flag suspicious findings for a radiologist to review" [78, pg.7]. The majority of devices that fall under "Class II undergo what is known as a 510(k) review, in which a manufacturer demonstrates that its device is "substantially equivalent" to an existing device on the market with the same intended use and technological characteristics" [78, pg.7]. Similar to these FDA rules, manufacturers can gain the EU's CE mark of conformity under the MDR by demonstrating equivalence with another product, reducing costs from performing de novo clinical studies.

However, stakeholders such as the USA Patient Network [79] have criticized the FDA's 510(k) pathway for not adequately guaranteeing medical device safety and effectiveness and for increasing the burden on patients and clinicians to figure out which devices are safe, including AIaMDs. They have highlighted that "the 510(k) clearance can lead to chains of medical devices that claim substantial equivalence to each other, but over years may diverge substantially from the original device" [20, pg.15]. "For example, the AI-based medical device Arterys Oncology DL, cleared in 2018, which is indicated to assist with liver and lung cancer diagnosis, can be traced back to cardiac imaging software cleared in 1998, which was considered as substantially equivalent to devices marketed prior to 1976" [20, pg.16]. Then, the main challenge for AI medical devices with continuous learning from clinical application is that may produce outputs that differ from what was initially submitted for regulatory review or approval and what would otherwise be expected from that device's performance. As highlighted in our roundtable, classifying and placing a SaMD or AIaMD on the market, especially when using "substantial equivalence", doesn't necessarily mean that its risk profile will remain the same once the device is deployed and, in fact, its risk profile can change multiple times throughout its lifecycle, with limited awareness from both clinical staff and patients.

4.3 Managing cybersecurity risks and vulnerabilities

Embedded connectivity and intelligence have also exposed vulnerabilities to patient safety and device functionality across the medical device lifecycle. Manufacturers, healthcare providers and public authorities face novel challenges in ensuring secure, safe, and usable medical devices [80, pg.5].

Cybersecurity attacks can fatally disrupt a medical device's basic functions or availability, and may render hospital networks unavailable, delaying patient care [81]. A recent study conducted by Cynerio found critical security vulnerabilities in over 50% of connected medical devices and over 70% of IV pumps, stemming from maintaining default passwords or settings, issues with updating obsolete software, and long lifecycles of devices that are in continuous use as part of the healthcare infrastructure [82].

Our analysis shows that the main cybersecurity challenges being faced by different healthcare organisations involved in the deployment and use of CIMDs include: unclear password protection guidelines, poor security practices, unclear device management and software update policies, human errors, limited security awareness, limited coordinated incident response, huge constrains on budget and resources for prioritising device and network security, and limited understanding of vulnerabilities within a clinical setting or the entire medical systems. There are a number of highly publicized incidents in which hackers have uncovered cybersecurity vulnerabilities in connected medical devices or device software that would potentially allow them to gain remote access and control their operation. Examples of such incidents include:

- In 2016, St. Jude's pacemakers were subject to a "battery drain" and "crash attack" that resulted in the FDA issuing a safety communication outlining potential vulnerabilities to cyberattacks in this manufacturer's implantable cardiac pacemaker products. This was one of the first major events in the medical device industry that drew attention to the cybersecurity risks of cardiac implantable electronic devices [83].

- In 2016, researchers discovered that three different types of Johnson & Johnson's insulin pumps can be exploited and cause insulin overdoses in diabetic patients. The manufacturer issued a warning to patients though it described the risk as low. The three vulnerabilities were associated with wireless communication, weak pairing, and transmission assurance issues. The specialist literature noted that using industry standard encryption with a unique key pair would mitigate some of these issues [84].

- In October 2018, cybersecurity vulnerabilities were identified in two models of Medtronic's programmers that were used with implantable devices such as pacemakers, implantable defibrillators, cardiac resynchronization devices, and implantable cardiac monitors [85]. The FDA confirmed that when the programmers are connected to the Internet, the connection to the Medtronic network could be exploited and allow an unauthorized user to change the functionality of the implanted device during the device implantation procedure or during follow-up visits [86].

- In 2019, the FDA issued a safety communication, warning patients and healthcare providers that some of Medtronic's insulin pumps were being recalled due to potential cybersecurity vulnerabilities. The FDA was concerned that vulnerabilities identified in such high-risk devices could harm patients by stopping insulin delivery or overdosing it. As a result, the FDA recommended patients to replace affected pumps with models that are better equipped to protect them from these risks [87].

• In early 2020, the FDA also notified the industry of cybersecurity vulnerabilities in clinical information servers widely used in healthcare environments. According to the FDA, the vulnerabilities could potentially “allow an attacker to remotely take control of a device” connected to the server, and silence patient monitor alarms, generate false alarms, or otherwise interfere with their intended function [88].

> “*There is a lack of clarity on when regulatory documents need updating when upgrading software.”* (Manufacturer, Roundtable, 2022).

As already highlighted in the literature, it is of vital importance that “manufacturers consider an effective cybersecurity strategy that addresses possible cybersecurity risks not only during development but throughout the life of the software medical device. This means measures to ensure safe, secure, and effective transfer and utilisation of information among CIMDs have to be in place” [81, pg.21]. Another issue with compromised devices is that they can become a vulnerable entry point to the entire IoMT ecosystem, as highlighted in the case of cybersecurity vulnerabilities that were identified in two models of Medtronic programmers above. Together, these cases illustrate the increasing concerns in the public domain about the cybersecurity of CIMDs. Thus, the link between medical device security and its safety and performance has never been stronger. When security specifications are not appropriate, hackers could alter the intended performance of software through several interventions such as “deactivating features; delaying, interfering, or interrupting communications; or altering programming” [58]. Lastly, many Internet-connected medical devices, such as remote patient monitoring or heart rate monitoring devices store or transmit patient data. Once a device is compromised, it could have consequences for the integrity of the data and the wellbeing of the patient. To address some of these concerns, in 2020, the Emirate of Abu Dhabi Department of Health outlined several domains critical to ensuring IoMT ecosystem security (Figure 5).

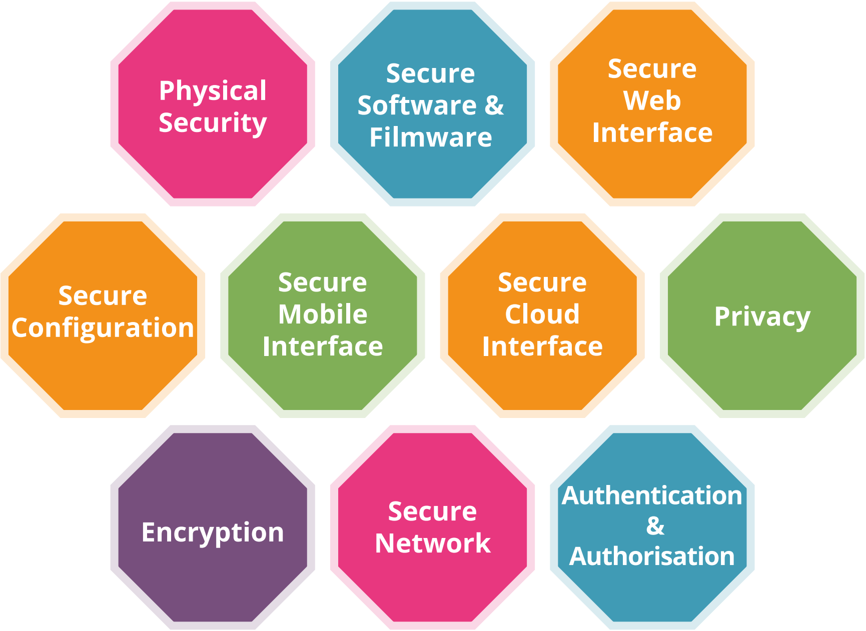


Figure 5: Domains of IoMT Security, Emirate of Abu Dhabi Department of Health IoMT Security Standard [13]

4.4 Legacy components: devices are the endpoint of a larger digital healthcare infrastructure

Medical devices and software are generally in constant and long-term use and many can develop vulnerabilities, especially if they do not support or stopped supporting patches. While this is a reality in the medical device sector, legislators are continually updating the regulatory frameworks for medical devices to address some of these concerns, as we have seen in Europe with EU Regulation 2017/745 (MDR) and EU Regulation 2017/746 (IVDR), as well as international standards such as IEC 62366-1 (IEC usability) or IEC 62304 (software lifecycle). This raises the question of how different stakeholders deal with legacy devices. The vast majority of medical devices and the supporting ICT and digital infrastructures in healthcare are considered “legacy systems” that cannot be patched due to expired software update policies, limited availability of alternative solutions, or certification requirements [89]. Continuously adding new connected devices to legacy systems can increase vulnerabilities by expanding the attack surface [90]. Legacy software from the perspective of the IEC 62304: 2015 is interpreted as “software (part of a medical device or standalone software) that was placed on the market in accordance with the legal requirements in force [at the time] but that no longer meets today’s requirements (especially IEC 62304)” [91]. Here, “at the time” refers to March 2015, the date of application of the current version of IEC 62304.

Legacy medical devices are particularly problematic for cybersecurity because they are inherently more vulnerable to cyberattacks and compromise. In addition, technology vendors are limited in their ability to protect solutions developed without a security-first approach [91]. Exploiting a vulnerability within a legacy technology can lead to "medical device malfunction, disruption of health care services (including treatment interventions), and inappropriate access to patient information" [92]. The impact of the 2017 global WannaCry ransomware attack that affected many hospitals across the world including five acute trusts in the United Kingdom is a critical example of the vulnerability of these legacy systems. The WannaCry ransomware attacks exploited vulnerabilities on devices including "MRI scanners and blood test analysis devices that were running outdated versions of an old Windows operating system", encrypting the system and demanding that the users of infected systems pay a ransom to regain control of their devices [92, pg.8].

> *"Older medical devices weren't designed with cybersecurity as a forethought and are hard to properly secure. Now the boom in newly connected devices is exposing pre-existing vulnerabilities."* (Consultant, interview-006, 2022).

These devices tend to be easy targets for attackers because of well-known vulnerabilities that cannot be patched and, even if few of these systems can be patched, they are often improperly configured and maintained at the point of care, such as in the clinical setting. Having legacy and new devices connected to the same network increases the attack surface and exposes new devices to scanning for vulnerabilities and compromises. Furthermore, "complex legacy hardware and software architectures can make the implementation of even the "simplest" AI enabled feature difficult. Legacy systems that were not built for interoperation with other systems, or which contain old security vulnerabilities, can create system integration problems" [93, pg.7].

Currently, the legacy problem is made more challenging by the fact that there is limited legal clarity regarding the stakeholders in the supply and use chain who carry responsibility to implement security updates. For instance, should security updated be pushed automatically by the manufacturer on all its devices or should the healthcare providers ensure their systems are up to date (see also Section 4.1)? Our study identified the need to increase awareness in the health sector of cybersecurity risks by means of additional clinical staff training and development as a countermeasure against increased cyber threats. The need for cybersecurity awareness and skills extends beyond technical cybersecurity roles to the entire healthcare system, especially at the point of care.

> *"Legacy devices were never designed to be connected, let alone secured on today's digital networks. Yet they hold sensitive, personal, and often times life sustaining information"* (Regulator, interview-009, 2022).

4.5 Clarity in assessing algorithmic explainability and transparency

Explainability (sometimes used in conjunction with interpretability) "is the concept that a machine learning model and its output can be explained in a way that makes sense to a human being at an acceptable level" [94, para.1]. The majority of stakeholders interviewed in this study highlighted that assessing explainability of the algorithmic output is a key challenge in AI-based CIMDs. They expressed that transparency is key to gaining the trust of patients, healthcare providers, and regulators. This is reinforced in the specialist literature: "Medical applications, such as cancer prediction software, are an example where explainability is essential since it is considered a critical and a "life or death" prediction problem, in which high forecasting accuracy and interpretation are two equally essential and significant tasks to achieve" [95, pg.2]. However, reasoning, interpreting, and explanation of their predictions is one of their greatest limitations. ML predictive models, which are largely inscrutable, have led to serious societal problems that deeply affect health, freedom, equality, and safety [95]. It is universally agreed that interpretability is a key element of trust for AI models [96].

This raises the question: how can an AI-based medical device or an AIaMD be trusted if it is not fully understood? Then, the critical challenge becomes to identify what needs to be transparent in the entire data lifecycle and what processes should be in place to monitor it: should we have transparency at input (e.g. data source, problem formulation, selection), process (e.g. machine learning, auditing), output, and/or outcome (e.g. clinical)? As noted in the specialist literature, if CIMD "providers do not fully understand how and why an algorithm arrived at a particular decision or result, they may struggle to interpret the result or have clinicians apply it to a patient" [78, pg.5].

> *"A significant risk for AI enabled medical devices is a lack of transparency concerning their design, development, evaluation, and deployment. For example, there is a lack of understanding and trust in predictions and decisions generated by the AI-based device, difficulties in independently reproducing and evaluating AI algorithms, difficulties in identifying the sources of AI errors and defining who and/or what is responsible for them"* (Manufacturer, interview-04, 2022).

Furthermore, "AI-based medical devices are not only run autonomously but also capable of making clinical decisions on behalf of doctors. Unlike traditional medical device software, AI-based medical devices can continuously evolve and update with new data. The lack of standards that address transparency, explainability, interpretability, accountability and predictability on the part of algorithmic medical devices could pose serious risks to patients" [77, pg.7]. This critical gap in standards is also acknowledged by the European Parliament in its governance framework for algorithmic accountability and transparency [40].

> *"With traditional software you can explain how the software has come to a decision while with AI it becomes a bit blurred as you are reliant on good data being fed into the algorithm"* (Manufacturer, interview-07, 2022).

4.6 Understanding and assessing types of bias in data for AI-based medical devices

Bias in digital medical technologies can be analysed along three dimensions: data-driven, algorithmic, and human [97]. Algorithmic bias in CIMDs and the healthcare sector at large can propagate discriminatory practices and broader societal biases deeply entrenched in the datasets used to train algorithms, which can lead to misdiagnosing particular patient groups such as ethnic minorities or women. For example, in cardiology, a heart attack is overwhelmingly misdiagnosed in women [97].

> *"Training datasets must be robust enough to support diagnosis of the intended population so as to avoid bias."* (Software Developer, interview-008, 2022).

Ensuring that appropriate training data is used in model training is critical to the overall quality of the algorithmic decisional tool. Recently, standards providing ethical considerations for AI have started to emerge, such as *the ISO/IEC TR 24027: 2021 - Information technology, AI, bias in AI systems and AI aided decision making*. This standard acknowledges that developing AI systems with outcomes free of unwanted bias is a challenging goal [98]. The challenge of bias was emphasised on several occasions throughout our interviews, predominantly highlighting bias in the datasets used in AIaMDs training. However, focusing exclusively on bias in algorithmic training data is insufficient, especially for continuous learning and adaptive algorithms that produce outputs based on continuous clinical data feeds, where human bias can manifest.

4.7 Data quality and integrity

Our mapping exercise also found a critical gap in data quality standards and guidance documents that integrate principles of inclusivity, openness, and trust in the design of AI-based medical devices, which can be applied to eliminate implicit bias and support interoperability. Our analysis shows that both data quality and handling are essential to the achievement of data governance and that AI ethics cannot be implemented if explicit data governance practices are not in place. The quality of the data used at the development stage of SaMDs and AIaMDs is of critical importance if medical devices are deployed with the ambition to make accurate, valid and unbiased real world decisions [71].

However, roundtable participants in our research highlighted that it is a challenging task for CIMDs manufacturers to obtain and maintain high quality data. This view was echoed in another recent study that highlighted several attributes "such as training datasets or explainability of device inputs versus outputs, which challenge the transparency and trust of AI-based applications. These characteristics are either directly or indirectly linked to data quality; hence, the quality of datasets used to train and validate AIaMDs is seen as an all-encompassing topic" [58, pg.79]. Consistent with the roundtable participants' perspectives, previous studies have highlighted that data quality affects how well AI and ML models will operate [99]. "These aspects include the completeness, correctness, and appropriateness of the data; annotation; bias; and consistency in labelling of the data" [55, pg.9].

Most interview respondents also highlighted data integrity is a persistent challenge in the current healthcare sector. Data integrity can be understood as "the completeness, consistency and accuracy of data" [100, pg.2]. Data integrity is imposed within a system at its design stage through the use of standard rules and procedures, and is maintained through the use of error checking and validation routines [101, pg.1]. Others highlighted that the integrity of data in transit or at rest must be protected from unintended or unauthorized modification, highlighting the critical link between cybersecurity, algorithmic and data integrity. Ensuring data integrity is a continuous process, so new standards must capture processes for monitoring, detection, correction, and reporting measures as inevitable data gaps or compromises emerge.

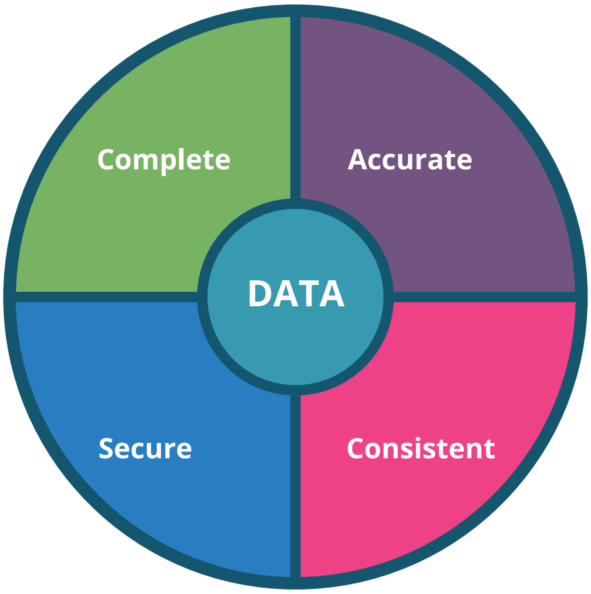


Figure 6: Elements of data integrity that contribute to data trustworthiness

> *“Data integrity are those elements such as completeness and accuracy that give data trustworthiness.”* (Software Developer, Roundtable, 2022).

5. Conclusion

This White Paper addressed a pressing question for current and future digital healthcare transformations: how and to what extent do current regulatory frameworks and standards address the critical challenges and unique risks posed by connected, intelligent medical devices (CIMDs)? Through a scoping review, a standards mapping exercise, interviews with experts and practitioners, and a roundtable with critical stakeholders in the field, we identified that key artificial intelligence, cybersecurity, and data governance challenges are not yet comprehensively and consistently addressed by existing and emerging standards, guidelines, and regulatory frameworks, although we are also seeing considerable policy and standardisation initiatives emerging in this space.

From our research, we identified seven priority areas that require further regulatory and legal clarity, where standards and guidelines can be developed to support stakeholders through the development, implementation, testing, and post-market surveillance of connected, intelligent medical devices (Section 4). We summarise these in Figure 7 below.

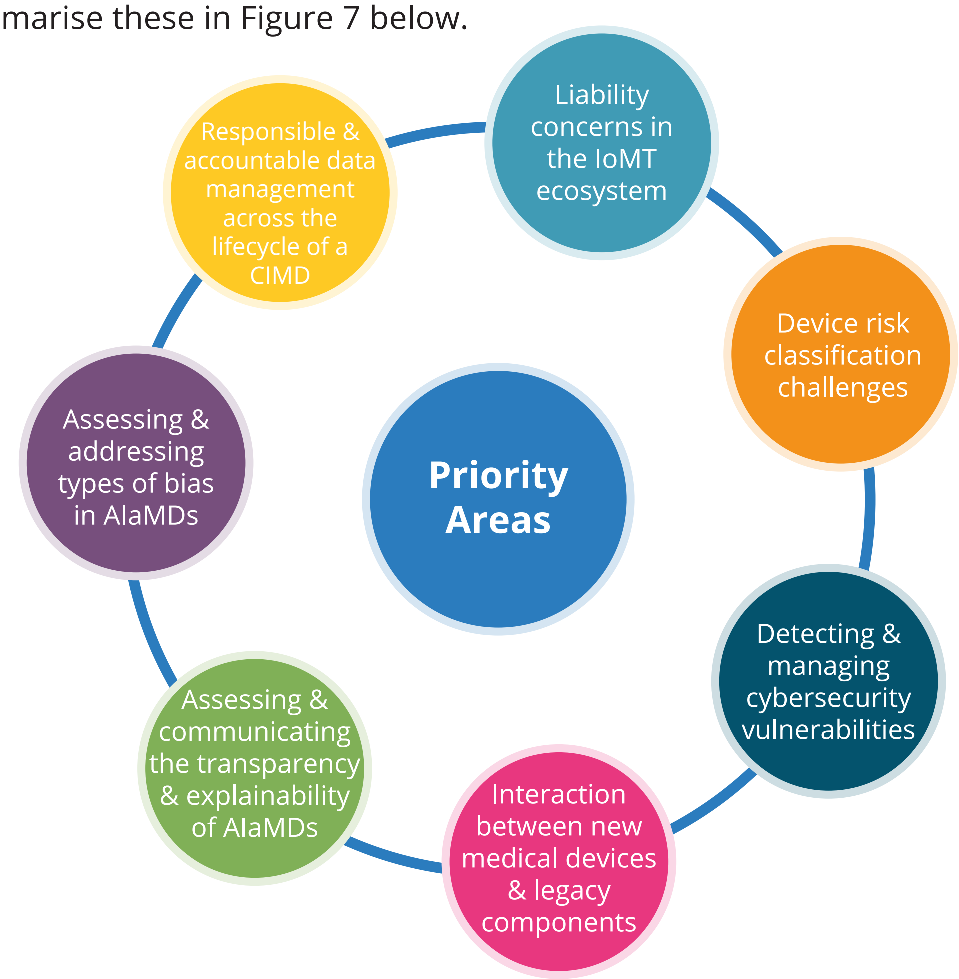

Priority Areas
Liability concerns in the IoMT ecosystem
Device risk classification challenges
Detecting & managing cybersecurity vulnerabilities
Interaction between new medical devices & legacy components
Assessing & communicating the transparency & explainability of AIaMDs
Assessing & addressing types of bias in AIaMDs
Responsible & accountable data management across the lifecycle of a CIMD

Figure 7: Priority areas for future CIMDs standards and regulations

CIMDs are at the confluence of sectors with different and even diverging dynamics, which need to be understood if we are to fully tackle the risks associated with these technologies. On the one hand, CIMDs are digital innovations and, over the years, the digital sector has benefited from limited regulation and obligations to tackle the risks associated with technological advancements such as IoT or AI, although this landscape is currently changing. On the other hand, medical devices have been under strict sectoral regulatory requirements for decades, so updating rules, obligations, and ultimately manufacturing and product surveillance practices is inevitably a long-term endeavour. Lastly, CIMDs are largely deployed at the point of care in hospitals and other clinical facilities, in patients' homes, and even implanted in the human body. As a result, the healthcare sector dynamics are critically important as they impact directly on the preparedness of medical staff and clinical administrators, as well as on the resilience of the current healthcare infrastructure to respond to the ongoing challenges and different practices required when utilising CIMDs.

To address these sectoral dynamics and foster the responsible development, deployment, and monitoring of CIMDs requires a coordinated approach between policy, regulatory, and standards development organisations at the national and international level. In recent years, we have seen several standards and regulatory initiatives emerge that address critical horizontal issues pertaining to the security of connected devices or the integrity of algorithmic tools and systems. While these are important initiatives, we see strategic opportunities for standards-making, regulators, and international harmonisation bodies such as the IMDRF to address the priority areas we've identified above (Section 4) with more concrete measures.

We make the following recommendations for short to medium-term action:

1. National standards-making bodies can work closely with regulators to formalise an agenda for new standards and regulatory guidance development for connected, intelligent medical devices, especially AIaMDs. Priority areas for standards and guidance development include: addressing **software lifecycle management** issues for locked and adaptive algorithms used in or as medical devices, as well as **explainability and transparency** of AI as a component in medical devices or a standalone medical device.
2. National standards-making bodies can work jointly and in collaboration with international harmonisation bodies such as IMDRF to develop a new work programme that addresses **data governance** issues in medical devices, including data quality, data integrity, management, oversight, and audit processes in line with emerging regulatory frameworks such as Art 10 in the proposed EU

AI Act.

3. International standards-making bodies can prioritise the development of a single standard addressing **cybersecurity of connected medical devices**, which should include legacy device cybersecurity, in order to avoid duplication of device cybersecurity standards and address the critical need to update general health informatics standards.
4. Regulators can provide further guidance on **the responsibilities and obligations of critical stakeholders** in the development, deployment, use and monitoring of connected, intelligent medical devices, so that their integrity, safety, and performance can be ensured.
5. National and international guidance needs to be provided to support **clinical and administrative staff** in hospitals and other healthcare facilities to understand and monitor the performance of connected, intelligent medical devices deployed and used on their premises, and how to record and report incidents triggered by cybersecurity, algorithmic, or data integrity breaches or failures.

Appendix A: List of interviews conducted by stakeholder category

Respondent Code	Stakeholder Category	Date	Place of Interview
01	Manufacturer/Consultant	16 Feb 2022	United Kingdom
02	Lawyer	22 Feb 2022	United Kingdom
03	Security practitioner	22 Feb 2022	United Kingdom
04	Manufacturer	28 Feb 2022	United Kingdom
05	Regulator - MHRA	03 Mar 2022	United Kingdom
06	Manufacturer	04 Mar 2022	United Kingdom
07	Manufacturer	07 Mar 2022	United Kingdom
08	Software developer/Academic and research institution	10 Mar 2022	United Kingdom
09	Academic and research institution	17 Mar 2022	United Kingdom
10	Standards makers	28 Mar 2022	United Kingdom
11	Software developer/Academic and research institution	29 Mar 2022	United Kingdom
12	Clinician	13 Apr 2022	United Kingdom

Appendix B: Categories of stakeholders who participated in the roundtable

Stakeholder Category	Number of participants
Medical device manufacturers/ Software developers	12
Regulators	4
Standards makers	7
Researchers	9
Lawyers	1
Security practitioners	1
Clinicians	3
Industry association/Other	9
Total number of participants	45

Appendix C: Programme of "The Future of Medical Device Regulation and Standards: Dealing with Software Challenges" Round-table held by the Reg-MedTech Project on Wednesday 27th April 2022, 10:00 – 13:30 BST

<table>
<tr><th>Time</th><th colspan="2">Session</th><th>Speaker</th></tr>
<tr><td><b>10:00 – 10:05</b></td><td colspan="2">Welcome and introduction</td><td>Irina Brass - UCL</td></tr>
<tr><td><b>10:05 – 10:20</b></td><td colspan="2"><b>Keynote</b>: Latest regulatory responses to software-based medical devices</td><td>Johan Ordish - MHRA</td></tr>
<tr><td><b>10:20 – 10:35</b></td><td colspan="2"><b>Keynote</b>: How can standards support regulatory developments for soft-ware-based medical devices</td><td>Rob Turpin - BSI</td></tr>
<tr><td><b>10:35 – 10:45</b></td><td colspan="2"><b>Reg-MedTech</b>: Project overview and preliminary findings</td><td>Irina Brass & Andrew Mkwashi - UCL</td></tr>
<tr><td colspan="4"><b>Roundtable Session 1</b>

The purpose of this session is to collaboratively analyse, validate, and refine preliminary REG-MEDTECH project findings, consult on gaps in current standards and regulations, and identify critical organisational needs</td></tr>
<tr><td></td><td><b>Activity</b></td><td><b>Description of activity /Questions</b></td><td></td></tr>
<tr><td rowspan="2"><b>10:45 – 11:05</b>
(Using white-boarding software Miro)</td><td><b>Activity 1:</b></td><td>1. List at least three <b>critical challenges you have encountered in the development, approval, or post-market monitoring</b> of a connected, intelligent medical device.

Hint: Refer to software as a component of a medical device, software as a medical device (SaMD) including apps, AI-based medical devices (rules-based, locked ML, continuous ML).</td><td>All</td></tr>
<tr><td><b>Activity 2:</b>
Refer to the standards mapping tool and summary of findings</td><td>2. Now focus on <b>specific standardization and regulatory challenges</b> you have encountered or are aware of, pertaining to <b>AI/ ML, cybersecurity and data governance</b> in software-based medical devices.
Hint: Are there any standards missing in this area? Are there any challenges to device classification? Any challenges for specific clinical applications?</td><td>All</td></tr>
</table>

	Activity 3: Refer to the standards mapping tool and summary of findings	3. List at least **three concrete measures to address these challenges or gaps**. Hint: Examples include changes in market approval/ post market surveillance requirements, organizational processes, missing standards, new regulatory guidelines, changes to legislation, internationally harmonised guidelines or standards, etc.	All
11:05 – 11:30	**Activity 4:** Moderated group discussion	4. What **safety, security, data quality, and/or algorithmic integrity measures** does your organization adopt to ensure responsible management and vigilance over software-based medical devices or SaMDs throughout their lifecycle? 5. What measures are or should be in place if you are **suspecting or identifying potential failures, faults, or incidents with** your connected, intelligent devices? 6. Are you clear about the **responsibility and potential liability** your organization might have over security or data breaches linked to connected, intelligent medical devices you develop, manufacture, or use? 7. How about over data quality and algorithmic integrity linked to these devices? 8. What **support** would you like to see from **regulators, standards-making bodies, and professional associations** to have more clarity?	(All) Breakout rooms
11:30 – 11:50	**Feedback group sessions (Main room)**		Presentation by groups
11:50 – 12:05	**Tea break**		

Roundtable Session 2 The purpose of this session is to look into the future at the innovation landscape for connected, intelligent medical devices, and to explore opportunities for regulators and standards-making bodies to encourage future-proof, responsible innovation with patient safety at the core.			
	Activity	**Description of activity /Question**	**Speaker**
12:05 -12:55	**Activity 5:**	1. What do you think **the state of the art will look like in 5 years' time for connected, intelligent medical devices**? Be as specific as possible. 2. How will these developments affect: • data quality for AI as a medical technology • performance metrics for AI tools • explainability of AI outputs • cybersecurity • human oversight • other aspects? 3. What **organizational processes and support** would you like to see in place to support these technological advances? For instance: • continual assurance throughout the software lifecycle • new quality and risk management standards • monitoring and evaluation protocols • professional qualifications, training, and protocols • other aspects? 4. What changes would you like to see so that standards and regulations further **enable responsible innovation** in software-based medical devices, and keep pace with innovation and patient protection requirements? Hint: Examples include flexible regulatory pathways (e.g. SaMS Airlock rule); new standards to support current and future regulation, as well as new security, safety, quality, risk assessment, and governance requirements on developers, manufacturers, users (e.g. clinicians); new conformity assessment standards and guidelines.	(All) Breakout rooms
12:55 -13:15	**Feedback group sessions (Main room)**		Presentation by groups
13:15 -13:20	Closing remarks		Emma Glass - BSI
12:55 -13:05	Next steps, thanks, and closure		Irina Brass - UCL

References

1. Reg-MedTech: Regulatory and Standardization Challenges for Connected and Intelligent Medical Devices Project, PETRAS National Centre of Excellence for IoT Systems Cybersecurity. Available at: https://petras-iot.org/project/regulatory-and-standardization-challenges-for-connected-and-intelligent-medical-devices-reg-medtech/ .

2. MHRA, *Consultation on the future regulation of medical devices in the United Kingdom. Available at* https://www.gov.uk/government/consultations/consultation-on-the-future-regulation-of-medical-devices-in-the-united-kingdom. 2022.

3. MHRA, *Software and AI as a Medical Device Change Programme. Available online at* https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme. 2021.

4. The Alan Turing Institute, *Defining data science and AI. Available online at* https://www.turing.ac.uk/news/data-science-and-ai-glossary. 2022.

5. Caroline, B., et al., *Artificial Intelligence Cybersecurity Challenges; Threat Landscape for Artificial Intelligence*. 2020.

6. NCSC, *The NCSC glossary - a set of straightforward definitions for common cyber security terms. Available at* https://www.ncsc.gov.uk/information/ncsc-glossary. 2021.

7. FDA, *Artificial Intelligence and Machine Learning (AI/ML) Software as a Medical Device Action Plan. Available at* https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device. 2021.

8. FDA, *Proposed Regulatory Framework for Modifications to Artificial Intelligence/ Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD). p4. Available at* https://www.fda.gov/media/122535/download 2019.

9. MHRA., *Consultation outcome: Chapter 10 - Software as a Medical Device. Available at* https://www.gov.uk/government/consultations/consultation-on-the-future-regulation-of-medical-devices-in-the-united-kingdom/outcome/chapter-10-software-as-a-medical-device. 2022.

10. TGA, *Regulation of software based medical devices. Available at* https://www.tga.gov.au/regulation-software-based-medical-devices. 2022.

11. IMDRF, *Software as a Medical Device (SaMD): Key Definitions. Available at* https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf. 2013.

12. ISO, *ISO/IEC TR 24027:2021(en): Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making. Available at* https://www.iso.org/obp/ui/ - iso:std:iso-iec:tr:24027:ed-1:v1:en. 2021.

13. Emirate of Abu Dhabi, *DOH Internet of Medical Things (IOMT) Security Standard. Available at* https://www.dataguidance.com/news/emirate-abu-dhabi-de-

partment-health-sets-out-standard. 2020.

14. Wang, S., et al., *Artificial intelligence in lung cancer pathology image analysis*. Cancers, 2019. **11**(11): p. 1673.

15. Corrales Compagnucci, M., *The Future of Medical Device Regulation: Innovation and Protection. ed./I. Glenn Cohen; Timo Minssen; W. Nicholson Price II.; Christopher Robertson; Carmel Shachar*. 2022, Cambridge University Press.

16. Haughey, J., et al., *Medtech and the internet of medical things: How connected medical devices are transforming health care. Deloitte. Available at* https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf. 2018.

17. European Commission, *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. Available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745. 2017.

18. European Commission, *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. Available at* https://eur-lex.europa.eu/eli/reg/2017/746/oj. 2017.

19. MDCG, *MDCG 2021-24 Guidance on classification of medical devices. Available at* https://health.ec.europa.eu/system/files/2021-10/mdcg_2021-24_en_0.pdf. 2021.

20. Vokinger, K.N., T.J. Hwang, and A.S. Kesselheim, *Lifecycle Regulation and Evaluation of Artificial Intelligence and Machine Learning-Based Medical Devices. In The Future of Medical Device Regulation: Innovation and Protection. ed./I. Glenn Cohen; Timo Minssen; W. Nicholson Price II.; Christopher Robertson; Carmel Shachar*. 2022: Cambridge University Press.

21. Biasin, E. and E. Kamenjasevic, *Cybersecurity of medical devices: regulatory challenges in the EU*. 2020.

22. Brass, I. and J.H. Sowell, *Adaptive governance for the Internet of Things: Coping with emerging security risks*. Regulation & Governance, 2021. **15**(4): p. 1092-1110.

23. Florin, M.-V., *Governing Cyber Security Risks and Benefits of the Internet of Things: Application to Connected Vehicles and Medical Devices*. 2016, International Risk Governance Center (IRGC).

24. IMDRF, *Principles and Practices for Medical Device Cybersecurity. Available at* https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf. 2020.

25. WHO, *Generating Evidence for Artificial Intelligence-based Medical devices: A Framework for Training, Validation and Evaluation*. 2021.

26. McFadden, M., et al., *Harmonising Artificial Intelligence. The role of standards in the EU AI Regulation*. 2021, Oxford Information Labs. Available at https://oxil.uk/

publications/2021-12-02-oxford-internet-institute-oxil-harmonising-ai/.

27. European Commission, *Proposal for a regulation of the European Parliament and of the council. Laying down harmonised rules on artifical intelligence (ARTIFICIAL INTELLIGENCE ACT) and amending certain union legislative acts. A. Available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206. 2021.

28. KPMG, *Connected medical device cybersecurity: The competitive advantage of regulatory compliance. Intended for groups or individuals who represent manufacturers and others along the connected medical device distribution chain*. 2022.

29. European Parliament, *Resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)). Available at* https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.pdf. 2019.

30. Mkwashi, A.S., *Medical Device Regulations, Industrial Capabilities, and Affordable Healthcare Technology Development: Case Studies from the United Kingdom and South Africa*. 2020: Open University (United Kingdom).

31. MHRA, *Guidance: Regulating medical devices in the UK. Available at* https://www.gov.uk/guidance/regulating-medical-devices-in-the-uk. 2022.

32. MHRA, *Government response to consultation on the future regulation of medical devices in the United Kingdom. Available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1085333/Government_response_to_consultation_on_the_future_regulation_of_medical_devices_in_the_United_Kingdom.pdf. 2022.

33. Parasa, S., et al., *Proceedings from the first global artificial intelligence in gastroenterology and endoscopy Summit*. Gastrointestinal endoscopy, 2020. **92**(4): p. 938-945. e1.

34. Benjamens, S., P. Dhunnoo, and B. Meskó, *The state of artificial intelligence-based FDA-approved medical devices and algorithms: an online database*. NPJ digital medicine, 2020. **3**(1): p. 1-8.

35. Tsang, L., et al., *The impact of artificial intelligence on medical innovation in the European Union and United States*. Intellect Prop Technol Law J, 2017. **29**(8): p. 3-12.

36. FDA, *Classify Your Medical Device. Available at:* https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device. 2020.

37. Yaeger, K.A., et al., *United States regulatory approval of medical devices and software applications enhanced by artificial intelligence*. Health Policy and Technology, 2019. **8**(2): p. 192-197.

38. EPRS, *Understanding algorithmic decision-making: Opportunities and challenges. Available at* https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf. 2019.

39. Diab, W., *IEC and ISO work on artificial intelligence: Covering the entire AI ecosystem. Available at* https://etech.iec.ch/issue/iec-and-iso-work-on-artificial-intelli-

gence. 2022.

40. EPRS, *Artificial intelligence in healthcare: Applications, risks, and ethical and societal impacts. European Parliamentary Research Service Scientific Foresight Unit (STOA). PE 729.512* 2022.

41. EPRS, *Governing data and artificial intelligence for all Models for sustainable and just data governance. Available at* https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729533. 2022.

42. European Parliament, *Draft Opinion on the proposal for a regulation of the European Parliament and of the Council establishing the Union Secure Connectivity Programme for the period 2023-2027 (COM(2022)0057 – C9-0045/2022 – 2022/0039(COD)). Available at* https://www.europarl.europa.eu/doceo/document/ITRE-PA-719801_EN.pdf. 2022.

43. IMDRF, *Machine Learning-enabled Medical Devices: Key Terms and Definitions. IMDRF/AIMD WG/N67. Available at* https://www.imdrf.org/sites/default/files/2022-05/IMDRF AIMD WG Final Document N67.pdf. 2022.

44. Turpin, R., Hoefer, E., Leweling, J. and Baird, P. , *Machine Learning AI in Medical Devices: Adapting Regulatory Frameworks and Standards to Ensure safety and Performance [White Paper]. Association for the Advancement of Medical Instrumentation (AAMI), British Standards Institute (BSI).* 2020.

45. FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Guidance for Industry and Food and Drug Administration Staff. Available at* https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices. 2018.

46. FDA, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. Draft Guidance for Industry and Food and Drug Administration Staff. APRIL 2022. Available at* https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions. 2022.

47. European Parliament, *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). Available at* https://eur-lex.europa.eu/eli/reg/2019/881/oj. 2019.

48. MDCG, *MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices. Available at* https://ec.europa.eu/health/system/files/2022-01/md_cybersecurity_en.pdf. 2019.

49. TGA, *Medical device cyber security guidance for industry. Available at* https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf. 2021.

50. IMDRF, *Principles and Practices for the Cybersecurity of Legacy Medical Devic-*

es. Available online at https://www.imdrf.org/consultations/principles-and-practices-cybersecurity-legacy-medical-devices. 2022.

51. European Commission, *A European strategy for data, Available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN.2020.

52. European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act). Available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0767. 2020.

53. European Commission, *Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act). Available at* https://www.europeansources.info/record/proposal-for-a-regulation-on-harmonised-rules-on-fair-access-to-and-use-of-data-data-act/. 2022.

54. European Commission, *Shapping Europe's digital future: Data Act. Available at* https://digital-strategy.ec.europa.eu/en/policies/data-act - :~:text=While%20the%20Data%20Governance%20Regulation,of%20Things%20(IoT)%20devices. 2022.

55. European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space. Available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197. 2022.

56. Pesapane, F., M. Codari, and F. Sardanelli, *Artificial intelligence in medical imaging: threat or opportunity? Radiologists again at the forefront of innovation in medicine*. European radiology experimental, 2018. **2**(1): p. 1-10.

57. TFDA, *Guidance for Industry to Register Artificial Intelligence / Machine Learning - Based Software as Medical Device (AI/ML-Based SaMD). Available at* https://www.fda.gov.tw/TC/site.aspx?sid=39&r=1920435221. 2021.

58. Walsh, K., *An investigation into the regulatory challenges associated with artificial intelligence (AI) based medical devices and in-vitro diagnostic medical devices within Europe and the United States. MSc Thesis*. 2020.

59. Giantsidis, J., *FDA Releases Guidance On Cybersecurity In Medical Devices. Avaliable at* https://www.meddeviceonline.com/doc/fda-releases-guidance-on-cybersecurity-in-medical-devices-0001. 2022.

60. Fenech, M.E. and O. Buston, *AI in cardiac imaging: A UK-based perspective on addressing the ethical, social, and political challenges*. Frontiers in cardiovascular medicine, 2020. **7**: p. 54.

61. ISO, *ISO/IEC TR 29119-11:2020 Software and systems engineering — Software testing — Part 11: Guidelines on the testing of AI-based systems. Available at* https://www.iso.org/obp/ui/ - iso:std:iso-iec:tr:29119:-11:ed-1:v1:en. 2020.

62. Johner, C., *Regulatory Requirements for Medical Devices with Machine Learning. Johner-Institute. Available at* https://www.johner-institute.com/articles/ai-ma-

chine-learning/. 2022.

63. Greenlight guru, *What are the Stages of the Medical Device Life Cycle? Glossary. Available at* https://www.greenlight.guru/glossary/medical-device-life-cycle. 2022.

64. Johner, C., *Software Life Cycle Processes for Medical Devices. Johner-Institute. Software & IEC 62304. Software Lifecycle*. 2015.

65. FDA, *General Principles of Software Validation; Final Guidance for Industry and FDA Staff. Available at* https://www.fda.gov/files/medical devices/published/General-Principles-of-Software-Validation---Final-Guidance-for-Industry-and-FDA-Staff.pdf. 2019.

66. IEC, *International IEC Standard 62304: 2006 - Medical device software – Software life cycle processes. Available at* https://webstore.iec.ch/preview/info_iec62304%7Bed1.0%7Den_d.pdf. 2006.

67. OECD, *Series on principles of good laboratory practice and compliance monitoring. Number 22. Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity. JT03481133. Available at* https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=env/cbc/mono(2021)26&doclanguage=en. 2021.

68. ISO/IEEE, *ISO/IEEE 11073-10201: 2020(en) Health informatics — Device interoperability — Part 10201: Point-of-care medical device communication — Domain information model. Available at* https://www.iso.org/obp/ui/ - iso:std:iso-ieee:11073:-10201:ed-2:v1:en. 2020.

69. ISO/IEEE, *ISO/IEEE 11073-10207: 2019 (en) Health informatics — Personal health device communication — Part 10207: Domain information and service model for service-oriented point-of-care medical device communication. Available at* https://www.iso.org/obp/ui/ - iso:std:iso-ieee:11073:-10207:ed-1:v1:en. 2019.

70. GDS, *A guide to using artificial intelligence in the public sector. The economic impact of artificial intelligence on the UK economy (PwC, 2017). Available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/964787/A_guide_to_using_AI_in_the_public_sector__Mobile_version_.pdf. 2017.

71. Digital Curation Centre, *The Role of Data in AI. Report for the Data Governance Working Group of the Global Partnership of AI. Available at* https://gpai.ai/projects/data-governance/role-of-data-in-ai.pdf. 2020.

72. European Commission, *European Council conclusions, 28 June 2018. Press release. Available at* https://www.consilium.europa.eu/en/press/press-releases/2018/06/29/20180628-euco-conclusions-final/. 2018.

73. Turpin, R., et al., *Machine learning and medical devices: data quality and bias. Available at* https://compliancenavigator.bsigroup.com/en/medicaldeviceblog/machine-learning-and-medical-devices-data-quality-and-bias/. 2020.

74. European Parliament, *Resolution of 20 October 2020 with recommendations*

to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). 2020.

75. Tschider, C.A., *Medical Device Artificial Intelligence: The New Tort Frontier*. BYU L. Rev., 2020. **46**: p. 1551.

76. Rud, A., *Artificial Intelligence in Medical Devices Verifying and validating AI-based medical devices. TUV SUD White paper. Germany. Available at* https://www.tuvsud.com/en-gb/press-and-media/2021/august/artificial-intelligence-in-medical-devices. 2021.

77. Hassan, S., et al., *Big data and predictive analytics in healthcare in Bangladesh: regulatory challenges*. Heliyon, 2021. **7**(6): p. e07179.

78. PEW, *How FDA Regulates Artificial Intelligence in Medical Products As technology evolves, oversight will need to keep pace. Issue brief. Available at* https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2021/08/how-fda-regulates-artificial-intelligence-in-medical-products. 2021.

79. Kelly, S., *FDA pushes back against criticism of third party 510(k) review. Available at* https://www.medtechdive.com/news/fda-pushes-back-against-criticism-of-third-party-510k-review/564957/. 2019.

80. Ezeani, G., Maj, N., Sassenberg, J., Song, J., Tedroff, M., , *Regulatory and Standardization Challenges for Connected and Intelligent Medical Devices. University College London. 2020. Available at* https://www.ucl.ac.uk/steapp/sites/steapp/files/group_11_report_202011068.pdf. 2020.

81. HSA, *Regulatory Guidelines for Software Medical Devices - A Lifecycle Approach. Available at* https://www.hsa.gov.sg/docs/default-source/announcements/regulatory-updates/regulatory-guidelines-for-software-medical-devices--a-lifecycle-approach.pdf. 2019.

82. McKeon, J., *53% of Connected Medical Devices Contain Critical Vulnerabilities. Available at online at* https://healthitsecurity.com/news/53-of-connected-medical-devices-contain-critical-vulnerabilities. 2022.

83. Baranchuk, A., et al., *Cybersecurity for cardiac implantable electronic devices: What should you know?* Journal of the American College of Cardiology, 2018. **71**(11): p. 1284-1288.

84. Finkle, J., *J&J warns diabetic patients: Insulin pump vulnerable to hacking. Available online at* https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L. 2016.

85. Beardsley, T., *R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump. Available online at* https://www.rapid7.com/blog/post/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/. 2019.

86. FDA, *FDA In Brief: FDA warns patients, providers about cybersecurity concerns with certain Medtronic implantable cardiac devices. Available at* https://www.fda.gov/news-events/fda-brief/fda-brief-fda-warns-patients-providers-about-cyber-

security-concerns-certain-medtronic-implantable. 2018.
87. FDA, *FDA warns patients and health care providers about potential cybersecurity concerns with certain Medtronic insulin pumps. Available at* https://www.fda.gov/news-events/press-announcements/fda-warns-patients-and-health-care-providers-about-potential-cybersecurity-concerns-certain. 2019.
88. FDA, *Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication. Available at* https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-ge-healthcare-clinical-information-central-stations-and. 2020.
89. Alexander, B. and A. Baranchuk, *Cybersecurity and cardiac implantable electronic devices*. Nature Reviews Cardiology, 2020. **17**(6): p. 315-317.
90. Crotty, J. and I. Horrocks, *Managing legacy system costs: A case study of a meta-assessment model to identify solutions in a large financial services company*. Applied computing and informatics, 2017. **13**(2): p. 175-183.
91. Johner, C., *What Manufacturers Need to Know about Legacy Devices. Available at* https://www.johner-institute.com/articles/health-care/and-more/what-manufacturers-need-to-know-about-legacy/. 2022.
92. Smart, W., *Lessons learned review of the WannaCry ransomware cyber attack*. Department of Health and Social Care: London, UK, 2018. **1**: p. 10-1038.
93. Laplante, P., et al., *Artificial intelligence and critical systems: from hype to reality*. Computer, 2020. **53**(11): p. 45-52.
94. C3.ai, *Glossary: Explainability What is Explainability? Available online at* https://c3.ai/glossary/machine-learning/explainability/ - :~:text=Explainability%20(also%20referred%20to%20as,being%20at%20an%20acceptable%20level. 2022.
95. Pintelas, E., et al., *Explainable machine learning framework for image classification problems: case study on glioma cancer prediction*. Journal of imaging, 2020. **6**(6): p. 37.
96. Rudin, C., et al., *Interpretable machine learning: Fundamental principles and 10 grand challenges*. Statistics Surveys, 2022. **16**: p. 1-85.
97. Norori, N., et al., *Addressing bias in big data and AI for health care: A call for open science*. Patterns, 2021. **2**(10): p. 100347.
98. Khalilipur, E., et al., *Clinical decision-making and personality traits; Achilles' heel of artificial intelligence*. Research in Cardiovascular Medicine, 2022. **11**(1): p. 36.
99. Walch, K., *9 data quality issues that can sideline AI projects. TechTarget. Available at* https://www.techtarget.com/searchenterpriseai/feature/9-data-quality-issues-that-can-sideline-AI-projects. 2020.
100. FDA, *Data Integrity and Compliance With CGMP Guidance for Industry. DRAFT GUIDANCE. Available at* https://www.fda.gov/files/drugs/published/Data-Integrity-and-Compliance-With-Current-Good-Manufacturing-Practice-Guidance-for-Industry.pdf. 2016.

101. Karthikeyan, C. and A. Benjamin, *An exploratory study on business data integrity for effective business; a techno business leadership perspective*. International Journal of Research in Social Sciences, 2019. **9**(4): p. 167-201.