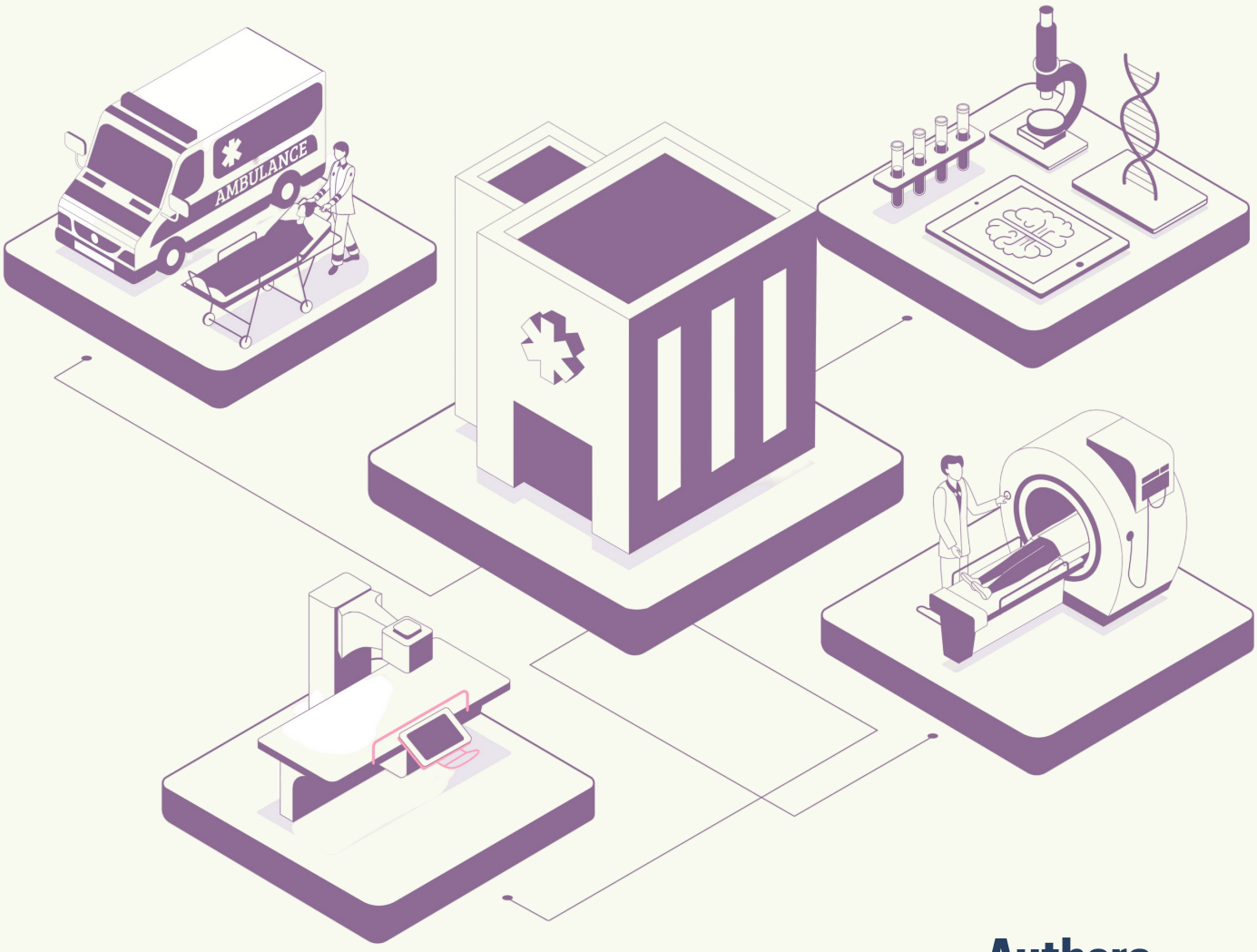
Report

Regulatory and Standardization Challenges for Connected and Intelligent Medical Devices



Authors

Gabriella Ezeani
Jan Sassenberg
Jiehui Song
Malla Tedroff
Natalia Maj

UCL In Partnership with bsi.

CONTENTS

Please cite this report as:

Ezeani, G., Maj, N., Sassenberg, J., Song, J., Tedroff, M., Regulatory and Standardization Challenges for Connected and Intelligent Medical Devices. University College London. 2020.

ACKNOWLEDGEMENTS

UCL team acknowledgements

Throughout the eight months of intensive research, we have received a significant amount of support which was crucial for the success of this project.

First and foremost, we would like to thank our inspiring project mentor, Dr Irina Brass, for going above and beyond and investing so much time in providing us with valuable guidance and constructive feedback, guiding us through the months of research, and for generously sharing her knowledge with us. Her enthusiasm and encouragement were crucial in keeping us on track and helped us manage the unexpected complications arising from COVID-19. Irina's energy, passion and expertise never ceased to impress us during our Friday morning calls.

To our most supportive clients, Dr Matthew Chiles, Rob Turpin, Paul Sim and Gill Jackson from the BSI, we deeply appreciate your active involvement in our research project and for providing us with valuable inputs and resources. We are also extremely grateful for your patience in guiding us through the complicated landscape of standards and medical devices. Thank you for giving us the opportunity to work with your esteemed organisation.

Our sincere thanks also go to the UCL Department of Science, Technology, Engineering and Public Policy (UCL STEaPP) faculty, especially Dr Carla Washbourne and Mr Alan Seatwo, for equipping us with the knowledge and tools which guided our research. We would also like to thank Dr Leonie Tanczer for patiently guiding us through the research ethics application process, and for the extremely prompt responses to our queries. To our UCL STEaPP Master of Public Administration colleagues, thanks for the great memories – we couldn't have asked for better people to go through this intense year with.

Finally, we would like to sincerely thank all participants who took part in our interviews and survey. Your insights were fundamental for this research.

BSI acknowledgements

The BSI team of Matthew Chiles, Rob Turpin, Paul Sim and Gill Jackson would like to acknowledge and thank the UCL project team for their tremendous effort, commitment, diligence and professionalism in undertaking the research, compiling the final report and producing the supporting documents.

The group's desire and capacity to learn, openness to feedback and debate, and their creativity in approach has meant they have been an absolute pleasure to work with. Their knowledge, skills and abilities were most amply demonstrated when they developed and delivered a hugely successful session at the BSI Standards Conference in April 2020. Without exception, each team member is a credit to both STEaPP and UCL.

We would also like to extend our enormous thanks and gratitude to Dr Irina Brass, the team's supervisor, for her leadership and support in the overall management of the project, her passion for standards education and her commitment to enhancing and strengthening the BSI/UCL education partnership.

For BSI, this student research project provides an important source of information and contribution to the medical technology standards development process, which will help to ensure the currency of existing standards and the content of future standards.

EXECUTIVE SUMMARY

Recent healthcare innovations are disrupting the established regulatory and standardization frameworks. With rapid technological advancements, such as artificial intelligence, wearables and wellness apps, new device functionalities and characteristics are introduced. They increasingly blur the lines between medical devices and consumer technology.

Moreover, embedded connectivity and intelligence have 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.

This report investigates these regulatory and standardization challenges related to connected and intelligent medical devices. It also identifies the main trends shaping this field and provides recommendations to the British Standards Institution (BSI) on how to adapt its standards development practices.

Key Findings

- Regulations and standards do not address the characteristics and complexities of new technologies, such as artificial intelligence. In addition, technological development occurs faster than regulatory changes. As a result, regulations and standards are falling behind the pace of innovation, leading to the emergence of regulatory and standardization gaps. These, in turn, have adverse effects on patient safety and manufacturers' ability to introduce innovative solutions.
- Stakeholders recognise the benefits of using standards to ensure quality of devices and provide the presumption of conformity with the European regulatory requirements. However, the perceived inaccessibility of standards may prevent stakeholders from using them throughout the lifecycle.
- There are numerous barriers to innovation in the healthcare sector. The main ones include regulatory burdens (particularly affecting small and medium sized enterprises), organisational challenges such as hiring the right expertise and aligning software teams with compliance requirements.
- Innovation and trends in the sector are driven by factors such as technological developments, investments, regulatory change, cross-industry developments, stakeholder collaboration, and current events such as COVID-19.

- Connected, intelligent medical devices give rise to new safety and security risks. To mitigate them, manufacturers should apply a safety and security by design approach to the medical device development process.
- Connected, intelligent medical devices can be used in ways unintended and unaccounted for by manufacturers, resulting in the circumvention of safety mechanisms that have been put in place.

Based on these findings, the following recommendations are presented for BSI's consideration:

Recommendation 1	Recommendation 2	Recommendation 3	Recommendation 4
•Champion global standards development for emerging technologies such as AI	•Review ethical considerations arising from the use of connected and intelligent medical devices to build trust in these devices	•Facilitate SMEs' participation in the standards-making process, by providing incentives, supporting agile standards-making practices and providing educational resources	•Make standards more understandable, by including clear descriptions and visualisations and using simple language

Additionally, based on the research insights, an accompanying Entrepreneurs' Guide (Annex 6) was produced to support medical device entrepreneurs in navigating the relevant regulations and standards.

These findings and recommendations are based on a mixed-method research approach (Annex 1). The secondary research involved a literature review (Annex 2) and horizon scanning exercise. The primary research comprised interviews with 19 experts across academia, industry and public authorities (Annex 3) and the UCL-BSI survey with 50 participants (Annex 4).

Information on the project

This report is a result of an eight-month collaboration between University College London's Department of Science, Technology, Engineering and Public Policy (UCL STEaPP) and the BSI. The UCL STEaPP team comprised five Masters of Public Administration in Digital Technologies and Policy candidates, mentored by Dr Irina Brass.

GLOSSARY

AI – Artificial Intelligence

CE mark – certification mark indicating conformity with health, safety and environmental protection standards, for products sold in the European Economic Area

CEN – European Committee for Standardization

DCB – Data Coordination Board

European harmonized standards – standards used to demonstrate the presumption of conformity with the European regulatory framework on medical devices (the MDR/ IVDR)

GSPR – the General Safety and Performance Requirements, as set out in Annex I MDR

GDPR – General Data Protection Regulation (2016/679)

Global consensus standards – the attempt to harmonize standards globally

ICO – Information Commissioner's Office

IMDRF – International Medical Device Regulators Forum

ISO – International Organization for Standardization

IVDD – the In Vitro Diagnostic Medical Device Directive (98/79/EC)

IVDR – the In Vitro Diagnostic Medical Device Regulation (2017/746)

MDD – the Medical Device Directive (93/42/ECC)

MDR – the Medical Device Regulation (2017/745)

Medical device – under Article 2(1) of the MDR, it means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,

- investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
- providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,
- and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

NHS – National Health Service

Presumption of conformity – a concept commonly used in the European Union (EU) to demonstrate compliance with relevant EU legislation through the use of European harmonized standards[1,2]

SaMD – Software as Medical Device

SME – Small and medium sized enterprise

UK – United Kingdom

US FDA – United States Food and Drugs Administration

1 INTRODUCTION

The emergence of connected, intelligent medical devices creates significant benefits for the healthcare sector and offers new solutions to patients. The medical device industry is highly diverse, and advanced technologies give rise to innovations such as smart monitoring, personalised healthcare, and clinical support systems. Overall, new technologies can automate processes, add capabilities to existing products, increase the efficiency of the healthcare system and, ultimately, improve patient care.

However, these rapid technological advancements also create considerable risks and challenges. Embedded connectivity and intelligence enable new device functionalities and use cases, which create questions around transparency, safety and security. Moreover, as devices are increasingly used directly by patients, the boundaries between medical devices and consumer technology are blurred. This introduces issues around usability and end-user interactions. There is also a question whether consumers can use a device to capture measurements or administer treatment as accurately as a trained clinician would.

Additionally, embedded connectivity and intelligence have significant safety and security implications across the entire device lifecycle and supply chain. They make devices more prone to cybersecurity risks and vulnerabilities. The use of AI in healthcare also creates new legal and ethical questions, regarding fairness, interpretability and accountability.

As a result, connected, intelligent medical devices disrupt the established regulatory and standardization frameworks. Medical devices operate in a highly regulated environment with well-established regimes in Europe, North America and Asia to ensure patient safety and efficacy. Traditionally, standards have played an essential role in complementing regulations, and ensuring patient safety by enhancing the reliability and performance of medical devices and establishing accountability across various stakeholders. However, the fast pace of technological development as well as the complex nature of advanced technologies make it difficult for the regulatory and standardization frameworks to adapt. This gives rise to regulatory and standardization gaps. These gaps, in turn, create challenges for regulators and organisations in the sector, and may have adverse effects on the public.

Given these immense risks and challenges, as well as the potential benefits of connected, intelligent devices, this report explores the regulatory and standardization challenges in the field.

Based on these key identified challenges, this report has been guided by the following key research questions to structure the analysis:

- What are the regulatory and standardization gaps regarding connected and intelligent medical devices?
- What are the challenges to the safety and security of connected and intelligent medical devices across the supply chain?
- What are the main trends and innovations emerging in the field of intelligent and connected medical devices?

2 METHODOLOGY

This research project relied on a mixed-methods approach, using primary and secondary data sources. See Annex 1 for further details on the methodology.

Literature review (for details see Annex 2)

The literature review focused on academic literature and policy-relevant documents, including standards, legislation and guidelines. The purpose was to understand the state of academic research on connected and intelligent medical devices. To answer the research questions, the review focused on:

- the regulatory and standardization challenges,
- the safety and security risks arising across the device lifecycle, and
- the innovation landscape and emerging trends.

The literature review served to identify the key findings which were subsequently explored and validated through other research streams.

Horizon scanning (for findings see Figure 7)

A horizon scanning exercise was conducted to complement the literature review. The focus was on reviewing documents such as government reports, whitepapers and news articles. The purpose of horizon scanning was to inform our understanding of the drivers of change in the field of connected and intelligent medical devices, especially the main trends and potential future regulatory and standardization gaps.

Interviews (for details see Annex 3)

Interviews with 19 representatives of industry, academia and public authorities were conducted from 9 June 2020 to 25 August 2020. They provided the opportunity to obtain detailed insights into the challenges created by connected and intelligent medical devices. Interviews were semi-structured, which allowed for a free discussion, whilst also ensuring that the 'core' topics were covered. The interviews were subsequently thematically coded. Each interviewee is represented by a reference from P1 to P19 in this report.

UCL-BSI Survey (for details see Annex 4)

An online survey on connected, intelligent medical devices was hosted by BSI between 10 June 2020 and 24 July 2020. It consisted of 19 questions (single and multiple-choice, and open-ended). 50 respondents took the survey. The UCL-BSI survey provided qualitative and quantitative responses on various challenges encountered by medical device manufacturers.

Participant observation

The researchers attended online industry events to engage with stakeholders, as the initial plan to participate in conferences in-person was affected by the COVID-19 outbreak. Most significantly, we delivered a presentation during the BSI e-Conference in April 2020. We will also present our research at the IMPACT 2020 conference on 29 September 2020.

3 RESEARCH FINDINGS

PART A: CURRENT CHALLENGES

3.1 Regulations and standards

3.1.1. Evolving regulatory landscape

The rapid pace of innovation and the growing recognition of safety risks resulting from connected, intelligent medical devices, have contributed to increased regulatory activity around the world.

The recognition of technological change was crucial in driving changes to the EU legislation[3–5] and the decision to implement new regulations, the MDR and the IVDR. The decision to use regulations, rather than directives as in the past, has important implications. Regulations are more prescriptive and detailed, and automatically apply to all Member States, without the need to introduce separate legislation. There is also significant regulatory activity at the IMDRF level and in the US, primarily linked to the emergence of software-based medical devices and technological change.[6,7] Moreover, Brexit has fuelled policy discussions on the future of the regulatory framework for medical devices and patient safety protection in the UK (see section 3.1.3).

In addition to regulations specific to medical devices, manufacturers of connected, intelligent devices must also comply with other regulatory frameworks, for instance, the GDPR in Europe. It imposed onerous privacy and data management obligations and has important implications for various stages of a medical device lifecycle.[7] This creates new questions and challenges which do not apply in the case of 'traditional' devices. Manufacturers need to consider how to implement such GDPR provisions as the data minimisation principle or the right to be forgotten.

Overall, the regulatory landscape around medical devices is complex and highly rigorous. This helps to ensure patient safety and device efficacy but can also lead to unintended consequences. This is particularly evident in the context of possible adverse impacts on innovation (see section 3.2.1). Moreover, despite medical devices being highly regulated, the increased embedding of connectivity and intelligence creates important regulatory gaps and grey areas (see section 3.5.3).

3.1.2. MDR/IVDR perception and impact

The MDR/ IVDR will reshape the medical devices landscape in Europe and lead to significant consequences for the manufacturers of connected, intelligent medical devices. Below, we address the main implications of the new framework for these devices.

Key changes – a broader definition of medical devices

A broader definition of a 'medical device' under the MDR/IVDR compared to the previous regulatory framework has important implications for connected, intelligent devices. The definition (Article 2(1)) now explicitly includes software.[6] It also covers devices dealing with 'prognosis' and 'prediction' of diseases. These functions are often performed by software-driven devices, meaning that more connected, intelligent medical devices will be regulated under the MDR/IVDR. This is confirmed by the UCL-BSI survey – certain devices that were unclassified under the MDD, will be classified as Class IIa under the MDR (3 respondents).

This change creates important challenges for manufacturers and regulators, as the scope of the regime and classification are not widely understood. Developers of digital health solutions may not realise that their products are regulated (P7). Indeed, it has been observed that numerous digital health apps are not certified as medical devices, although they most likely should be (P7, P19). Accordingly, certain products enter the market without being subject to regulatory oversight, potentially creating risks for patient safety. Alternatively, manufacturers may realise that their device is a medical device at the late stage of product development (P15). This may result in significant compliance challenges and affect the commercial feasibility of the project.

Importantly, digital health apps also enter the market in different ways than traditional medical devices, for instance through app stores. However, there is currently no clear process in place on dealing with devices available through app stores that are potentially misclassified (P3, P19). Nevertheless, it has been noted that European regulators are currently working on how to apply the MDR in those circumstances (P19). For instance, if app stores qualify as distributors (P19), they would have the obligation to verify whether digital health apps are appropriately certified.

Key changes – up-classification of software

Classification Rule 11 in Annex VIII MDR means that software is generally up-classified to at least Class IIa. As highlighted in the literature[8] and one interview (P7), Class I software devices will be uncommon. Moreover, the UCL-BSI survey shows that re-classification is common – 26 out of 50 respondents noted that their device classification increased. This even included one device changing from Class I to Class III.

This up-classification has significant implications for manufacturers of connected, intelligent medical devices. In contrast to Class I devices which can be self-certified, Class IIa devices and above, require a Notified Body oversight and are subject to more rigorous compliance procedures.

Key changes – new requirements for medical software

The MDR also includes new obligations for medical software manufacturers. This is evident in Annex I, which includes software-specific GSPRs. They concern, for instance, cybersecurity, data management and interactions between software and the environment. They also reflect the recognition of the increasingly connected nature of medical devices. Overall, the GSPR changes have a positive impact on how software is regulated (P19). There are also specific technical documentation provisions under Annex II MDR, requiring manufactures to provide information on software verification and validation.

However, in some areas, these changes are not sufficient, as the MDR does not cover more advanced algorithms, such as AI and ML (P19). This has important implications for manufacturers and creates regulatory gaps, discussed in detail in section 3.5.3.

GSPRs	Requirement
14.2 Annex I	Devices shall be designed and manufactured in such a way to remove or reduce the risks associated with the possible negative interaction between software and the IT environment
17.1 Annex I	Software must ensure repeatability, reliability and performance in line with the intended use
17.2 Annex I	Software shall be developed and manufactured in accordance with the state of the art
17.4 Annex I	Manufacturers shall set out minimum requirements concerning hardware, IT network characteristics and IT security measures

Figure 1: Key software-related GSPRs in the MDR

Key benefits – patient safety

The main benefit that the MDR and IVDR bring is improved patient safety, through better transparency, evidence requirements and post-market surveillance regime (see Annex 2). This has been confirmed by several industry stakeholders, who noted that the legislation is successful at achieving this objective and has resulted in significant improvements to safety (P18, P19). In this context, increased rigour and quality are also recognised as important improvements of the MDR/IVDR (P11). Moreover, the broadening of the medical device definition was also a beneficial change, as it helped address deficiencies in the MDD/IVDD framework (P6, P18).

Software up-classification under Rule 11 has attracted significant coverage in the industry because of the increased compliance burdens. This change is also crucial in ensuring safety (P19). Moreover, software classification will be more risk-based under the MDR, rather than focused on physical hazards like under the MDD – this approach reflects risks to patient safety more adequately (P19).

However, doubts were also expressed about how significant the practical impact of the new regulations was on patient safety, as manufacturers were already able to produce safe devices under the MDD (P2). In particular, malicious intent to 'cut corners' may still not be prevented (P2). Still, it overall appears that the new framework imposes more robust, stringent obligations on manufacturers across the entire life cycle, likely to result in improved safety.[8]

Key challenges – regulatory burdens and challenges

Overall, the MDR/IVDR mean that manufacturers will have to comply with more onerous compliance requirements, both at the pre-market and post-market stage. This also applies to other stakeholders in the supply chain, such as distributors and importers.

The key pre-market obligations on manufacturers include an increased software classification and greater clinical evidence requirements. There have also been changes to the GSPRs compared to the MDD's Essential Requirements, for instance, with tighter rules around risk and quality management. Importantly, existing devices need to be recertified under the new regulations, even if they operated safely. At the post-market stage, there are enhanced post-market surveillance and vigilance requirements, with new rules around clinical and performance evaluation and clinical investigations.

These onerous requirements have certain unintended consequences – they make it more difficult for manufacturers to manage regulatory compliance. Manufacturers, especially SMEs, find it difficult to understand regulations and apply them in practice, according to several industry and regulatory representatives (P7, P8, P10, P11). The UCL-BSI survey further

highlighted that compliance burdens are among the key challenges faced by organisations in the medical device market.

When asked about the specific regulatory challenges faced (Figure 2), most respondents noted challenges around the technologies they deploy (27 respondents), classification (25 respondents) and generally in the healthcare sector (25 respondents). In addition, a large group of respondents noted challenges related to the costs of compliance (18 respondents). Indeed, costs and compliance with the MDR are considered by some UCL-BSI survey participants as the key challenges to their organisation within the next three years.

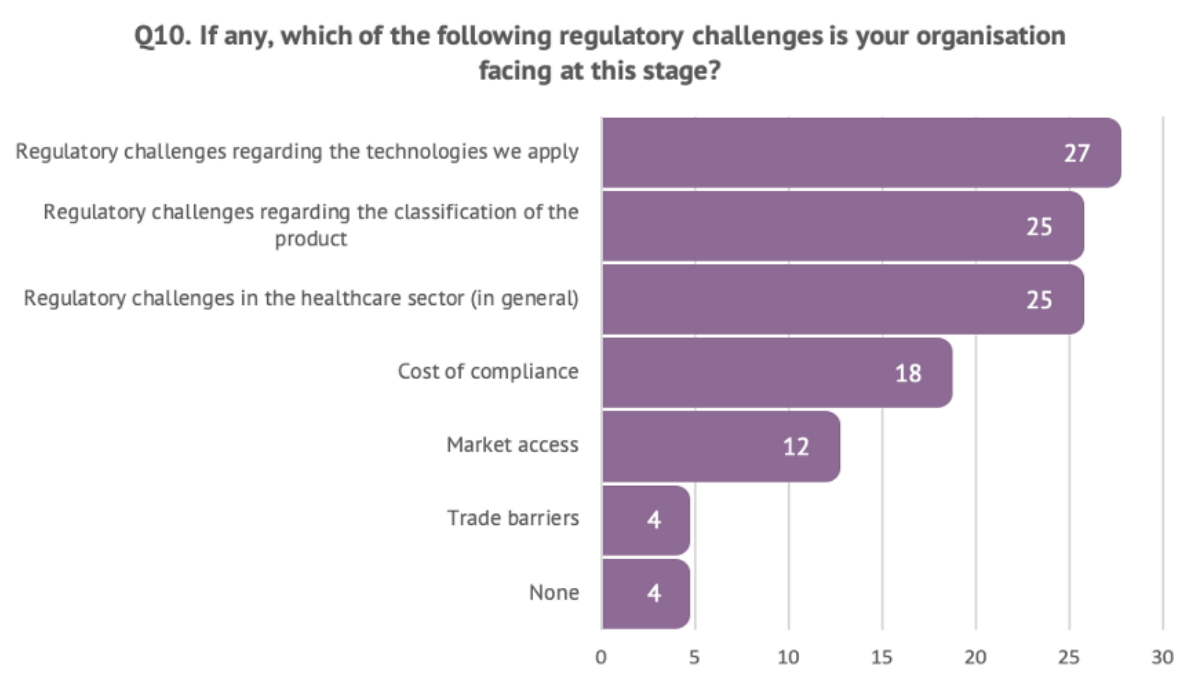


Figure 2: Regulatory challenges faced by UCL-BSI survey respondents

Importantly, the MDR also created organisational challenges, with some UCL-BSI survey respondents mentioning the difficulty of finding and affording the expertise to manage regulatory compliance (2 respondents) or the need to establish a new internal function (1 respondent).

Increased compliance burdens are likely to have a significant impact, especially on smaller manufacturers, who are crucial in driving innovation in the field of medical devices. Further insights into the impact of the MDR on innovation are covered in section 3.2.1.

Key challenges – MDR readiness

Readiness for the original MDR application date of May 2020 has emerged as an important challenge across all research streams. This has been linked to two critical issues. First, there was a challenge relating to manufacturers' readiness, as they had to adapt their internal processes and prepare for frequently more burdensome notification processes. Industry research indicated that a significant proportion of manufacturers did not feel ready for the transition in May 2020.[9] Second, there was an issue around the limited Notified Body capacity. Under the MDR, Notified Bodies must be redesignated and are subject to more onerous rules. Moreover, all devices currently on the market must be recertified. This results in significant issues with Notified Body capacity to process applications (P7, P18, P19).

In this context, the European Commission's decision to delay the application period by one year, to May 2021, as a result of COVID-19, was considered highly beneficial for the healthcare industry (P7, P11). Nevertheless, it emerges that that 12 months may be insufficient to address the Notified Body capacity shortage.[10] This, in turn, may result in bottlenecks and delays to obtaining regulatory approvals in the EU, potentially slowing down market access, with negative implications for innovation and patient safety. Furthermore, stakeholders also request delaying the IVDR transition.[11]

Moreover, it emerges that the delay is being used by manufacturers to circumvent the MDR, rather than to ensure an effective transition (P11). Manufacturers have more time to apply for certificates under the MDD provisions, which may be valid up to 2024. It is feared that this may have a negative impact on the quality of devices on the market, as they will be subject to less stringent requirements than under the MDR (P11).

3.1.3. International landscape

The global character of the medical devices market and innovation underlines the importance of international approaches to support convergence. In particular, international convergence is considered crucial in improving patient safety, by supporting innovation, facilitating market access and supporting trade.[12] In recent years, there has been significant international progress in achieving greater convergence through the IMDRF and the move towards regulations in the EU.[7,13,14]

However, achieving international convergence is a challenging process, and areas of potential divergence are emerging. For instance, the EU and the US are taking different regulatory approaches to digital health solutions and new technologies, such as AI (P11, P18). In particular, the US FDA has been active in issuing guidance and establishing programmes

around AI. Its approach is sometimes considered more risk-based and flexible than the MDR framework.[15]

Brexit will also likely contribute to international divergence, as indicated in the horizon scanning exercise and interviews (P18). The delayed MDR application date (May 2021) falls after the end of the Brexit transition period, meaning that it will not form a part of the retained law. On 1 September 2020, the MHRA published its guidance on the future of medical devices' regulation in the UK.[16] Crucially, the regulatory system in Northern Ireland will differ from the framework in Great Britain – Northern Ireland will follow the EU framework and the MDR will apply there from May 2021. In Great Britain, future legislation will establish a new market route and all devices will have to be registered with the MHRA. A new UKCA mark will be introduced to demonstrate that medical devices can be placed on the British market, but it will not be recognised in the EU/EEA. However, the CE mark will be recognised in the UK until the end of June 2023.

These Brexit-related changes have important implications. Manufacturers intending to sell their devices in the UK and the EU will have to go through different approval routes. Non-UK-based manufacturers will also have to designate a UK Responsible Person to register their device with the MHRA. However, it remains unclear to what extent the conformity assessment requirements in the UK and the EU will differ. The MHRA noted that it would engage with the stakeholders to build a robust system. It will also consider international standards. It is worth noting that there appears to be a tension in the UK policy direction (P19) between encouraging greater market access and imposing stricter safety requirements, as proposed in the Independent Medicines and Medical Devices Safety Review[18] published by Baroness Cumberlege.

However, the MHRA's September 2020 guidelines reflect that safety is the key focus .[16] Furthermore, the MHRA's position will be significantly strengthened after Brexit. In particular, the Medicines and Medical Devices Bill will give it more enforcement powers, for instance, to pursue civil sanctions for non-compliance. Although the MHRA's guidelines provided greater clarity on the post-Brexit regulatory landscape, manufacturers should continue to monitor developments in the UK as changes remain subject to stakeholder engagement and parliamentary approval.

3.1.4. Standards

Role of standards

Standards are a documented and "agreed way of doing something".[19] In the context of medical devices, they span a wide range of activities, including manufacturing a device, providing a healthcare service or managing electronic health records.[19]

The central role of standards in the field of medical devices is to ensure patient safety by enhancing the reliability and performance of medical devices.[20] Standards serve to define the criteria for a minimum viable product, provide quality assurance of an organisation's processes and establish accountability across various stakeholders in this industry.[20]

Types of standards

Standards which apply to connected and intelligent medical devices are developed by various organisations and may apply on different levels, such as the following:

- International[21] and regional standards[22–24]
- National standards[25]
- Healthcare system standards[26,27]

These standards may be further categorised based on the sectors, processes or devices for which they are used.[19] This is presented in Figure 3 below:

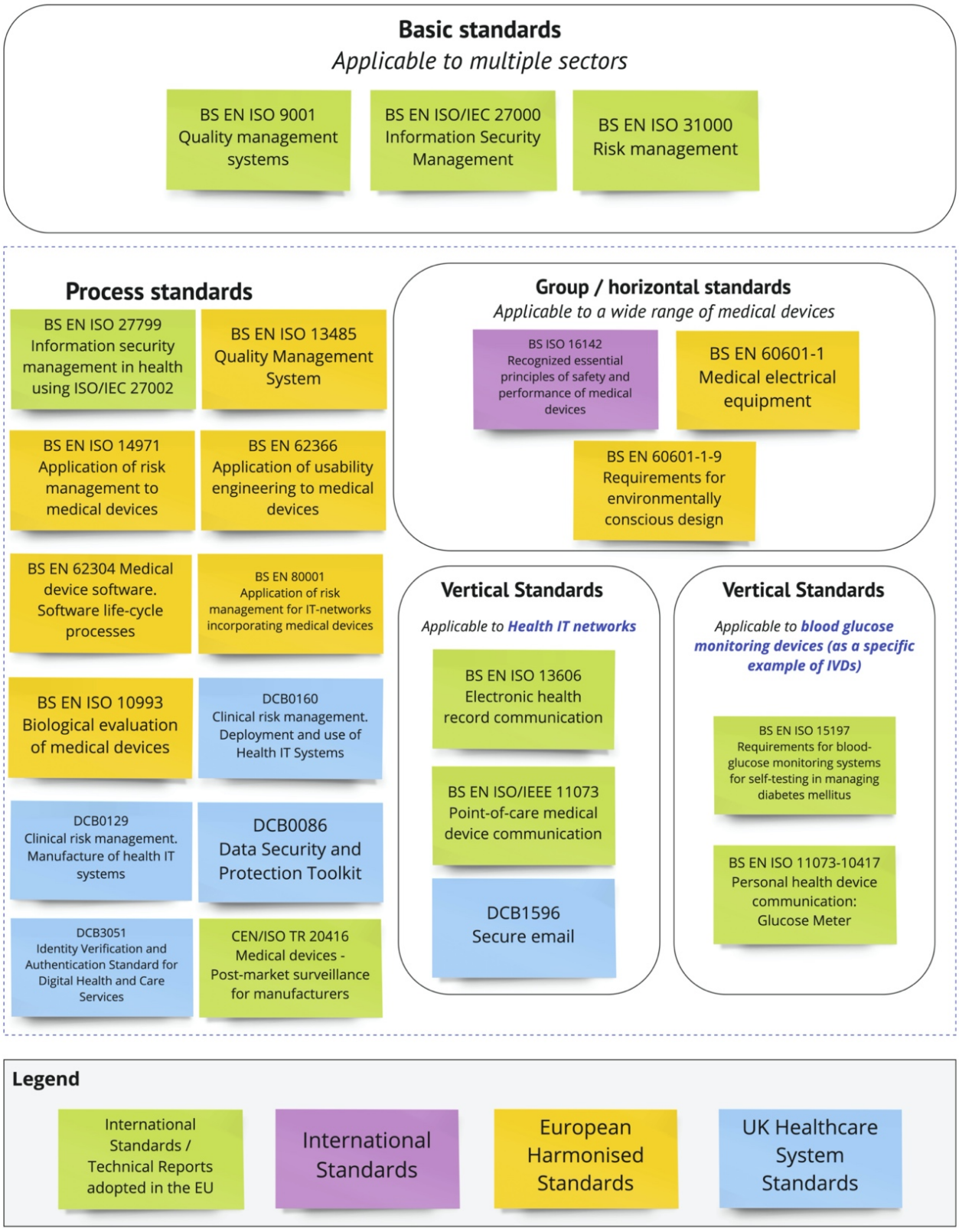


Figure 3: Types of standards

How standards complement regulation

Regulations and standards are closely connected.[28] For instance, compliance with European harmonized standards is considered to provide the presumption of conformity with European regulatory requirements.[28]

However, there are some key differences between standards and regulations in the medical devices industry. While medical devices are subjected to mandatory regulations, the use of standards is always voluntary[29], even when referenced in regulations. Regardless of the level at which standards are applied, they could serve similar purposes. For instance, international standards and health system standards, such as the BS EN ISO 13485 and DCB0129 respectively, generate the chain of evidence required to prove device efficacy and impact on patient safety under the relevant regulations[30] such as the MDR/IVDR and the UK's Health and Social Care Act 2012. Manufacturers of medical devices may choose to adopt the applicable standards fully or partially or choose alternative means to provide the presumption of conformity with specific regulatory requirements.

Moreover, regional and international standards may be applied and adopted across various countries, while regulations are usually applied on a national level and are limited to certain jurisdictions.[22,31] For example, manufacturers may use European harmonized standards to demonstrate conformity with the MDR's GSPRs. Similarly, the US FDA recognises a list of consensus standards which they will recognise as a Declaration of Conformity.[32] In this context, standards play an essential role in facilitating access to international markets.

Lastly, compared to the legalistic nature of enacting and updating regulations, standards may be updated and revised as long as there is consensus from committee members.[22,31] With a review of key international standards occurring every five years[33,34], standards are more likely to be up to date and represent the state-of-the-art (P19).

Engaging with standards

The UCL-BSI survey reflected that all respondents engage with standards, including formal standards and industry standards.

There is consensus among interviewees that the primary role of standards is to ensure patient safety, through quality assurance of device designs, organisational processes and information governance (P3, P5-P9, P11-P12, P14, P15, P19). The UCL-BSI survey similarly indicated that standards were used to ensure safety and security across the supply chain (16 respondents), provide quality assurance (15 respondents) and to design and manufacture a good technical product (20 respondents).

The UCL-BSI survey also reflected the role of standards in improving an organisation's understanding of requirements regarding regulatory matters (14 respondents) and healthcare sector access (5 respondents). In addition, standards could be viewed as a competitive advantage for market access and a steppingstone for international expansion (P17), by improving an organisation's ability to understand the global operating context through the definition of terminology and best practices (P13).

Nonetheless, there are several challenges which may hinder organisations from engaging with standards. In the UCL-BSI survey, respondents ranked regulatory, security and market access as the top three areas that were most challenging to identify and implement standards (see Figure 4).

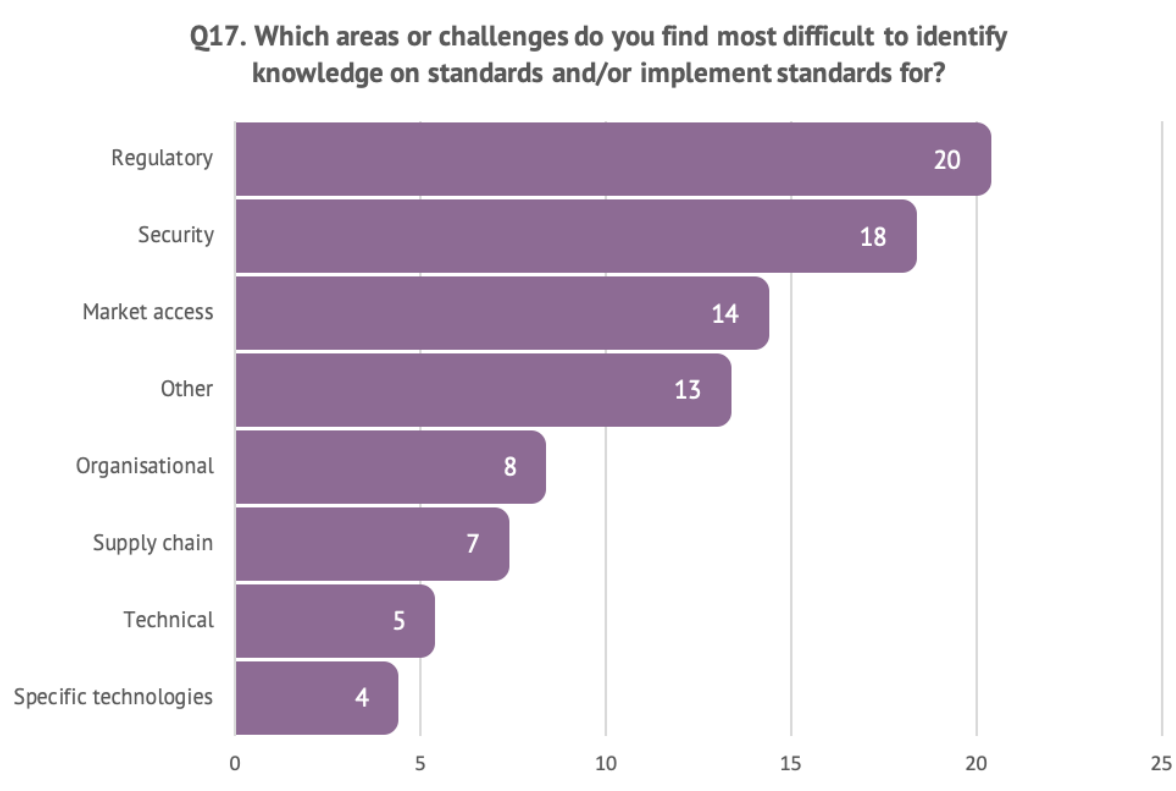


Figure 4: Challenging areas for identifying and implementing standards

This is partly due to the multitude of standards which may apply to different aspects of a single medical device (see Figure 3), that may be too complex or burdensome for organisations to navigate (P3, P5, P13, P14, P17). For instance, a manufacturer of a connected glucose meter will minimally have to consider process standards (ISO 13845 and ISO 14971), horizontal standards (ISO 16142 and BS EN 60601-1) and vertical standards (BS EN 15197 and BS EN 11073-10417). Furthermore, a lack of standardization on medical taxonomy and the use of jargons create barriers in understanding standards (P2, P7, P8, P11, P13). This is

further exacerbated by a lack of organisational capacity to engage with standards (P8, P15, P16), even for large companies (P8).

The benefits of using standards may not be apparent to some manufacturers (P3). Some perceive standards as the 'lowest common denominator' among manufacturers involved in the standards-setting process (P1, P18), being disproportionately tedious relative to the device's safety risks (P7) and being slow to keep up with technology (P13, P17). This indicates a standardization gap, which is further discussed in section 3.5.3 below.

3.2 Innovation

3.2.1. Adverse effect of regulations

There is an ongoing debate in the literature on whether regulations can stifle innovation. The primary research revealed several perspectives on this topic. As some respondents in the UCL-BSI survey and interviewees highlighted, strict and complicated regulatory frameworks are considered obstacles to innovation (P2, P9-11 P17, P19).

Especially, regulatory burdens remain among the biggest hurdles for SMEs with limited resources.[35] This has been echoed by an expert working with start-ups in the field, who would advise against newcomers with limited knowledge to enter the field because of these strict requirements (P9). This indicates that regulations are considered to create high market entry barriers. Regulations are also perceived as complex to understand, and it is common for employees in an organisation to lack awareness about device classification, especially in software teams and start-ups expanding at a fast pace (P15).

However, despite the hurdles that regulations bring, it is crucial to bear in mind that regulatory frameworks exist to protect patients. Rigorous requirements are therefore necessary to ensure the quality of devices. As one stakeholder noted, "the role of regulations is to maintain public safety and confidence in medical devices, while not acting as a barrier to innovation. This is a very delicate balance." (P14).

Impact of the MDR

The transition to the MDR is feared to threaten innovation, partly because of the increased regulatory burdens and limited Notified Body capacity (P7, P19). Compliance burdens may negatively affect newcomers and SMEs (P7, P8). Although enhanced post-market surveillance requirements under the MDR address safety challenges and capture technical areas such as software, they also impose further burdens on organisations.

However, early MDR adoption could be used as a competitive advantage for companies, as it could prove readiness, safety and facilitate access to multiple markets. Despite this, it is important to recognise its potential impact on innovation and smaller players. Large, well-resourced companies are more likely to be ready for the MDR transition (P8). When asked about one of the critical challenges for their organisation in the next three years, one UCL-BSI survey respondent noted: "Transition to MDR and that regulatory costs may delay market access". Moreover, the MDR could result in more acquisitions of smaller organisations that may struggle with the compliance burdens associated with product commercialisation (P8).

This trend could potentially limit competition in the market and thus, limit innovation as it could mean that SMEs may be squeezed from the market (P8). As smaller players and entrepreneurs have historically played a crucial role in developing new, innovative products, the framework must continue to allow these small players to operate.[35]

Standards

Regulators and industry stakeholders generally held positive views on the role of standards in supporting innovation (P9-P11). The purpose of standards is to help manufacturers understand regulatory requirements, design safe medical devices based on best practices, and generate evidence to demonstrate the presumption of conformity with the applicable regulations (P7, P8, P10, P14, P19). At the same time, several industry stakeholders recognised the difficulty in understanding and interpreting standards (P6, P11, P13-P15). Moreover, standards can be difficult to use because of their inaccessible nature and it was pointed out that they should be formatted in a more collaborative, digital way, in line with how companies operate today (P9, P11).

Some interviewees recommended using standards as early as possible in the company's lifecycle (P11, P15), especially for newcomers with limited knowledge. This was considered necessary to avoid scenarios in which adjustments are required after product development, due to non-compliance of the initial product with the regulatory requirements (P15).

In summary, primary research reveals a more negative sentiment towards regulations because of the complexity and the burdens they impose. On the other hand, standards are seen as helpful, although at times difficult to interpret, in the innovation journey to meet these complex demands.

Key drivers for innovation

There are numerous factors driving innovation in the field of connected, intelligent devices.

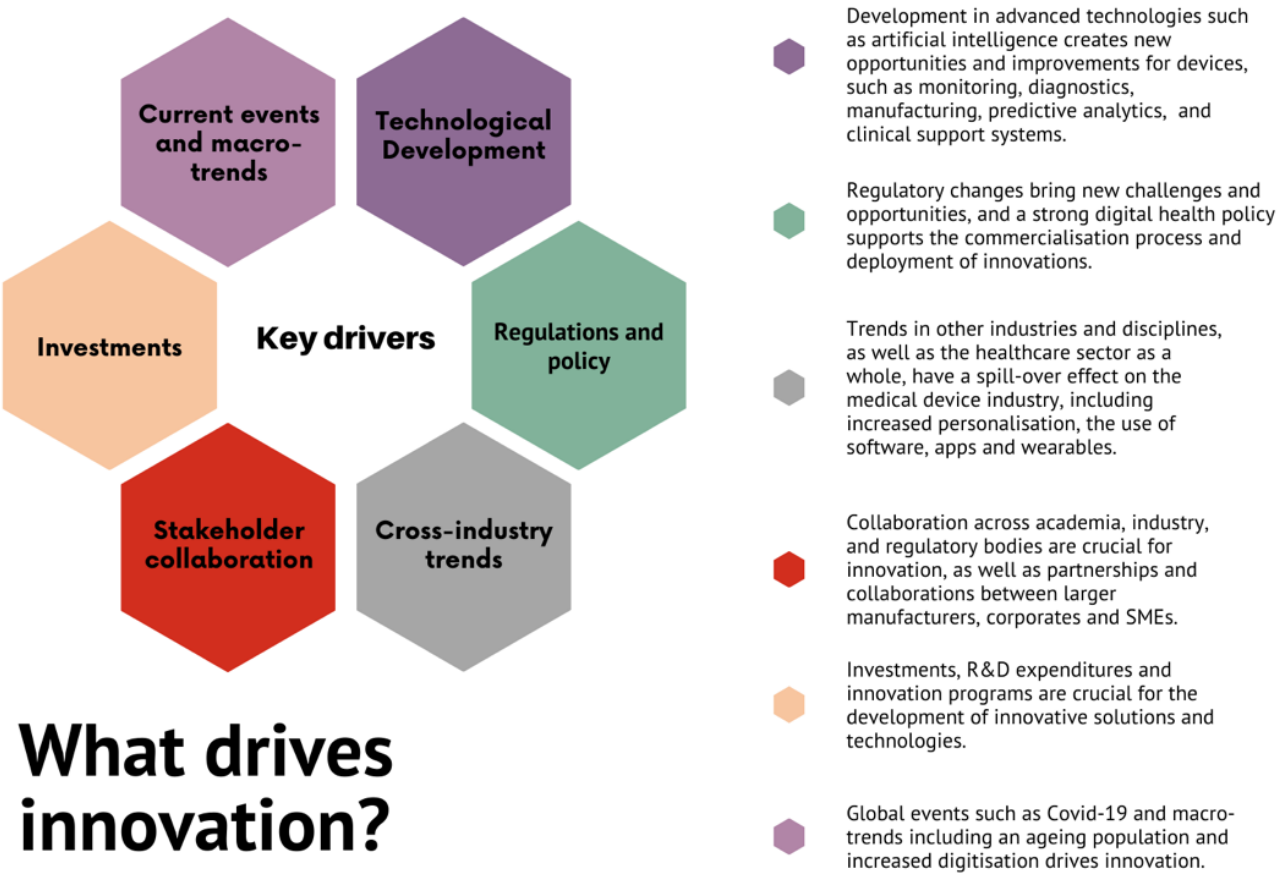


Figure 5: Key innovation drivers

Figure 5 above represents the key innovation drivers identified throughout the research, including technological development, investments, regulatory changes, cross-industry trends, collaboration across academia and industry, macro-economic factors, and current events.

3.2.2. Key challenges to innovation

Correspondingly, there are several barriers to innovation, ranging from regulatory challenges to hiring the right expertise, organisational boundaries, and commercialisation issues. Understanding and addressing these challenges is necessary, to ensure that the potential of digital technologies is used to benefit patients and the healthcare system.

Regulatory challenges

From the innovation perspective, high barriers to entry and regulatory frameworks with costly processes are commonly seen as significant threats to scalability. The UCL-BSI survey reveals concerns that there will be challenges to market access due to the transition to the MDR and the Notified Body capacity bottleneck (2 respondents). The limited Notified Body capacity was also highlighted in several interviews (P7, P19).

The UCL-BSI survey conveys that medical devices manufacturers deploy a broad range of innovative technologies, including AI (30 respondents), advanced digital imaging (21 respondents), robotics (16 respondents) and internet of things (15 respondents) (see Figure 6 below). At the same time, it is striking that most respondents considered the regulatory challenges related to technologies they deploy as the main regulatory challenge (27 respondents). This suggests that regulatory frameworks may be a barrier to innovation and deployment of these technologies.

This underlines the importance of overcoming these barriers to innovation, for instance by providing manufacturers with guidance. For instance, a respondent in the UCL-BSI survey noted that regarding AI, it is crucial to establish best practices around data sharing, validation, responsibility and transparency. For AI-algorithms, the more advanced the algorithms are, the more difficult it is to interpret and understand the outputs. In highly regulated industries with strict requirements to ensure safety, such as the medical device industry, interpretability is necessary, but it is currently a grey area due to complexity of the algorithms (P4).

Expertise

The multidisciplinary nature of the medical device industry requires expertise from a wide range of backgrounds. As reflected in the UCL-BSI survey, identifying the right expertise is seen as a tough challenge (19 respondents), with some respondents reporting difficulties in finding and affording regulatory expertise. While there is an ever-increasing demand for advanced technologies in healthcare, there are not enough experts who can holistically assess how these technologies fit into the healthcare industry and thoroughly understand the complexity around the algorithms (P4).

Commercialisation and organisational challenges

As highlighted in the UCL-BSI survey, delivering solutions to hospitals is difficult as organisations can struggle with procurement rules (2 respondents). Additionally, it is particularly hard for SMEs to consider the adoption framework and piece price so early in the company's cycle (P8). Linked to the commercialisation process are also other organisational challenges, such as capital requirements[36] and ensuring that internal teams are aware of rules around the products they build (P15, P16). In addition, internationalisation is also a key

challenge for organisations, as reflected in the UCL-BSI survey (13 respondents). In this context, the value of standards in facilitating market access to various regulatory jurisdictions was highlighted (P17).

3.2.3. Emerging trends

The medical device industry is characterised by heterogeneity and a wide range of products and services,[37] which are also reflected in the emerging trends. These trends include the use of advanced technologies such as AI, new solutions, more personalised care and new forms of collaboration across disciplines.

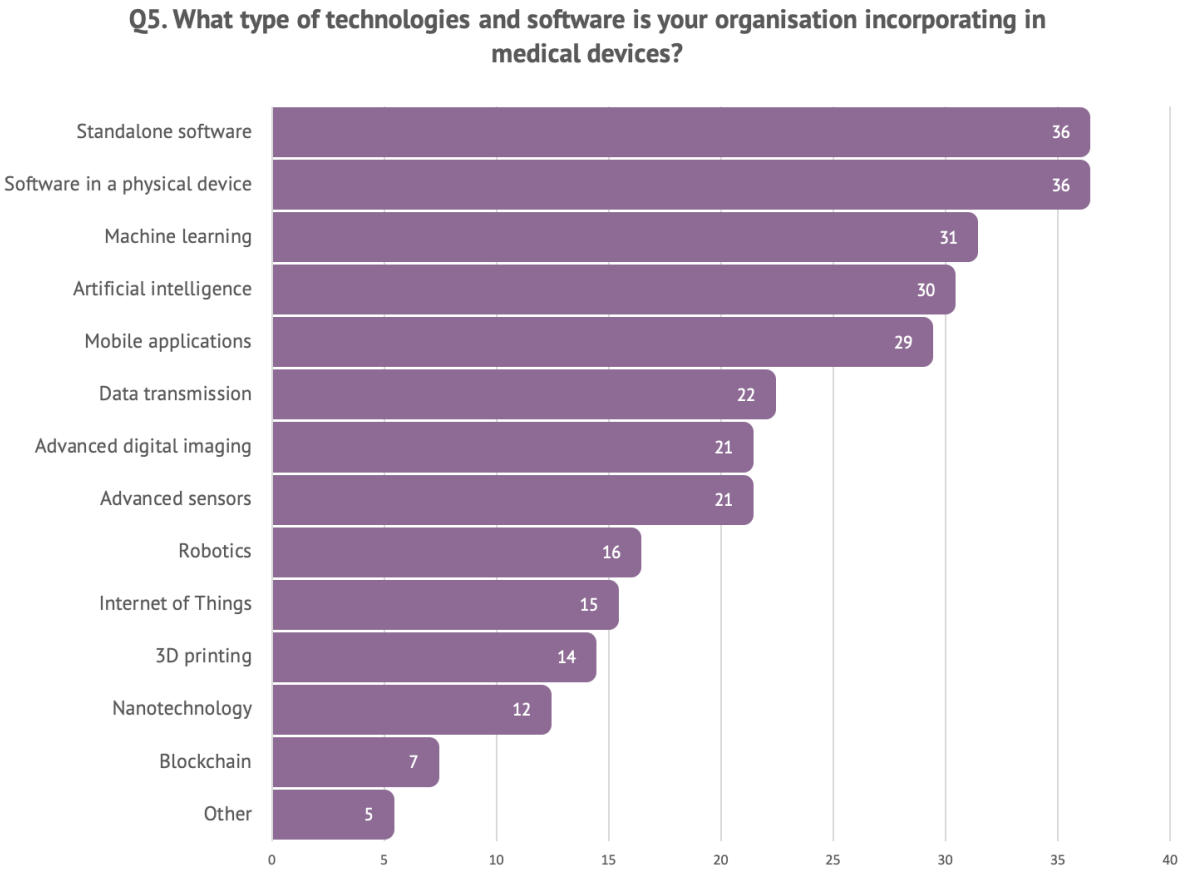


Figure 6: Technologies incorporated in medical devices by UCL-BSI survey participants

Advanced technologies

Figure 6 reflects the wide range of technologies incorporated in medical, including AI, robotics, digital imaging, internet of things, and 3D printing. These technologies will continue to drive change in the sector and bring new, innovative products to market, as well as add capabilities to existing devices. AI was seen by stakeholders as the dominant technology in the coming years (P1, P4, P8-P10, P16-P19). Technological development has

fuelled new trends such as predictive analytics, diagnostics, monitoring solutions, and connected wearables. AI also comes with safety risks, ranging from opaque decision-making processes to uncertainties in classification and regulations (P7, P19). Nevertheless, stakeholders remain positive about the value and potential AI could bring to the medical device industry (P1, P4, P8-P10).

The UCL-BSI survey revealed that diverse products are being developed. Respondents were mainly developing smart medical monitoring tools (31 respondents), wearables (30 respondents) and implanted medical devices (17 respondents). Others included clinical support systems, ultrasound, electromechanical diagnostic and therapy devices (e.g. imaging system and PAP machines), drug delivery, non-wearable medical devices (pacemaker), Integrated Care Clinical Information systems, mental health solutions, digital consultations, cardio-respiratory diagnostic/monitoring devices, and digital therapeutics. In essence, the field is highly diverse in terms of devices, uses, and approaches.

Blurring boundaries between disciplines and uses

The lines between digital health, consumer products and clinical use of devices are getting increasingly blurred. This includes, for instance, the lines between wellness and medical devices, as these are often not clear (P18), and classification for software versus hardware (P13). Further, end-users might interact with a device in a way which was not intended by the manufacturer (P15). As sensors grow more advanced and accurate, and the use cases develop, unregulated wellness devices may be used by patients to make health-related decisions, such as whether to consult a clinician or not.[6] When it comes to more advanced technologies such as AI, a stakeholder noted that devices will initially be incorporated in the existing processes in the healthcare system, rather than replacing functions entirely (P9). This reflects that AI is still at the early stage when it comes to wide scale market adoption, and shows the wide range of areas these technologies can be incorporated in.

Personalised care

In recent years, patients have been gradually more engaged in treatment, decision-making and monitoring.[38] The growing popularity of personalised care can shift some burden from healthcare professionals to patients, by moving some tasks from the hospital to the home, for instance through monitoring. This will also result in more proactive management of health (P13). Indeed, monitoring, remote care and wearables were seen as key trends by some interviewees (P3, P6). Moreover, the growing popularity of apps, connected devices and wearables affects how consumers, patients, and clinical practitioners engage with medical devices. This creates new safety and security challenges (see section 3.4.2 for further details).

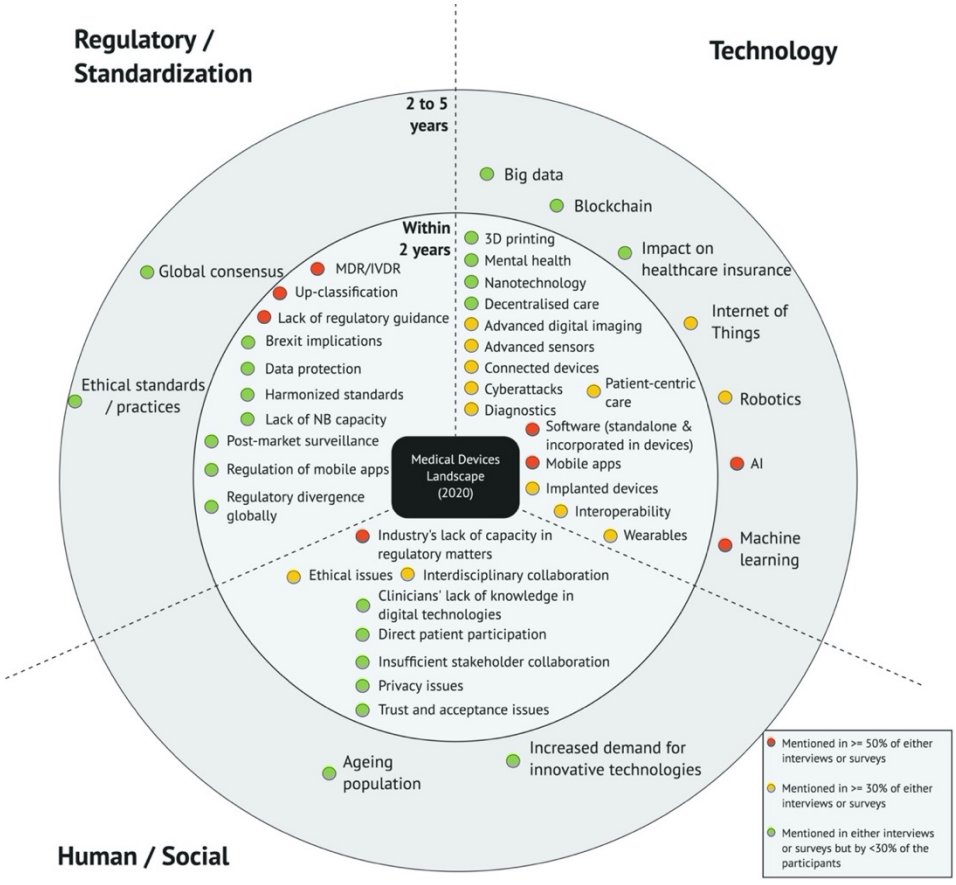
A wider ecosystem

The medical industry relies on collaboration on the broader healthcare ecosystem. Most recently, COVID-19 has demonstrated the importance of complete, multi-stakeholder collaboration and knowledge exchange, as noted by respondents in the UCL-BSI survey. Moreover, COVID-19 also shown that collaboration is crucial for accelerated development and market access for medical technology products in urgent times. For instance, innovation networks were involved in the response to COVID-19 in Scotland and helped develop the track and trace system (P1). As noted in the horizon scan, stakeholder collaboration between regulators, academia, large technology and medical device firms, entrepreneurs, and innovation programs will enable the creation of new solutions in the medical device industry.[39] This will likely result in further cooperation as smaller companies can tap into larger market players' resources.

Drivers of change

To conclude the discussion of main trends, Figure 7 below provides an overview of the drivers of change in the medical devices industry within the next five years, based on the horizon scanning exercise, interviews and surveys.

Figure 7: Drivers of change



3.3 Product lifecycle

There has been a growing interest in the lifecycle of connected, intelligent devices, as it has been recognised that there are specific considerations that must be addressed at each step to manage risks. Manufacturers of devices embedding connectivity and intelligence should consider three main lifecycles.

Medical device lifecycle

Medical devices follow a very set lifecycle structure. However, there appears to be no consensus on what the specific stages are among stakeholders (P5, P11, P17). One of the possible classifications, identifies seven main phases.[40]

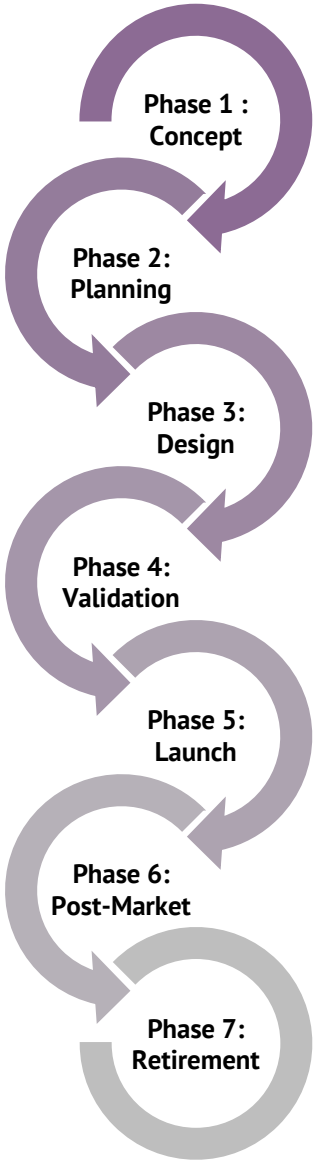


Figure 8: Product lifecycle

Phase 1: Concept

The concept phase focuses on an initial evaluation of a possible commercial product. It is crucial to consider the products' intended use and definition initial risk analysis, intellectual property considerations, product classification, commercial plan, potential markets and entry routes, and resource requirements. This stage is also referred to as the ideation or early stage.

Phase 2: Planning

In the planning phase, manufacturers define the design input based on user needs and technical requirements. The main tasks at this stage include concept development, prototype analysis, initial testing, initial design file and risk analysis, and formulating commercial strategy, quality management system, regulatory strategy, data protection and project plans. This stage is also referred to as early development.

Phase 3: Design

The design phase concentrates on the development of product design and manufacturing process, verification and validation. In this phase, manufacturers should focus on user feedback, manufacturing process, design verification and validation, technical documentation, regulatory strategy and requirements, product claims and branding, and risk management.

Phase 4: Validation

The validation phase focuses on the final validation of the manufacturing process and preparation for market entry. This includes a market plan, process validation, clinical validation, product claims, labelling, regulatory submission, product reimbursement, EU CE marking and other global certification. Importantly, the CE mark and other certifications are essential for market success and a component of procurement procedures for various healthcare institutions, including the NHS. This stage is also referred to as testing.

Phase 5: Launch

Following regulatory approval, the medical device can be launched into the market. Other tasks in this phase include sales, clinician training and individual country reimbursement approvals. This stage is also referred to as market entry.

Phase 6: Post-market

The post-market surveillance phase concentrates on traceability and efficient reporting of errors. Tasks in this stage include post-market clinical follow-up, complaints and adverse events, product and process improvements, external body audits, market performance assessment and entry into new markets.

Phase 7: Retirement

The retirement phase concerns the end-of-life of the product. Tasks include disposal procedures, data deletion, checking device functionality, incident reporting, evaluations and device recycling and reuse.

Software lifecycle

The software lifecycle covers all aspects from ideation to the de-installation or decommissioning of the product (see Figure 9).

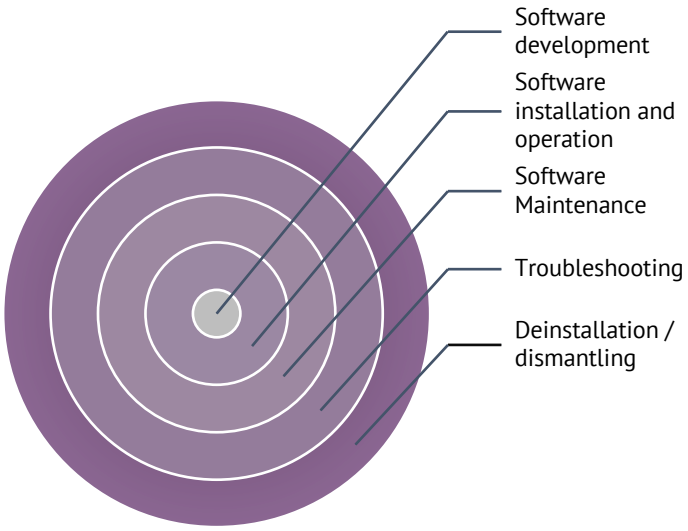


Figure 9: General Overview of Software Lifecycle Process[41]

Both the MDR and the MDD require software manufacturers to develop it "in accordance with state of the art". This has important implications for the device lifecycle. According to the MDR, manufacturers must take "into account the principles of development lifecycle, risk management, including information security, verification and validation".

The UCL-BSI survey indicates that IEC 62304 is often utilised to provide the presumption of conformity with these regulatory obligations (4 respondents). This standard provides requirements on medical device software lifecycle and development process. It should be noted that the development process depends on the device risk classification and typically involves activities noted in Figure 10.

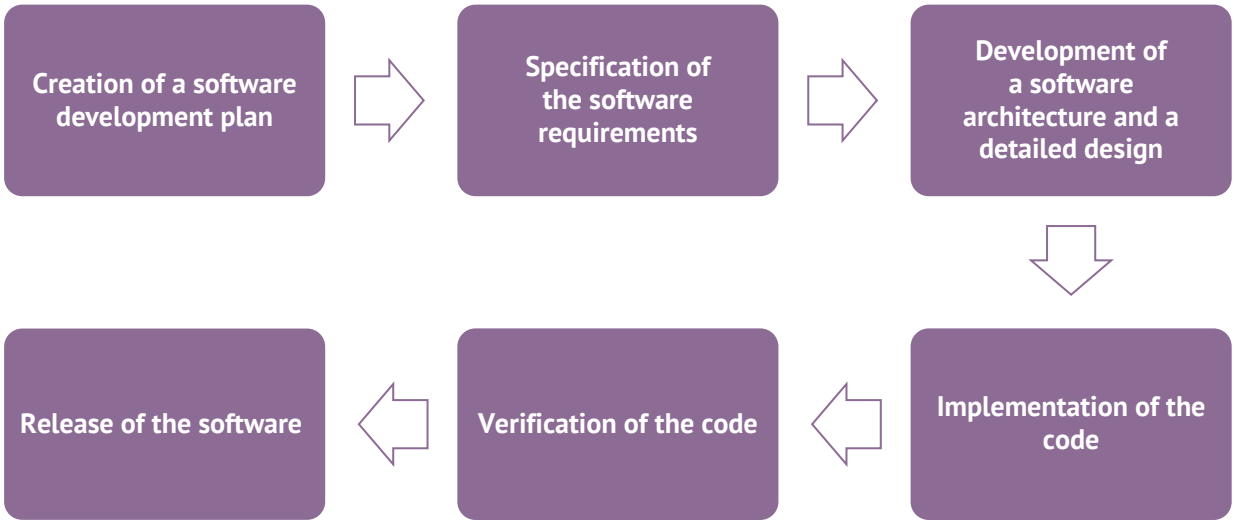


Figure 10: General overview of the software development process

Artificial intelligence lifecycle

The Artificial Intelligence Lifecycle is pertinent to AI-driven medical devices. According to the ICO, the AI lifecycle consists of seven stages (see Figure 11).[42] The ICO utilises this lifecycle process to highlight the stages where data protection risks could occur. It can also be used by manufacturers to assess where the controls might be most effective. Some stakeholders recognise this lifecycle as a necessary consideration for AI algorithms (P3). However, this lifecycle is not linked to any standards and is not specific to medical devices.

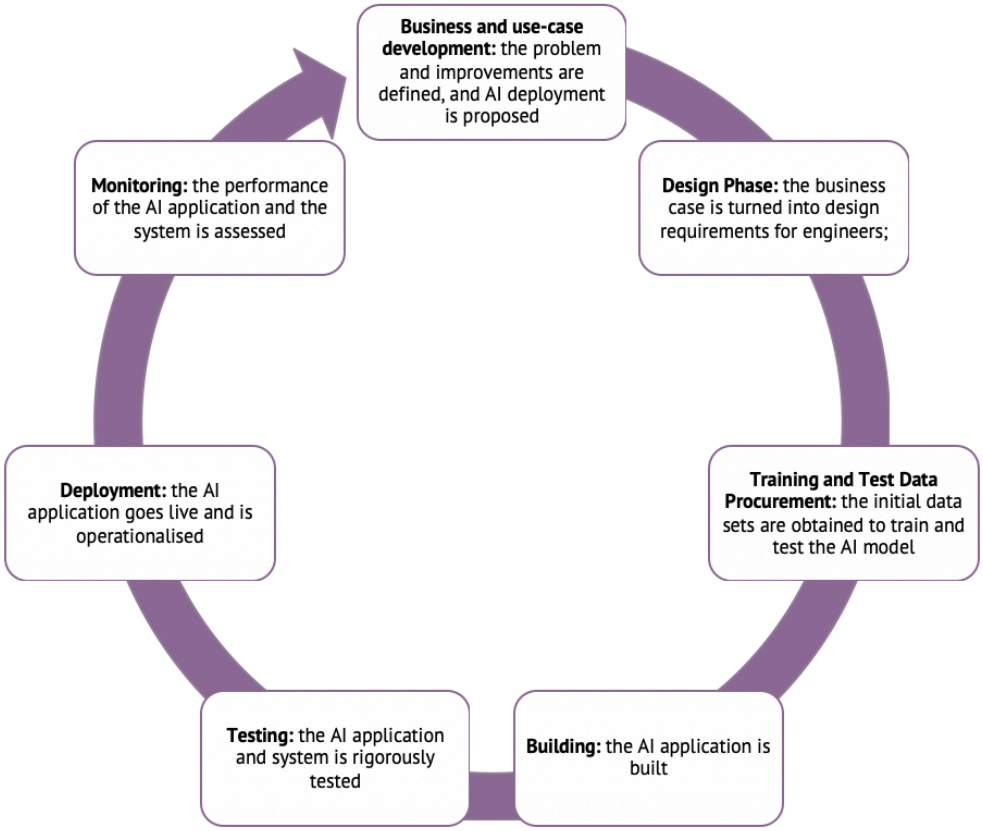


Figure 11: General Overview of Artificial Intelligence Lifecycle[42]

PART B: EMERGING CHALLENGES

3.4 Risks from emerging trends

Connectivity and intelligence are incorporated into medical devices to enhance healthcare quality, efficiency and safety.[43,44] These devices are cyber-physical devices, as cyber systems, such as software, interact with the physical environment and humans.[45] However, these interactions and the introduction of connectivity and intelligence raise novel security, safety and ethical challenges.[46]

3.4.1. Cybersecurity Challenges

Connectivity risk

Connectivity significantly increases device security risks, making devices vulnerable to a large range of malicious actors.[47,48] Wireless communication, such as via Bluetooth, allows connectivity between devices. This can provide an entry point for intruders within proximity to implement a hostile takeover (P8). This risk is even greater when the device is connected to the internet, allowing perpetrators from anywhere in the world to hack into a medical device (Figure 12). Concerningly, multiple studies underlined the low barriers to hacking connected medical devices.[49–52] Attacks can be carried out by less experienced perpetrators with off-the-shelf commercial products.[51]

There was a broad consensus among stakeholders that connectivity is the most considerable security challenge and the main cybersecurity risk (P2, P4, P8, P11, P13). In this context, the WannaCry ransomware attack in 2017 was considered “eye opening”, due to the impact on the NHS systems, which were locked out and could not deliver vital services to patients (P12).

Figure 12: Hacker interfering in medical device communications

Interoperability challenges

Another significant cybersecurity risk is the increasing need for medical device interoperability.[53] Effective and safe interoperability ensures seamless information exchange with other medical devices and the broader IT network.[54] It can provide many benefits for patient care. For instance, interoperability is necessary to support increased task automation, error and cost reduction as well as effective patient health-record maintenance, improved clinical decision support and patient safety.[44,54–56]

Nevertheless, as conveyed in the UCL-BSI survey, increasing interoperability creates challenges for ensuring the security, safety and performance of connected, intelligent medical devices (1 respondent). Indeed, the literature highlights that introducing greater interoperability increases the attack surface because it increases the interconnectedness within a system.[55] This means that device vulnerabilities offer entry points, not only to the device itself but also to the wider healthcare IT environment.[57] Several interviewees noted that such gateways allow hackers to compromise, or even take down, the entire healthcare network, together with devices and systems connected to it (P4, P6, P11, P13). Clearly, security is a key requirement for interoperable medical devices, particularly in life-critical settings and when dealing with sensitive data.[55]

However, secure interoperability is difficult to achieve, given the possible vulnerabilities (P17). For instance, if an attacker forces a component in the environment of an interoperable medical device to deviate from its original functionality, the system environment can no longer be considered safe.[55] It can cause a domino effect with severe implications for other interoperable devices in that system and may corrupt data (P6).

Additionally, interoperability of connected, intelligent medical devices could bring about greater risks of data breach.[58] Interoperable medical devices are designed to continually collect and disseminate data wirelessly, often in real-time. The advantage is that patients and clinicians can easily access the data, but it also creates vulnerabilities in maintaining data security and confidentiality (P4, P6, P13, P14, P16, P19). These vulnerabilities could lead to privacy breaches, identity theft, financial theft and possible psychological harm to patients.[59] According to industry research, the healthcare sector experienced the largest healthcare cost in 2019 with $7.13 million.[60]

Intelligent medical devices

It also emerges that the introduction of intelligence to medical devices can amplify these cybersecurity vulnerabilities.[61] For instance, if hackers obtain access to and change data sets that AI depends upon, the algorithm will reinforce these modifications. However, an intelligent medical device relies on correct data for its efficacy. Thus, an AI algorithm would potentially derive a faulty conclusion and provide incorrect information to users.

This could have fatal consequences for a patient. If an AI-powered insulin pump derives an excessive blood sugar level from the alteration, the resulting overdoses may kill a patient.[52]

Physical vulnerabilities

The security of connected, intelligent devices is also affected by physical vulnerabilities. As one interviewee pointed out, the largest security risk to protecting a medical device physically is poor cyber hygiene of the users (P1). Cyber hygiene refers to the routine steps and best practices that users take to protect devices and maintain system security.[59] For instance, poor cyber hygiene would include basic passwords that are written on a sticky note hanging from a monitor. Stakeholders in the field suggested that good cyber hygiene from users and manufacturers is necessary to increase the security of connected, intelligent medical devices (P1, P11).

Moreover, devices face further security risks if they have physical sensors (P9).[62,63] For instance, these sensors could collect data on temperature, blood pressure and light exposure. Depending on the tolerance and resilience of the medical device, the sensors could be intentionally or unintentionally interfered with, for instance, by increasing the temperature. This may distort the data and, as a result, affect device accuracy and safety particularly for intelligent devices.

However, besides external hackers, intelligent devices could be influenced and hacked by users. For instance, biohacking is a trend on the rise and occurs pre-dominantly in the US (P3). Under one scenario, non-technical users may accidentally hack themselves (P6). For instance, by playing around with the device software, they could influence data sets, alter the algorithm or a vital functionality, raising risks to their safety. Another scenario occurs where patients with IT experience hack into their device to identify vulnerabilities that can be exploited in other devices.

Security by design

Despite the severe consequences that cybersecurity vulnerabilities and breaches may have, the horizon scan indicated a false sense of security among stakeholders.[44,64–66] There appears to be a discrepancy between their perception of being secure and having the necessary security measures in place. For instance, industry research indicates that 96% of healthcare provider executives believe their practices are protected against cybersecurity risks. However, only 34% have a cybersecurity audit and 36% an access management policy in place.[66]

This false perception of security introduces severe security-safety risks and may be expensive. In the UCL-BSI survey, an SME noted that it was problematic that they only investigated cybersecurity issues and the GDPR requirements quite late in the lifecycle and

had to seek expensive consultancy advice. As this respondent noted, they will aim to consider these issues earlier in the lifecycle in future. Numerous interviewees emphasised the importance of this approach, which is called security by design (P2, P6, P8, P9, P11, P13). Here, security is considered from the beginning and throughout the medical device lifecycle.[67]

Standards emerged as the core tool to address this disconnect and to ensure security by design. The UCL-BSI survey revealed that standards were the most common method to ensure safety and security across the supply chain (16 respondents). Some standards were mentioned specifically by respondents, including the application of risk management to medical devices standard, ISO 14971 (3 respondents) and the information security management standard, ISO 27001 (2 respondents).

Challenges in using security standards

Although standards are a popular method of ensuring security, the UCL-BSI survey indicates that security standards may be challenging to use. Besides regulatory standards (20 respondents), security standards are the most difficult to understand and implement (18 respondents) (Figure 4). This indicates challenges that may hinder the engagement with security standards. The following main challenges were identified.

Firstly, as already noted in the standards section (see section 3.1.4), stakeholders highlight that standards can be difficult to understand, especially for SMEs (P2, P6-P8, P11, P13-P15). More understandable, accessible and interactive formats of standards should enhance stakeholders' comprehension.

Secondly, there are difficulties in implementing security standards. Even if security requirements in standards are understood in theory, they may be much harder to apply in practice (P6). The cybersecurity of medical devices is a technical field that requires expertise and funding to implement standards. Therefore, due to a lack of organisational capacity, SMEs may find it particularly hard to follow the guidelines and implement standards (P8, P15, P16). Case studies. implementation examples and guidance should aid the practical implementation of standards. An example of this is the 2020 revision of the ISO/TR 24971 standard. It aims to aid manufacturers in meeting the requirements for and applying ISO 14791.[33] This includes guidance on the development, implementation and maintenance of risk management processes for medical devices across the lifecycle.

Thirdly, the multitude of security standards that may apply to different aspects of a medical device may be challenging. The non-centralised and fragmented nature of standards may be too complex and burdensome for organisations to navigate (P3, P5, P13, P14, P17). Therefore,

the number of various security standards may make priority identification and a clear overview of security standards difficult for stakeholders.

However, the IMDRF and MCGM cybersecurity guidance papers, published in 2020, aim to reduce this problem.[67,68] They offer key principles and practices to ensure the cybersecurity of medical devices, pre-market and post-market considerations and a brief overview of the standards landscape.

Cybersecurity and patient safety

Cybersecurity vulnerabilities can have severe consequences for patient safety, digitally and physically. On the digital end, privacy and data security are critical aspects. Patient data sets are valuable since there is a significant demand for them, such as for AI/ML training purposes (P14). Therefore, there is a financial incentive to hack and extract data.

However, this has created security challenges for stakeholders, with data security being most pressing (P4, P6, P13, P14, P16, P19). According to the UCL-BSI Survey, user data and data security (17 respondents) are important challenges to ensuring the safety, security and performance of devices. This is followed by technical challenges of infrastructure and software (11 respondents) and supply chain security vulnerabilities (4 respondents) (Figure 13).

Figure 13. Organisational restrictions and challenges for ensuring safety, security and performance of connected, intelligent medical devices

Importantly, security risks may translate into risks for patient safety. This is particularly the case for Class III devices, representing the highest risk class, such as implantable medical devices. The literature and an interviewee pointed out that connected pacemakers can be hacked, code be altered and a cash ransom be requested to restore its live-saving defibrillation functionality (P13).[49,51] In the worst case, stakeholders mentioned the scenario that commands by hackers could initiate electric shocks with potentially fatal consequences (P5, P13). Therefore, security is essential to ensuring the safety of patients.

Overall, it emerges that security and safety are strongly interlinked. One interviewee pointed out that both security and safety should be seen together because one cannot be fully understood without the other (P6). However, while cybersecurity is vital to ensure patient safety, safety should not be solely reduced to ensuring device security. As one interviewee remarked: "Recent prominent security incidents have pushed safety to the backstage" (P11). This points towards a conflation between security and safety. While it is important to understand how security and safety converge, the safety considerations that go beyond security should be recognised. There are additional factors to patient safety beyond security.

3.4.2. Safety Challenges

Interpretability

The outputs of AI may be hard to understand and interpret.[69] This applies particularly to complex algorithms, which may function as black boxes. Opaque and unintelligible outputs complicate human interpretations of individual predictions.[70] In addition, there is a significant skills gap in the healthcare sector, as clinical end-users lack the expertise and skills required to understand AI outputs. This prevents them from retrospectively understanding an action or decision that caused harm, what went wrong and why. Equally, it might prove challenging to understand the system, making it impossible for clinical end-users to anticipate, mitigate and prevent harmful actions or decisions in the future. As a result, they may be unable to report errors arising from these devices, which can jeopardise patient safety.

To address this, a stakeholder emphasised the importance of developing a new medical curriculum, that can adapt to the digitisation of healthcare and equip healthcare professionals with the required digital skills (P1).

Usability

Another safety theme emerging from the literature is usability. As medical devices become increasingly patient-centric, the need to account for the ease of use is crucial to the adoption and scalability of these devices in the healthcare sector. Equally, it is essential to prevent safety risks, as users may interact with the device in ways that were unintended by the manufacturer.[69,71] Stakeholders emphasised that usability testing and accounting for end-users throughout the lifecycle is crucial to ensure safety and prepare for possible safety risks arising out of user interactions with the device interface (P12).

Yet, there appears to be a disconnect between the manufacturers' and the end-user's perception of usability. Some interviewees noted that manufacturers tend to have their own opinion on the devices' design, but this may not necessarily align or sufficiently account for the ways in which users may use the device (P6, P14).

This results in a mismatch between the manufactures' technical requirements and the user's usability requirements (P12). For example, medical devices are often used in very intensive environments, with stress and emergency situations being the norm (P6). In these stressful conditions, clinical end-users often do not comply with the technical requirements and their ability to understand what is being communicated on a device interface is diminished (P6).[69,72,73] The inability of users to appropriately use these devices in varied contexts and environments suggest that the interface may not be user-friendly. To address these safety concerns, it is pertinent that manufacturers consider the cyber-physical nature of these devices as being a crucial design consideration in the medical device and software lifecycle.

There was a broad consensus amongst the UCL-BSI survey respondents that standards play a key role in meeting usability requirements. Popular standards used to address device design, with a focus on usability and consideration for other human factors, include ISO 62366 on the application of usability engineering to medical devices, ISO 13485 on medical devices quality management systems, and ISO 14971 on the application of risk management to medical devices.

Integration

The deployment of AI-driven devices within healthcare could enhance patient safety and care.[74] However, integrating intelligent devices into the healthcare environment requires hospitals to have the necessary infrastructure in place, including an interoperable data infrastructure and adequate training for hospital end-users.[75,76] In the absence of crucial infrastructures, the deployment of intelligent devices in the healthcare sector, has the potential to introduce new and different safety risks.

In addition, there is a lack of transparency regarding the capabilities, functionality and limitations of AI-driven devices. Hence, from the onset, it is imperative that manufacturers are transparent about the cost, infrastructure and human labour needed to sustain these devices. Addressing these considerations is crucial to mitigate the integration challenges that may arise from the deployment and use of these applications. Moreover, they would enable clinical end-users to account for the limitations of these devices for diagnosis and supporting clinical decisions.

3.4.3. AI Ethics and Patient Safety

The adoption of AI-driven medical devices creates critical ethical issues with significant implications for patient safety. Addressing these issues in both pre-market and post-market stages is critical for the scalability and deployment of AI-driven devices.

Trust

AI-driven medical devices can have a significant impact on transforming trust relationships. Most importantly, these devices could transform the therapeutic relationship between a patient and clinician (P3). Across the globe, this relationship is rooted in trust, with the clinician held in high esteem. If clinicians are to rely more on AI to inform decisions, algorithms need to be explainable and easily understandable.

Ethically, the issue of trust has cascading effects on the ability of clinicians to obtain a patient's informed consent to the use of AI for clinical decisions.[77,78] Presently, ambiguities remain as to how the "right to explanation" of decisions made by intelligent medical devices

can be applied in a way that maintains patient's confidence.[79] This challenge has been depicted as the inability of patients to know who to trust; the device or the clinician (P1, P7, P9, P14, P17). As it has been suggested in recent research, building trust in AI and other intelligent, autonomous systems requires more focus on ethical governance.[77] Moreover, several interviewees stressed the need to develop these devices with the patient in mind, which involves ensuring trust (P3, P4, P5, P9, P11, P14, P17).

Algorithmic Bias

AI is prone to algorithmic bias, as the trustworthiness and effectiveness of human-trained algorithms largely depend on the composition of the training dataset.[80–82] However, the data may include biases, for instance as a result of the limited dataset, human bias in data labelling and the use of retrospective datasets. This may negatively affect marginalised groups. For instance, it is well-documented in the literature that a training dataset skewed towards a certain race, might make a device better at diagnosing health issues for certain groups compared to individuals of other races [81,83] This may lead to an inaccurate diagnosis, rendering the suggested treatment ineffective for a particular demographic group and compromising their safety.[82]

While the issue of bias is not an ethical concern specific to AI applications, the encoding of bias in AI-driven medical devices and software raises the stakes. The increasing automation of certain elements of clinical decision-making give rise to critical safety risks given that clinical end-users may perceive such outputs as objective, evidence-based and neutral.[78,81] Such over-reliance on algorithmic objectivity and neutrality risks encoding and re-enforcing these biases, which in turn exacerbates their effects on marginalised populations.

There is a broad consensus that some of these biases may be resolved through data access and availability.[56,70,81,84,85] This would ensure that manufacturers of AI applications can gather data that is inclusive of varied demographics and that accounts for varied characteristics during the pre-market stages of the device's lifecycle. As illuminated in other industry contexts where AI is increasingly being used, manufacturers and designers will typically resist disclosure of their AI training process.

In the absence of regulatory oversight of AI, a stakeholder noted that developers of AI-based medical devices and software typically refrain from applying for patents (P4). This is largely due to their reluctance to disclose their code upon receipt of the patent, and the self-learning functionality of these devices which renders the patented elements irrelevant (P4). As a result, manufacturers prefer to maintain the AI black box and keep the code in-house, which contributes to the complexity of AI governance (P4).

Transparency

AI introduces an issue of transparency, giving rise to novel safety and ethical risks. As intelligent medical devices are highly dependent on data, individuals are encouraged to share more personal data. However, this also creates the risk of data being used in non-transparent manner, for instance to influence decisions about the eligibility for insurance premiums, financial loans, or job opportunities.[78,86,87] Here, it is critical to restrict the use of patient data for clinical use – in Europe, the GDPR introduced important safeguards in this area.

Transparency issues have a significant impact on the perception of AI. An example of this, was the use of AI algorithms to provide cancer treatment options for several patients. However, the algorithm was criticised for giving unsafe and incorrect recommendations for cancer treatments.[88] It was found that the software was trained with a few synthetics' cancer cases.[86,88] While the errors were identified at the testing stage, the lack of transparency surrounding the model limitations and discrepancies put the industry in a negative light. In a healthcare context, transparency fosters trust among end-users, including patients and clinicians, which is key to the increased adoption and use of AI applications in the healthcare sector. This viewpoint was echoed in the UCL-BSI survey, with some respondents noting the importance of receiving clinician's interest and backing of their medical device products (2 respondents).

Traceability

Traceability is another critical ethical issue that arises from the deployment and use of AI medical devices. Ethically, AI traceability involves the identification of harm caused by algorithmic activities and the attribution of responsibility for it.[78,89] Deployment of intelligent medical devices makes the allocation of responsibilities extremely challenging.

This is due to the fragmented and opaque nature of the AI ecosystem, resulting from the need for multidisciplinary expertise to develop and maintain AI-based medical devices and software. As such, a standalone AI-driven medical device might involve many actors in its supply chain working and maintaining different components of the device.[78,87] This makes the allocation of responsibilities near impossible. In addition, the black box nature of AI adds to the complexity of AI traceability. This is because the inability of humans to explain how an algorithm came to a decision makes it difficult to identify and mitigate harm.[78,79,90]

Consequently, questions about how liability should be determined among the many actors who develop, use and maintain these AI-driven devices and software remain unanswered. In this context, the literature review highlights the potential of a systems-wide approach to address AI traceability challenges.[76] To this end, it is essential for stakeholders to work collaboratively to ensure that the risks arising from the technical, systemic and societal layers

of these devices are properly mapped out. This allows appropriate measures to be taken to build resilience, enable effective incident reporting and ultimately prevent harm to the end-users of these devices. Nevertheless, questions pertaining to where liability lies when using a systems-wide approach remain unresolved.[87]

3.4.4. Negative interactions

The MDR / IVDR introduced an explicit requirement in Annex I for manufacturers to consider the possible negative interactions between software and the IT environment within which it operates. However, so far, limited guidance has been provided on this requirement by public bodies.[67,91] The literature review and the horizon scan indicate that the key negative interactions between software-driven medical devices and their IT environment reflect a convergence between safety and cybersecurity challenges. This convergence reflects the need for manufacturers to consider both human factors and the cyber-physical systems in which these devices operate.

Despite limited guidance on this requirement, the literature review, regulatory documents and the horizon scan indicate that the main negative interactions arise from user interactions, device-information source interactions and software-hardware interactions (Figure 14).

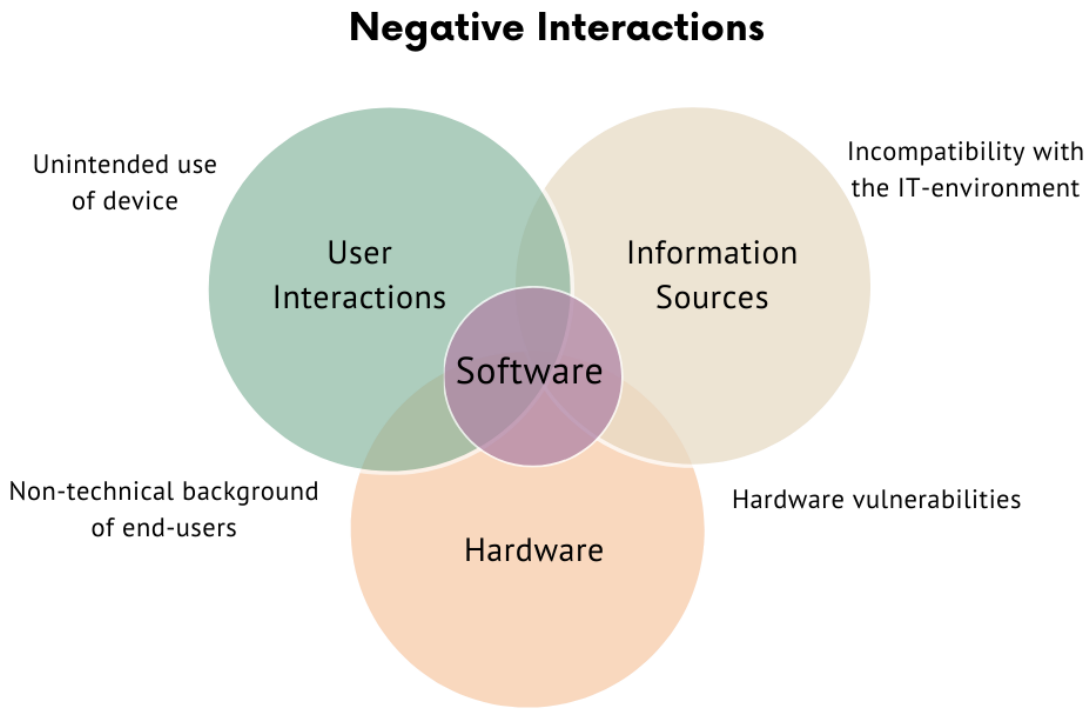


Figure 14: Key negative interactions between software and IT environment

User interactions

These negative interactions can arise from the non-technical background of end-users, such as doctors, nurses, administrators and patients.[92–94] End-users may use the device in an unexpected manner, even though manufacturers are expected to account for various ways in which users might interact with their product. In this context, if a device is used for purposes it was never designed for, this could potentially erode safety mechanisms built into it.

In effect, end-users do not always have a clear understanding of how to operate and use complex devices safely (P12, P16). In addition, negative user interactions can be attributed to the suitability of the design and the fact that the design and use are poorly adapted. One UCL-BSI survey respondent noted that manufacturers would need to describe very carefully and accurately the conditions necessary for the safe deployment of their product in its end-user IT environment. This would help ensure that the device is used as intended.

Information source interactions

Negative interactions between software-driven devices and information sources arise from the connected and networked nature of these devices. IT systems in healthcare deviate from the isolated clinical setting in which devices are clinically tested and validated.[95,96] New safety risks emerge when a device interacts with different elements of the networked healthcare environment, in which a device was never tested before going live (P3).

Interactions may also occur at the system and network level, via implementation of software into the broader IT environment.[67,97] Importantly, while device and system interoperability is a broader concern, highly relevant to cybersecurity, these negative interactions are specific to incompatibility with the end-use IT environment (P3). Given the large number of providers involved in different parts of the system (P3), and the large number of various software and information source interactions, it is difficult to keep an overview of the system.

Thus, for manufacturers, on the one hand, safety consists of ensuring the proper functioning of the device and preventing random and inadvertent safety risks. In this context, the need for manufacturers to conduct extensive usability testing with beta customers and to use an iterative engineering design process from the outset was underlined by a UCL-BSI survey respondent. On the other hand, cybersecurity considerations reflect the need for manufacturers to account for the potential risks associated with the device's interactions with various networks and systems in the end-use environment and the security vulnerabilities that can arise when these incompatibilities are not adequately addressed.

Software and hardware interactions

Negative interactions with hardware can arise from a possible disconnect of the devices' software-hardware interface.[75,93,98] This disconnect can be as minor as an incompatible power

cord to the impact of hardware damage on the software's functionality. This interaction is linked to the depiction of medical devices in the literature as being cyber-physical systems with safety-critical functions where considerations must be given to how each component of the device interacts or alters the function of another component.[56,99]

3.5. Regulations, standards and policy challenges

This section outlines the main challenges arising with respect to regulations, standards and policy.

3.5.1. Global consensus standards

However, several interviewees highlighted the practical challenges surrounding achieving consensus globally (P7, P13, P17). The tension between the benefits and challenges of regional consensus standards was also evident in the horizon scanning exercise. On one hand, European harmonized standards are used to provide the presumption of conformity to the relevant European Union legislation.[28] On the other hand, the horizon scan also suggested that stakeholders found the European harmonization process to be slow and tedious. This could lead to European harmonized standards being outdated when the process is completed in the context of rapidly evolving technologies.[100] These challenges were also encountered when China tried to achieve consensus and support the convergence of standards across different provinces.[29] These regional and national challenges serve to illustrate the possible challenges faced in the development of global consensus standards.

Nevertheless, global consensus standards could bring about improvements in patient safety and a nuanced approach could be taken. This was highlighted by one interviewee (P16) who suggested that consensus and cooperation between international public agencies and private stakeholders could begin with an agreement on defining the terminology for emerging technologies such as AI. In the long run, this could facilitate a better understanding of how these technologies would develop (P16).

3.5.2. Failure to keep up with innovation

One of the key themes emerging from the specialist literature is that regulations are not designed with emerging technologies in mind and that they are failing to keep up with innovation (see Annex 2 for details). For instance, because of the top-down nature of most regulatory initiatives, studies show that there is a high probability of information asymmetry, resulting in regulations which are not fit-for-purpose.[15,101]

One of the drivers behind the MDR/IVDR was the recognition that regulations should reflect the technological change in the field of medical devices.[14] This is especially evident in the case of medical software. The MDR and the IVDR are more adequate at regulating software, because of a broader definition of a medical device as well as software-specific classification rules and GSPRs.

However, important limitations persist. Regarding software, although the MDR contemplates to an extent that a medical device may change during its lifecycle, it generally assumes that devices are fixed and stable once placed on the market.[6] This is not reflective of the nature of connected, intelligent devices, which may require software updates or, in more advanced versions, be self-learning algorithms.

The interviews corroborate this finding. There was a broad consensus among the interviewed stakeholders that new technologies and their applications develop at a much faster pace than regulatory frameworks can catch up (P1, P4, P14, P16). Indeed, the regulatory process is long and complicated – this is evidenced by a long process which preceded the passing of the MDR/IVDR, as consultations commenced in 2008.[102]

It has been highlighted that the specific field of connected, intelligent medical devices is relatively immature from a regulatory perspective (P7). This also applies to the standards landscape, which is still evolving (P16). As a result, stakeholders indicated that the existing regulations and standards are often inapplicable to new technologies in the medical device sector, for instance, because of the new ways in which these technologies are applied (P17, P19). It has also been highlighted that this creates a challenge for regulators, as they have to apply the existing regulations to new technologies (P19).

Limitations of the framework are particularly evident in the context of AI and ML. The existing literature identifies significant hurdles to the adoption of these technologies, primarily linked to the absence of the appropriate regulatory requirements. Shortcomings of the regulatory frameworks are also highlighted in the primary research. Although the MDR has brought improvements in how software is regulated, ML/AI remain unaddressed (P17, P19).

3.5.3. Regulatory and standardization gaps

Regulations and standards do not address some of the specific characteristics and risks of connected, intelligent medical devices. They are also failing to catch up with the pace of technological change, thus resulting in regulatory gaps.

Artificial intelligence

AI is an area where a regulatory gap is most evident, given the absence of specific regulations.

The literature highlights gaps around opacity, accountability and dynamic nature of algorithms.[6,101,103] Addressing these issues is crucial to ensure patient safety and trust. For instance, clearer rules around transparency and opacity would help address the black box problem, which currently hampers wide-scale adoption of AI technologies.[86,103] Guidance is also lacking around the appropriate data governance and algorithmic training processes. In this context, there are significant ethical risks are emerging, for instance, around algorithmic bias, which may negatively affect marginalised groups and exacerbate health inequalities.[81]

The importance of guidance and clearer requirements in these areas has been validated through the primary research. It appears that the regulatory gaps have a significant impact on manufacturers, who may not know how to proceed with the device development (P19). This has also been echoed in the UCL-BSI survey, where one respondent considered the lack of guidance for AI/ML to be among the main challenges for their organisation (1 respondent). Overall, it appears that this gap contributes to the barriers to AI adoption, thus having tangible implications for the market, innovation, and the ability of the healthcare systems to benefit from the opportunities offered by these technologies.

Given the significant interest in AI in the healthcare space and the fact that AI creates novel challenges compared to traditional devices, regulators' attention is needed to support AI deployment without endangering patient safety. Indeed, AI is increasingly on regulators' agenda. This is evident, for instance, in the European Commission's White Paper on AI, signalling an intention to move towards a risk-based approach to AI.[104]

Moreover, standards-making bodies also increasingly focus on AI among standards-making bodies. ISO subcommittee ISO/IEC JTC1/SC42 commenced work on standards for AI.[105] It takes a broad approach to AI, focusing on the entire ecosystem.[106] So far, it has published standards regarding big data and trustworthiness, with numerous standards currently being developed, including on concepts and terminology, uses cases and bias. Moreover, specifically in the field of medical devices, BSI has commenced its

collaboration with the MHRA and the US' Association for the Advancement of Medical Instrumentation (AAMI) on a position paper which provides recommendations on the standardization of AI activities in healthcare.[107] Moreover, the IMDRF has established a new working group on Artificial Intelligence Medical Devices.[108] Similarly, there is also ongoing work on ethical standards, for instance, the IEEE P7000 series, focusing on ethical and technological considerations.[109]

Wellness devices

As noted in section 3.2.3, evolving patient behaviour, technological developments, and the changing nature of medical devices are blurring the boundaries between unregulated wellness devices and medical devices. In this context, the literature also highlights the importance of the growing popularity of digital health and wellness devices and their evolving applications.[6]

Manufactures may not know whether regulations apply to their products (P15), or intentionally choose to classify their product as a wellness device to avoid regulation (P18). Indeed, the reliance on the 'intended use' for the definition of medical devices potentially creates the opportunity to circumvent regulations.[15] This may negatively affect patient safety as these products would not have met safety and functionality standards. It has also been observed that some digital health products are pushed to the market quickly and may not be as safe, robust and secure as they should be (P7). These risks are particularly important because these devices are used directly by patients and consumers without medical or technical training. They may not be aware of the devices' limitations and use them for unintended purposes, such as to derive health-related information.[6] These challenges and risks are likely to become pronounced in future, as the wellness devices market is predicted to grow.

Evidence of efficacy

Our primary and secondary research findings indicate challenges around providing adequate evidence demonstrating the efficacy of AI-driven medical devices. It is considered in the literature as a regulatory and standardization gap, with significant implications for patient safety. This has been echoed by a UCL-BSI survey respondent, who noted that the efficacy of AI-driven medical devices is often not adequately evaluated. This creates a safety risk with a potentially significant negative impact on the healthcare system. At the same time, another UCL-BSI survey respondent indicated that regulators were asking more questions about the safety and efficacy of these devices, indicating that it is a growing concern.

The efficacy problem stems mainly from the regulatory framework that places the responsibility for determining the acceptable level of risk on manufacturers of medical devices. Yet, manufacturers have limited control over how the device is used within its end-

user environment. Consequently, devices on the market may have different functionality to the device that was initially approved (P3). In addition, the literature denotes that the MDR does not account for other stakeholders using the device in the healthcare system, including patients or clinicians.[79,104,113] This is particularly critical for the allocation of responsibility and investigating adverse errors arising out of these devices during the post-market phase of the lifecycle. It illustrates that the regulatory frameworks insufficiently consider the implications and risks created by technological change.

Equally, the efficacy problem is a question of balancing privacy and precision, best illuminated by the evident tensions between the MDR and the GDPR. To demonstrate safety and efficacy, the MDR relies on the evidence-based approach to clinical evaluation as well as post-market surveillance.[75,112,114,115] To achieve these objectives, a robust evaluation process and a comprehensive data collection and analysis process is required. Simultaneously, the GDPR places strict restrictions on data collection. Due to restricted access to data, this creates significant challenges to the ability of device manufacturers to prove the efficacy of their devices.

Although the full adoption of AI-based devices in health care will take some time, one UCL-BSI survey respondent from the regulatory sector commented on the difficulties in finding a way to demonstrate the efficacy of these devices that would be acceptable to both regulators and the public. Currently, achieving the acceptable level of trust for its deployment and use, would likely require AI-based devices to follow the path of drug regulation with onerous requirements, trials and patient testing that would ultimately prove cumbersome for the industry (P19).

Addressing regulatory gaps

There is no consensus in the literature or among the interviewed stakeholders on how to address these existing and emerging regulatory gaps and prevent the emergence of new ones. On the one hand, there is the perception that regulation and standards are complex to understand and that the landscape is already challenging to navigate (P7). On the other hand, there are also areas where regulatory safeguards and guidance are lacking (P19).

The absence of consensus could be attributed to the complexity of the policy issues involved. For instance, decisions are needed regarding the required level of transparency or safeguards needed to prevent algorithmic bias in intelligent medical devices.[103] Moreover, the horizon scanning exercise conveyed that diverse trade-offs are involved, for instance, balancing patient safety, effective regulatory supervision as well as innovation. These difficulties are exacerbated by the complexity of new technologies, and their different, and continuously evolving applications.

These tensions are evident in discussions regarding the possible role of standards in addressing regulatory gaps. Studies show that standards enhance innovation where there is high uncertainty in the industry.[15,101] This was attributed to the standards-making process, which is driven by the industry. As a result, it is considered that standards are more likely to adequately address innovative technologies, compared to the more top-down regulations. Therefore, these studies concluded that standards were a coordination instrument for regulators in highly uncertain industries.

Some stakeholders agree that standards have a crucial role in complementing regulations and that they can address the emerging regulatory gaps (P6, P19). Indeed, as the standards-making process is significantly faster than passing new regulation, they are considered well-placed to fill in regulatory gaps. Importantly, standards already played this role under the MDD. Both the MDD (Annex I) and the MDR (Annex I) include the requirement to design devices in accordance with 'state of the art' which is interpreted to be represented by standards, as indicated by the EU guidance (MDCG 2.7/1) and regulators (P19).

Although the MDD had no specific cybersecurity requirements, regulators verified whether devices were cyber secure by looking at compliance with standards (P19). It emerges that there is some support among the stakeholders of implementing new standards, specific to new technologies (P13, P17, P19). Given that the MDR does not address AI sufficiently, another interviewee highlighted that standards are likely to play an important role in filling in the gaps in this area (P19). It has also been highlighted that standards may have a role in helping to address the ethical questions posed by AI (P13).

At the same time, counterarguments are also present. Some experts consider the European and UK regulations and standards to be not sufficiently adaptive to address innovative technologies (P5, P13, P18). It has been suggested that a risk-based approach would be more appropriate in dealing with new applications of technology, such as wearable devices (P18). For instance, it has been pointed out that lessons can be learnt from the more flexible, risk-based approach employed by the US FDA.[15] Moreover, although standards can be adapted faster than regulations and better reflect the state of the art, there are also concerns about standards failing to keep up with the pace of innovation. This has been attributed, for instance, to the standards formulation process not being sufficiently inclusive and the fragmentation of standards across legal jurisdictions as well as across different regulatory bodies (P1, P9, P16, P17).

Overall, the research highlights that standards may have an important role in ensuring patient safety and providing regulatory guidance, even for innovative technologies which the existing regulations were not designed to address. In this context, it is crucial there is a growing number of standardization initiatives, for instance, in the context of AI, such as the

BSI/AAMI and IMDRF work on medical devices. However, it appears that the ability of standards to keep up to date is a crucial concern. Both regulations and standards must be more dynamic to adapt more effectively to new information and feedback (P13). This is particularly important given that the technology and its applications are likely to continuously evolve (P16), potentially leading to the emergence of further gaps.

Additionally, given the lack of consensus on the approach, diverse policy issues involved as well as technological complexity, it emerges that policy initiatives in this area require a multi-stakeholder approach and international collaboration. Indeed, this was evident in the conversations with stakeholders (P1, P9, P10, P12, P15, P16, P18) and the specialist literature.[116] This approach will also support a system-level approach to regulating connected, intelligent medical devices.

4 CONCLUSION

The medical device industry has traditionally been heavily regulated due to the need to ensure patient safety. However, the increased use of connected and intelligent medical devices introduces new regulatory and standardization challenges, disrupting the existing frameworks.

It emerges that current regulatory and standardization frameworks do not comprehensively address the nature and the risks created by connected, intelligent devices. Challenges result from the cyber-physical nature of these devices, as well as novel use cases which blur the distinctions between medical and wellness devices. Product classification is also becoming more complicated, with uncertainties regarding classifying combination products and understanding the behaviour of devices outside of the laboratory. Embedding of connectivity and intelligence in devices introduces new vulnerabilities, giving rise to novel safety and security risks, which are currently not addressed by regulations. To mitigate them, manufacturers should apply a safety by design and security by design approach to the development process.

This research has also found that security and safety are often conflated. Although security is an important prerequisite to device safety, ensuring the safety of connected, intelligent devices requires regulators and manufacturers to adopt a holistic approach and consider diverse factors. Additionally, these critical challenges around regulating connected, intelligent devices are compounded by the rapid pace of technological development, making it hard for regulators to understand the emerging risks and keep up with the pace of innovation. As a result, crucial regulatory gaps are emerging.

Standards may help address these risks and fill in the emerging regulatory gaps around connected, intelligent devices, for instance around AI and security. For a start, global harmonization of standards is needed for a technology such as AI by standardizing terminology used across different stakeholder groups and various jurisdictions. This will facilitate a common understanding of the technology by ensuring people “speak the same language”. This, in turn, will support innovation and trade, facilitate market access, encourage shared understanding of emerging technologies globally and may help manage safety risks across the supply chain. The importance of doing so is evident in the ongoing work by international and national standards organisations, such as ISO and BSI/AAMI. This research supports the BSI-AAMI position paper’s recommendations[107], including the creation

of an international task force led by the US and the UK, to provide oversight of these standardization activities.

However, to ensure that standards can fill in regulatory gaps concerning fast-developing technologies, there needs to be a shift in the standards-setting process. Some of the needed changes concern the composition of expert teams and making the process more inclusive, as well as ensuring that standards are more dynamic and adaptive. Moreover, alongside socio-technical concerns created by connected, intelligent medical devices, standards should also address ethical considerations, particularly regarding AI. The ethical implications of AI regarding the trust, algorithmic bias, transparency and traceability were explored.

Whilst new technologies create challenges and risks, innovation is crucial to improve patient outcomes. Through this research, numerous barriers to innovation have also been identified. Although SMEs drive innovation in the digital health space, they are particularly affected by regulatory burdens due to the high resource requirements. For instance, compliance with the MDR may require complicated and costly organisational changes such as hiring the right expertise and aligning software teams with compliance requirements. Moreover, small market players find it difficult to navigate regulations and standards, and onerous regulatory requirements may increase barriers to market entry. Excessive burdens on small market players may have adverse effects on innovation and, consequently, delay market access and affect patient outcomes. Therefore, it is necessary for regulators and standards-making bodies to ensure that obligations do not disproportionately burden SMEs.

Overall, the growing popularity of connected, intelligent devices creates new challenges that stakeholders, manufacturers and public authorities alike, need to address. Being aware of these challenges, trade-offs and possible mitigation options is necessary to ensure that new technologies are used to improve patient care in a safe, accountable manner.

Future research needs

Adaptive standards

It has emerged that standards may have an important role in filling in regulatory gaps. However, especially in the context of quickly evolving technologies, the relevance of standards depends on their ability to keep up with the fast pace of technological change. This is necessary to capture the emerging risks and new use cases. Accordingly, BSI should ensure that standards are more adaptive and iterative, accounting for feedback, innovation and the uncertainties brought about by new technologies. We note that BSI has already published research in this area[117] and introduced agile standards development practices such as Publicly Available Specifications.[118] Other bodies, such as NESTA, have also published

useful guiding principles.[119] BSI should further explore how to implement these principles in practice to fit into the modern methodologies applied by medical technology companies

Regulatory and standardization gaps

Interview participants hinted at other regulatory and standardization challenges and regulatory gaps. These were not further investigated because of the limited data points and the lack of a specific focus on connected, intelligent medical devices. However, it is recommended that BSI considers these areas in future work. These gaps and challenges include:

- Challenges around combining citizen-generated with official health data (P1).
- Medicines with software in them, which may not qualify as medical devices (P19).
- Blurring boundaries between diagnostic and clinical support systems (P15).

Terminology

Similarly, as the UCL-BSI research project conducted in 2019, this research identified that the terms 'standards', 'standardization' and 'standardized' are frequently used interchangeably.[120] For instance, when asked about standards, some stakeholders discussed the need to have 'standardized' processes (in the sense of having uniform, similar processes), rather than standards developed by standards-making bodies, such as BSI. We agree with the recommendation from the UCL-BSI 2019 project that further research could attempt to clarify how stakeholders understand these different terms.

5 RECOMMENDATIONS FOR BSI

Based on our research findings, the following recommendations are presented to BSI.

5.1 Champion global standards development for emerging technologies

This research validates the importance of the existing work by ISO's technical committee and BSI/AAMI.[107] The following recommendations are proposed to build on these activities:

Short-term (in line with the BSI-AAMI position paper's recommendations)[107]

- Identify and onboard key international private and public-sector stakeholders for an international task force, which should ideally include technology leaders from the European and Asia Pacific regions.
- BSI's ART/1 should continue to contribute to and mirror ISO's SC42 technical committee on AI by highlighting possible issues in healthcare use cases.
- Agree on a roadmap for the development of high-level global harmonization of standards for AI in healthcare, including an agreement/taxonomy on terminology and identifying areas of convergence and divergence.
- Ensure BSI's committees continue to be inclusive (see recommendation 5.3).

Long-term

- Set regular reviews to ensure standards remain fit for purpose, as use cases evolve with technological development.
- Continue to engage with ISO's development of AI standards for multiple sectors.

5.2 Review ethical considerations of connected and intelligent medical devices

It is recommended that BSI publishes standards on the ethical testing of connected, intelligent medical devices, similar to BS 8611 Ethics Design and Application of Robots and Robotic Systems.[121] Ethical standards in this field would provide a degree of assurance for end-users, who presently have low trust regarding the deployment of these devices in healthcare. As suggested by our primary and secondary research, these standards could include:

- Requirements for an ethical committee to perform, review and approve connected and intelligent medical devices. This could include the need for manufacturers to declare if an ethical review has been conducted and to detail how the ethics review was performed.
- Best practices similar to a proposed "Hippocratic Oath for Connected Medical Devices"[122] to ensure stakeholders in the healthcare ecosystem commit to uphold principles of cyber safety. The intention is to incentivise stakeholders to commit to these ethical principles. For instance, this could be achieved if access to a national healthcare system prioritises manufacturers who adhere to these ethical principles.

As this may place additional burden on SMEs, it is suggested that the BSI engages with stakeholders in the short-term to identify assistance which they may require to support this initiative.

5.3 Facilitate SMEs' participation in the standards-making process

BSI should ensure the standards-making process for new technologies is inclusive and collaborative.

Our research found that the inclusiveness and diversity of stakeholders should be at the core of the standard making process for new technologies. While current standards-setting process already includes representatives from various stakeholder groups, interviewees highlighted concerns around the exclusion of SMEs as well as the inaccessibility of standards to these firms due to a lack of financial resources.

As such, the following recommendations are provided:

- Provide financial subsidies and incentives to encourage SMEs' participation in standards-making. For instance, this could take the form of access to BSI's standards database or consultation services in exchange for the SMEs' participation.
- Provide standards in more collaborative formats, for instance, enable organisations to engage with standards through GitHub, to align these processes with how modern software teams operate.
- Develop learning development pathways for manufacturers of connected, intelligent medical devices to allow for a structured approach to assimilating these educational resources. These pathways could span the innovation journey and account for each phase of the product lifecycle. This could resemble the US FDA's 'CDRH learn', that provides the industry with comprehensive, interactive and accessible educational resources.[123]

5.4 Make standards more understandable

It is recommended that the BSI continues to provide educational resources explaining standards and regulations as numerous stakeholders faced difficulties in interpreting them.

These resources should include clear descriptions, visualisations and real-life case studies of practical implementations and use simple language to make it easier for manufacturers to apply standards and regulations to their devices. These resources should help organisations engage with and implement standards from the beginning in the device lifecycle.

The research highlighted that support is particularly needed in the following areas:

- Provide guidance for classification – although the MDR introduced clearer rules for software classification, it still appears that manufacturers find the classification process of medical devices is challenging. Guidance materials should include detailed, real-life examples of classification, reflecting the diversity of the available products on the market.
- Provide guidance to support MDR /IVDR readiness – transition to the new regulations remains a significant challenge. BSI should work with manufacturers and provide guidance to help prevent market access delays.
- Provide guidance for post-market surveillance – BSI should focus on overcoming practical challenges to the implementation of post-market surveillance systems. BSI should aim to evaluate potential monitoring platforms where organisations can do continuous self-reporting.

This research project has produced an accompanying Entrepreneurs Guide (Annex 6) which supports SMEs in navigating the regulatory and standardization landscape. This could be a starting point for making standards more understandable.

6 REFERENCES / BIBLIOGRAPHY

1. Portalier P. Myths and realities of the presumption of conformity [Internet]. 2017 [cited 2020 Jul 26]. Available from: https://www.orgalim.eu/sites/default/files/2019-01/2017-05-15c%20Paper%20Portalier%20on%20scope%20and%20relevance%20of%20the%20presumption%20of%20conformity%20with%20the%20NLF.pdf

2. European Committee for Standardization. CEN and CENELEC's response to the Communication of the European Commission, COM(2018) 764 'Harmonised standards- Enhancing transparency and legal certainty for a fully functioning Single Market'. 2018.

3. Melvin T, Torre M. New medical device regulations: the regulator's view. EFORT Open Reviews. 2019 Jun;4(6):351–6.

4. European Commission. New EU rules on medical devices to enhance patient safety and modernise public health [Internet]. 2017 [cited 2020 Jun 6]. Available from: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_847

5. European Commission. Medical Devices - Sector [Internet]. [cited 2020 Jul 6]. Available from: https://ec.europa.eu/health/md_sector/overview_en#new_regulations

6. Ordish J, Murfet H, Hall A. Algorithms as medical devices. Cambridge, UK: PHG Foundation; 2019 Sep.

7. Jeary T, Schulze K, Restuccia D. What medical writers need to know about regulatory approval of mobile health and digital healthcare devices. Medical Writing. 2019 Dec;28(4).

8. Becker K, Lipprandt M, Röhrig R, Neumuth T. Digital health – Software as a medical device in focus of the medical device regulation (MDR). it - Information Technology. 2019 Oct 25;61(5–6):211–8.

9. KPMG, Regulatory Affairs Professional Society. The race to EU MDR compliance [Internet]. KPMG; 2018 [cited 2020 Aug 23]. Available from: https://www.raps.org/getattachment/Publications-Resources/Research-Reports/The-Race-to-EU-MDR-Compliance.pdf.aspx?lang=en-US

10. Sommer J, Lugard M, Hoffman A. EU MDR delayed: How does this impact the industry? [Internet]. 2020 [cited 2020 Jul 7]. Available from: https://www.medicalplasticsnews.com/news/eu-mdr-delayed-what-is-the-impact-on-the-industry/

11. MedTech Europe. MedTech Europe Statement on EU Commission intention to postpone MDR deadline [Internet]. 2020 [cited 2020 Aug 25]. Available from: https://www.medtecheurope.org/news-and-events/press/medtech-europe-statement-on-eu-commission-intention-to-postpone-mdr-deadline/

12. Schönberger M, Hoffstetter M. Regulations for Medical Devices. In: Emerging Trends in Medical Plastic Engineering and Manufacturing [Internet]. Elsevier; 2016 [cited 2020 Aug 15]. p. 19–64. Available from: https://linkinghub.elsevier.com/retrieve/pii/B9780323370233000026

13. Donawa M. Global harmonization, its work items and clinical evaluation. BSI Compliance Navigator. 2019.

14. European Commission. Communication from the Commission on safe, effective and innovative medical devices and in vitro diagnostic medical devices for the benefit of patients, consumers and healthcare professionals. [Internet]. European Commission; 2012 [cited 2020 Aug 8]. Available from: https://ec.europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-540-EN-F1-1.Pdf

15. Quinn P. The EU commission's risky choice for a non-risk based strategy on assessment of medical devices. Computer Law & Security Review. 2017 Jun;33(3):361–70.

16. Medicines and Healthcare products Regulatory Agency. Regulating medical devices from 1 January 2021 [Internet]. 2020 [cited 2020 Sep 5]. Available from: https://www.gov.uk/guidance/regulating-medical-devices-from-1-january-2021

17. Prime Minister's Office. The Future Relationship with the EU: The UK's Approach to Negotiations. 2020.

18. Cumberlege J. First Do No Harm-The report of the Independent Medicines and Medical Devices Safety Review [Internet]. 2020 Jul [cited 2020 Aug 25]. Available from: https://www.immdsreview.org.uk/downloads/IMMDSReview_Web.pdf

19. British Standards Institution. What is a standard? [Internet]. 2020 [cited 2020 Aug 16]. Available from: https://www.bsigroup.com/en-SG/Standards/Information-about-standards/what-is-a-standard/

20. Health Sciences Authority Singapore. Medical device guidance. Health Sciences Authority Singapore; 2018.

21. International Organization for Standardization. ISO STANDARDS ARE INTERNATIONALLY AGREED BY EXPERTS [Internet]. ISO. n.d. [cited 2020 Aug 20]. Available from: https://www.iso.org/standards.html

22. International Organization for Standardization. Consumers and Standards: Partnership for a Better World [Internet]. n.d. [cited 2020 Aug 20]. Available from: https://www.iso.org/sites/ConsumersStandards/1_standards.html#section1_2

23. European Committee for Standardization. European Standards [Internet]. n.d. [cited 2020 Aug 20]. Available from: https://www.cen.eu/work/products/ENs/Pages/default.aspx

24. European Telecommunications Standards Institute. Types of Standards [Internet]. n.d. [cited 2020 Aug 20]. Available from: https://www.etsi.org/standards/types-of-standards

25. Willingmyre GT. Role of Standards: International Commerce for Medical Devices. IEEE Eng Med Biol Mag. 1984 Mar;3(1):26–30.

26. NHS England. Clinically-led Review of NHS Access Standards [Internet]. n.d. [cited 2020 Aug 20]. Available from: https://www.england.nhs.uk/clinically-led-review-nhs-access-standards/

27. Joyce R, Joshi I, Morley J. NHS Digital Health Technology Standard Draft [Internet]. NHSx; 2020 [cited 2020 Aug 10]. Available from: https://www.nhsx.nhs.uk/media/documents/NHS_Digital_Health_Technology_Standard_draft.pdf

28. European Commission. Harmonised Standards [Internet]. Internal Market, Industry, Entrepreneurship and SMEs - European Commission. 2016 [cited 2020 Aug 29]. Available from: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en

29. Marucheck A, Greis N, Mena C, Cai L. Product safety and security in the global supply chain: Issues, challenges and research opportunities. Journal of Operations Management. 2011 Nov;29(7–8):707–20.

30. Altayyar SS. The Essential Principles of Safety and Effectiveness for Medical Devices and the Role of Standards. MDER. 2020 Feb;Volume 13:49–55.

31. Anand K, Saini KS, Chopra Y, Binod SK. To Recognize the Use of International Standards for Making Harmonized Regulation of Medical Devices in Asia-Pacific. Journal of Young Pharmacists. 2010 Jul;2(3):321–5.

32. U.S. Food & Drug Administration. Recognized Consensus Standards [Internet]. 2019 [cited 2020 Aug 24]. Available from: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfstandards/search.cfm

33. International Organization for Standardization. ISO 14971:2019 [Internet]. ISO. 2019 [cited 2020 Aug 31]. Available from: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/27/72704.html

34. International Organization for Standardization. ISO/IEC 27009:2020 [Internet]. ISO. 2020 [cited 2020 Aug 31]. Available from: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/39/73907.html

35. Davey SM, Brennan M, Meenan BJ, McAdam R. Innovation in the medical device sector: an open business model approach for high-tech small firms. Technology Analysis & Strategic Management. 2011 Sep;23(8):807–24.

36. Ackerly DC, Valverde AM, Diener LW, Dossary KL, Schulman KA. Fueling Innovation In Medical Devices (And Beyond): Venture Capital In Health Care. Health Affairs. 2008 Jan 1;27(Supplement 1):w68–75.

37. Hourd PC, Williams DJ. Results from an exploratory study to identify the factors that contribute to success for UK medical device small- and medium-sized enterprises. Proc Inst Mech Eng H. 2008 May 1;222(5):717–35.

38. Haghi M, Thurow K, Stoll R. Wearable Devices in Medical Internet of Things: Scientific Research and Commercially Available Devices. Healthcare Informatics Research. 2017 Jan 1;23(1):4–15.

39. KPMG. KPMG. Medical Devices 2030 [Internet]. KPMG; 2020 [cited 2020 Aug 26] p. 10, 16, 19. Available from: https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/12/medical-devices-2030.pdf

40. British Standards Institution. Medical Device Product Development Lifecycle - BSI [Internet]. 2020 [cited 2020 Sep 6]. Available from: https://www.bsigroup.com/en-GB/medical-devices/our-services/product-lifecycle/

41. ISO. IEC 62304:2006 [Internet]. ISO. [cited 2020 Jul 8]. Available from: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/84/38421.html

42. ICO. An overview of the Auditing Framework for Artificial Intelligence and its core components [Internet]. ICO; 2020 [cited 2020 Sep 1]. Available from: https://ico.org.uk/about-the-ico/news-and-events/ai-blog-an-overview-of-the-auditing-framework-for-artificial-intelligence-and-its-core-components/

43. Dey N, Ashour AS, Shi F, Fong SJ, Tavares JMRS. Medical cyber-physical systems: A survey. J Med Syst. 2018 Mar 10;42(4):74.

44. Taylor K, Steedman M, Sanghera A, Thaxter M. Medtech and the Internetof Medical Things - How connected medical devices are transforming health care [Internet]. Deloitte; 2018 [cited 2020 Aug 12] p. 19–24. Available from: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf

45. Altawy R, Youssef AM. Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. IEEE Access. 2016;4:959–79.

46. Gatouillat A, Badr Y, Massot B, Sejdić E. Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine. IEEE Internet of Things Journal. 2018 Oct;5(5):3810–22.

47. Martignani C. Cybersecurity in cardiac implantable electronic devices. Expert Review of Medical Devices. 2019 Jun 3;16(6):437–44.

48. Camara C, Peris-Lopez P, Tapiador JE. Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of Biomedical Informatics. 2015 Jun 1;55:272–89.

49. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, et al. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In: 2008 IEEE Symposium on Security and Privacy (sp 2008). 2008. p. 129–42.

50. Kune DF, Backes J, Clark SS, Kramer D, Reynolds M, Fu K, et al. Ghost talk: Mitigating EMI signal injection attacks against analog sensors. In 2013. p. 145–59.

51. Marin E, Singelée D, Garcia FD, Chothia T, Willems R, Preneel B. On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. In: Proceedings of the 32nd Annual Conference on Computer Security Applications

[Internet]. Los Angeles, California, USA: Association for Computing Machinery; 2016 [cited 2020 May 22]. p. 226–236. (ACSAC '16). Available from: https://doi.org/10.1145/2991079.2991094

52. Li C, Raghunathan A, Jha NK. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In: 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services. 2011. p. 150–6.

53. Jin H, Luo Y, Li P, Mathew J. A Review of Secure and Privacy-Preserving Medical Data Sharing. IEEE Access. 2019;7:61656–69.

54. Lesh K, Weininger S, Goldman JM, Wilson B, Himes G. Medical Device Interoperability-Assessing the Environment. In: 2007 Joint Workshop on High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play Interoperability (HCMDSS-MDPnP 2007). 2007. p. 3–12.

55. Venkatasubramanian KK, Vasserman EY, Sokolsky O, Lee I. Security and Interoperable-Medical-Device Systems, Part 1. IEEE Security Privacy. 2012 Sep;10(5):61–3.

56. Alhumud MA, Hossain MA, Masud M. Perspective of health data interoperability on cloud-based Medical Cyber-Physical Systems. In: 2016 IEEE International Conference on Multimedia Expo Workshops (ICMEW). 2016. p. 1–6.

57. Argaw ST, Bempong N-E, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Medical Informatics and Decision Making. 2019 Jan 11;19(1):10.

58. Vasserman EY, Venkatasubramanian KK, Sokolsky O, Lee I. Security and Interoperable-Medical-Device Systems, Part 2: Failures, Consequences, and Classification. IEEE Security Privacy. 2012 Nov;10(6):70–3.

59. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018 Jul;113:48–52.

60. IBM. Cost of a Data Breach Report 2020 [Internet]. IBM; 2020 [cited 2020 Sep 6]. Available from: https://www.ibm.com/security/digital-assets/cost-data-breach-report/

61. Tschider CA. Deus Ex Machina: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future. Savannah L Rev. 2018;5(1):177–210.

62. Banerjee A, Venkatasubramanian KK, Mukherjee T, Gupta SKS. Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems. Proceedings of the IEEE. 2012 Jan;100(1):283–99.

63. Yaseen M, Saleem K, Orgun MA, Derhab A, Abbas H, Al-Muhtadi J, et al. Secure sensors data acquisition and communication protection in eHealthcare: Review on the state of the art. Telematics and Informatics. 2018 Jul 1;35(4):702–26.

64. Ghafur S, Fontana G, Martin G, Grass E, Goodman J, Darzi A. Improving Cyber Security in the NHS [Internet]. Imperial College London - Institute of Global Health Innovation; 2019 [cited 2020 Aug 15]. Available from: https://www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf

65. Marsh, Microsoft. 2019 Global Cyber Risk Perception Survey [Internet]. Marsh, Microsoft; 2020 [cited 2020 Aug 19]. Available from: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

66. PwC. Global top health industry issues: Defining the healthcare of the future [Internet]. PwC Health Research Institute; 2018 [cited 2020 Aug 20]. Available from: https://www.pwc.com/gx/en/healthcare/pdf/global-top-health-industry-issues-2018-pwc.pdf

67. Medical Device Coordination Group. MDCG 2019-16. Guidance on Cybersecurity for medical devices [Internet]. 2020 Jan [cited 2020 Jul 2]. Available from: https://ec.europa.eu/docsroom/documents/41863

68. IMDRF. Principles and Practices for Medical Device Cybersecurity. International Medical Device Regulators Forum; 2020 p. 46.

69. Choudhury A. AI in Healthcare: Improving Human Interface for Patient Safety. Better Standards Needed to Make Artificial Intelligence User-Friendly for Clinicians [Internet]. Rochester, NY: Social Science Research Network; 2020 Feb [cited 2020 Jul 30]. Report No.: ID 3529394. Available from: https://papers.ssrn.com/abstract=3529394

70. Ellahham S, Ellahham N, Simsekler MCE. Application of Artificial Intelligence in the Health Care Safety Context: Opportunities and Challenges. Am J Med Qual. 2020 Jul 1;35(4):341–8.

71. Marcilly R, Schiro J, Beuscart-Zéphir MC, Magrabi F. Building Usability Knowledge for Health Information Technology: A Usability-Oriented Analysis of Incident Reports. Appl Clin Inform. 2019;10(3):395–408.

72. Kasparick M, Andersen B, Franke S, Rockstroh M, Golatowski F, Timmermann D, et al. Enabling artificial intelligence in high acuity medical environments. Minimally Invasive Therapy & Allied Technologies. 2019 Mar 4;28(2):120–6.

73. Blandford A, Furniss D, Vincent C. Patient safety and interactive medical devices: Realigning work as imagined and work as done. Clin Risk. 2014 Sep;20(5):107–10.

74. Freed GL. When New Standards to Improve Safety Do Not Actually Improve Safety. JAMA Pediatr. 2019 Oct 1;173(10):921–2.

75. Sittig DF, Wright A, Coiera E, Magrabi F, Ratwani R, Bates DW, et al. Current challenges in health information technology–related patient safety. Health Informatics J. 2020 Mar 1;26(1):181–9.

76. He J, Baxter SL, Xu J, Xu J, Zhou X, Zhang K. The practical implementation of artificial intelligence technologies in medicine. Nature Medicine. 2019 Jan;25(1):30–6.

77. Winfield AFT, Jirotka M. Ethical governance is essential to building trust in robotics and artificial intelligence systems. Phil Trans R Soc A. 2018 Nov 28;376(2133):20180085.

78. Morley J, Machado C, Burr C, Cowls J, Taddeo M, Floridi L. The Debate on the Ethics of AI in Health Care: A Reconstruction and Critical Review [Internet]. Rochester, NY: Social Science Research Network; 2019 Nov [cited 2020 Aug 15]. Report No.: ID 3486518. Available from: https://papers.ssrn.com/abstract=3486518

79. Hoeren T, Niehoff M. Artificial Intelligence in Medical Diagnoses and the Right to Explanation. Eur Data Prot L Rev. 2018;4:308.

80. Benjamin R. Assessing risk, automating racism. Science. 2019 Oct 25;366(6464):421–2.

81. McCradden MD, Joshi S, Anderson JA, Mazwi M, Goldenberg A, Zlotnik Shaul R. Patient safety and quality improvement: Ethical principles for a regulatory approach to bias in healthcare machine learning. J Am Med Inform Assoc [Internet]. 2020 [cited 2020 Aug 2]; Available from: http://academic.oup.com/jamia/article/doi/10.1093/jamia/ocaa085/5862600

82. Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019 Oct 25;366(6464):447–53.

83. Buolamwini J, Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: Conference on Fairness, Accountability and Transparency [Internet]. PMLR; 2018 [cited 2020 Sep 8]. p. 77–91. Available from: http://proceedings.mlr.press/v81/buolamwini18a.html

84. Bukowski M, Farkas R, Beyan O, Moll L, Hahn H, Kiessling F, et al. Implementation of eHealth and AI integrated diagnostics with multidisciplinary digitized data: are we ready from an international perspective? Eur Radiol [Internet]. 2020 May 6 [cited 2020 Aug 18]; Available from: http://link.springer.com/10.1007/s00330-020-06874-x

85. Challen R, Denny J, Pitt M, Gompels L, Edwards T, Tsaneva-Atanasova K. Artificial intelligence, bias and clinical safety. BMJ Qual Saf. 2019 Mar 1;28(3):231–7.

86. Gerke S, Minssen T, Cohen G. Ethical and legal challenges of artificial intelligence-driven healthcare. Artificial Intelligence in Healthcare. 2020;295–336.

87. Morley J, Machado CCV, Burr C, Cowls J, Joshi I, Taddeo M, et al. The ethics of AI in health care: A mapping review. Social Science & Medicine. 2020 Sep 1;260:113172.

88. Brown J. IBM Watson Reportedly Recommended Cancer Treatments That Were 'Unsafe and Incorrect'. Gizmodo [Internet]. 2018 [cited 2020 Aug 6]; Available from: https://gizmodo.com/ibm-watson-reportedly-recommended-cancer-treatments-tha-1827868882

89. Pesapane F, Volonté C, Codari M, Sardanelli F. Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. Insights Imaging. 2018 Oct 1;9(5):745–53.

90. London AJ. Artificial Intelligence and Black-Box Medical Decisions: Accuracy versus Explainability. Hastings Center Report. 2019;49(1):15–21.

91. ANSM. ANSM'S Guideline. Cybersecurity of medical devices integrating software during their life cycle. 2019 Jul.

92. Hanna S, Rolles R, Molina-Markham A, Poosankam P, Fu K, Song D. Take two software updates and see me in the morning: the case for software security evaluations of medical devices. In: Proceedings of the 2nd USENIX conference on Health security and privacy. San Francisco, CA: USENIX Association; 2011. p. 6. (HealthSec'11).

93. Sharples S, Martin J, Lang A, Craven M, O'Neill S, Barnett J. Medical device design in context: A model of user–device interaction and consequences. Displays. 2012 Oct 1;33(4):221–32.

94. Skierka IM. The governance of safety and security risks in connected healthcare. 2018 Jan 1;2 (12 pp.)-2 (12 pp.).

95. Rimmer J. Improving software environments through usability and interaction design. J Audiov Media Med. 2004 Mar;27(1):6–10.

96. McHugh M. Medical Device Software and Technology: the Past, Present and Future. Articles [Internet]. 2015 Mar 1; Available from: https://arrow.tudublin.ie/scschcomart/38

97. Macombe L, Schroeder A. General Safety and Performance Requirements (Annex I) in the New Medical Device Regulation [Internet]. Available from: https://www.bsigroup.com/LocalFiles/es-MX/dispositivos-medicos/General_Safety_and_Performance.pdf

98. Rakitin SR. Coping with Defective Software in Medical Devices. Computer. 2006 Apr 1;39(4):40–45.

99. Guzman NHC, Wied M, Kozine I, Lundteigen MA. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. Systems Engineering. 2020;23(2):189–210.

100. Eisner L. Will We Have Harmonized Standards By The MDR's Date Of Application? Med Dev Online. 2019.

101. Recht MP, Dewey M, Dreyer K, Langlotz C, Niessen W, Prainsack B, et al. Integrating artificial intelligence into the clinical practice of radiology: challenges and recommendations. Eur Radiol. 2020 Jun;30(6):3576–84.

102. European Commission. Proposal for a Regulation of the European Parliament and of the Council on medical devices, and amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 [Internet]. 2012/0266 Sep 26, 2012. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0542:FIN:EN:PDF

103. Kiseleva A. AI as a Medical Device: Is it Enough to Ensure Performance Transparency and Accountability? European Pharmaceutical Law Review. 2020;4(1):5–16.

104. Kiseleva A. Comments on the EU White Paper on AI: A Regulatory Framework for High-Risk Healthcare AI Applications [Internet]. Rochester, NY: Social Science Research Network; 2020 Jun [cited 2020 Aug 5]. Report No.: ID 3627741. Available from: https://papers.ssrn.com/abstract=3627741

105. International Organization for Standards. ISO/IEC JTC 1/SC 42 Artificial Intelligence [Internet]. [cited 2020 Aug 30]. Available from: https://www.iso.org/committee/6794475.html

106. ISO and IEC Joint Technical Committee. Why artificial intelligence needs standards? [Internet]. Available from: https://jtc1info.org/technology/subcommittees/artificial-intelligence/

107. Rowley A, Turpin R, Walton S. AI and machine learning algorithms in healthcare: Position paper. BSI and AAMI; 2019.

108. IMDRF. Artificial Intelligence Medical Devices [Internet]. 2020. Available from: http://www.imdrf.org/workitems/wi-aimd.asp

109. Cihon P. Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development [Internet]. Center for the Governance of AI Future of Humanity Institute, University of Oxford; 2019 Apr. Available from: https://www.fhi.ox.ac.uk/wp-content/uploads/Standards_-FHI-Technical-Report.pdf

110. Hinton G. Deep Learning—A Technology With the Potential to Transform Health Care. JAMA. 2018 Sep 18;320(11):1101–2.

111. Hwang TJ, Kesselheim AS, Vokinger KN. Lifecycle Regulation of Artificial Intelligence– and Machine Learning–Based Software Devices in Medicine. JAMA. 2019 Dec 17;322(23):2285–6.

112. McGreevey JD, Hanson CW, Koppel R. Clinical, Legal, and Ethical Aspects of Artificial Intelligence–Assisted Conversational Agents in Health Care. JAMA [Internet]. 2020 Jul 24 [cited 2020 Jul 31]; Available from: https://jamanetwork.com/journals/jama/fullarticle/2768927

113. Christ A, Quint F. Artificial Intelligence : from Research to Application ; the Upper-Rhine Artificial Intelligence Symposium (UR-AI 2019). arXiv:190308495 [cs] [Internet]. 2019 Mar 20 [cited 2020 Aug 5]; Available from: http://arxiv.org/abs/1903.08495

114. Sujan MA, Koornneef F, Chozos N, Pozzi S, Kelly T. Safety cases for medical devices and health information technology: Involving health-care organisations in the assurance of safety. Health Informatics J. 2013 Sep 1;19(3):165–82.

115. FDA. Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff [Internet]. 2016 [cited 2020 Jul 3]. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

116. Ahmad OF, Stoyanov D, Lovat LB. Barriers and pitfalls for artificial intelligence in gastroenterology: Ethical and regulatory issues. Techniques in Gastrointestinal Endoscopy. 2019 Oct;150636.

117. Tait J, Banda G. Proportionate and adaptive governance of innovative technologies. The role of regulations, guidelines and standards [Internet]. BSI; 2016 Jul [cited 2020 Aug 8]. Available from: https://www.bsigroup.com/LocalFiles/en-GB/BIS/Innovate%20UK%20and%20emerging%20technologies/Summary%20Report%20-%20Adaptive%20governance%20-%20WEB.pdf

118. British Standards Institution. The PAS process [Internet]. BSI; Available from: https://www.bsigroup.com/globalassets/localfiles/en-gb/pas/The%20PAS%20Process/pas-info.pdf

119. Armstrong H, Gorst C, Rae J. Renewing regulation. 'Anticipatory regulation' in an age of disruption [Internet]. NESTA; 2019 Mar. Available from: https://media.nesta.org.uk/documents/Renewing_regulation_v3.pdf

120. Blanchier C, Down E, Manghi AI, O'Brien J-K. Burden or Benefit: Do Standards Work for IoT SMEs? [Internet]. Rochester, NY: Social Science Research Network; 2019 Sep [cited 2020 Jan 23]. Report No.: ID 3454591. Available from: https://papers.ssrn.com/abstract=3454591

121. British Standards Institution. BS 8611:2016 Robots and robotic devices. Guide to the ethical design and application of robots and robotic systems [Internet]. 2016 [cited 2020 Aug 31]. Available from: https://shop.bsigroup.com/ProductDetail?pid=000000000030320089

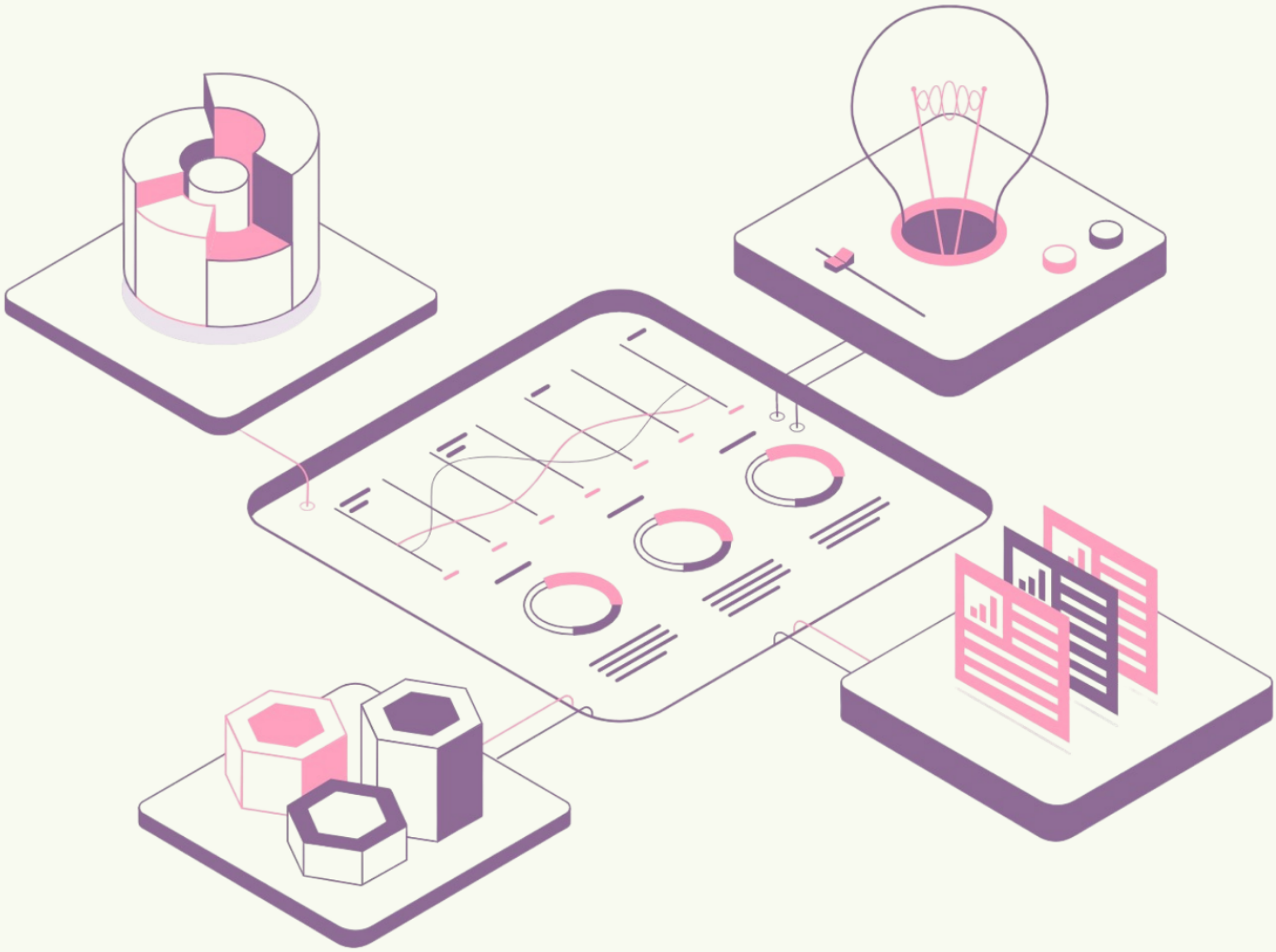
122. Woods B, Coravos A, Corman JD. The Case for a Hippocratic Oath for Connected Medical Devices: Viewpoint. Journal of Medical Internet Research. 2019;21(3):e12568.

123. FDA. CDRH Learn [Internet]. FDA. FDA; 2020 [cited 2020 Aug 31]. Available from: https://www.fda.gov/training-and-continuing-education/cdrh-learn

7 ANNEXES

Regulatory and Standardization Challenges for Connected and Intelligent Medical Devices

Annex 1: Methodology and Background



UCL In Partnership with bsi.

RESEARCH SCOPE

This research project investigated the regulatory and standardization challenges of connected, intelligent medical devices.

The main research questions guiding the project were:

- What are the regulatory and standardization gaps regarding connected and intelligent medical devices?
- What are the possible negative interactions between software and the IT environment in which it operates?
- What are the challenges to the safety and security of connected and intelligent medical devices across the supply chain?
- How can the BSI evolve its standards development practices regarding medical devices, information governance and health software?
- What are the main trends and innovations emerging in the field of intelligent and connected medical devices?
- How could regulations and standards help address emerging challenges?

DATA COLLECTION AND ANALYSIS

The research findings and recommendations were based on extensive data collection, covering secondary desk-based research (literature review and horizon scanning) and primary data collection (interviews, online survey). The researchers also participated in numerous webinars related to medical devices as participants. We also hosted a breakout session at BSI's Spring 2020 Standards e-Conference and will present the final finding at the IMPACT 2020 Conference.

1 DESK-BASED RESEARCH

1.1 Literature Review

It covered desk-based research on the existing standards, regulations, legislation and specialist academic literature. Given the novel character of the field, grey literature was also consulted.

The review focused on the following main areas:

- Regulatory and standardization challenges concerning connected and intelligent medical devices,
- Safety and security challenges arising across the device lifecycle, including negative interactions between software and the IT environment, and
- The innovation landscape and emerging trends.

The literature review process was divided into two phases. In the first phase, the aim was to understand the background and the context of the topic, as well as to refine the research scope and the main questions. The second phase served the specific purpose of answering the research questions and understanding the state of knowledge. This phase was used to identify the key findings, which were subsequently explored and validated through other research methods.

Numerous databases were searched to identify the relevant sources, including Web of Science, Scopus, ScienceDirect. Google searches were also conducted.

Detailed findings from the literature review are available in Annex 2.

1.2 Horizon scanning

A horizon scanning exercise was undertaken to complement the literature review. It covered government reports, news articles and materials published by international organisations, academia, manufacturers and consulting firms. The purpose of horizon scanning was to inform our understanding of the dynamics of change in the field of connected and intelligent medical devices, especially the main trends and potential future regulatory/ standardization gaps.

Horizon scanning was done in a three-phase approach[1] and covered major themes related to connected, intelligent medical devices including regulations, standards, patient safety, innovation, cybersecurity and negative interactions with the IT environment.

The first phase focused on exploratory scanning and processing to identify key areas for further analysis within each of the themes. In the second phase, an issue-centred scanning approach was adopted to further explore the key areas which were prominent in the previous phase. Through this, key signals of emerging trends and drivers of change were identified. We also correlated and condensed findings across the thematic areas. Finally, in the third phase, we combined our findings with other research activities in order to assess the associated policy implications and provide policy recommendations.

There was a minimum requirement of five articles for each key theme to ensure the robustness of the horizon scanning exercise. The same articles could be used across relevant areas of research. For each article, the corresponding search term was recorded to ensure the replicability of research findings. Key areas for which relevant articles were heavily skewed towards an extreme (i.e. most articles supported a certain view) were identified and search terms were intentionally modified to tease out the opposing position, to eliminate bias in the search terms.

Based on the findings from the horizon scanning, key drivers of change in the field of connected and intelligent medical devices were identified. These were grouped into three main areas (regulatory / standardization, technology and human/social), as well as by time horizon (within two years and two to five years) based on the likely pervasiveness of each driver of change. The frequency with which these drivers of change were mentioned in interviews and surveys were represented by different colour codes in the diagram. Frequency of occurrence in primary data may be indicative of the impact levels. However, further research is required to draw substantive conclusions.

The drivers of change analysis from the horizon scan is included in the report (Figure 7).

2 PRIMARY DATA COLLECTION

2.1 Interviews

Interviews were the main source of primary data. The intention was to obtain unique, qualitative insights into the challenges involved in working with connected and intelligent medical devices and the role of standards. Interviews were semi-structured, which allowed the group to cover 'core' topics, while also enabling us to engage in a free discussion and ask participants about their unique perspectives. Each interview was tailored to the specific areas of expertise while drawing upon the existing framework of questions set in the initial phase of the project.

Overall, 19 stakeholders were interviewed. We sought out interviewees from the three main stakeholder groups: industry, experts (including academics) and regulatory bodies/ public organisations. Interviewees comprised BSI contacts (5), team members' personal contacts (2), contacts identified from various organisation's websites (7), contacts identified from journal articles included in the literature review (1), contacts identified from conferences and events (2) and contacts referred by other interviewees (2).

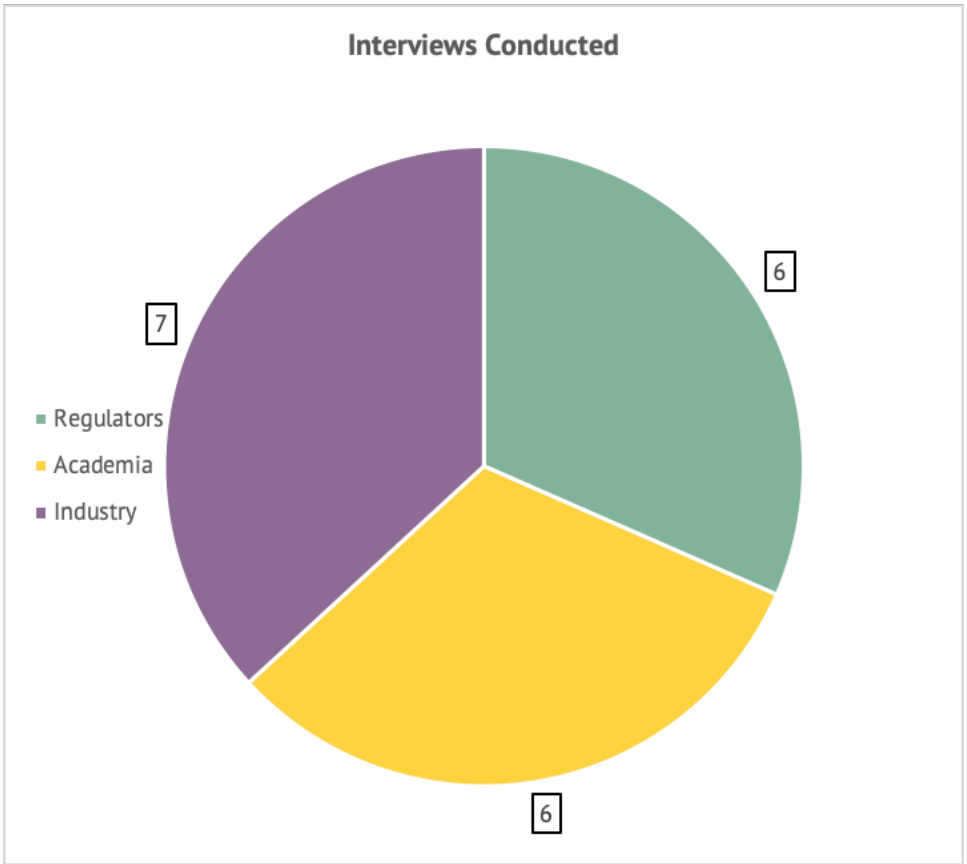


Figure 1: Breakdown of interviewees by stakeholder group

Two team members conducted each interview. One member was in charge of asking questions while the other focused on recording the interview and taking field notes. We used online communication platforms to conduct the interviews, primarily Microsoft Teams (UCL-preferred infrastructure). As detailed in the ethics application, a consent form and a participation information sheet were sent to interviewees and signed in advance. Participants were also asked whether they consented to the audio recording. Out of 19 interviews conducted, 18 were recorded.[1] Interviews generally lasted between 30 and 45 minutes.

The relevant parts of the interviews were then transcribed and complemented with field notes. Interviews were subsequently thematically coded within two days of the interview to ensure reasonable immediacy.

2.2 UCL-BSI online survey

An online survey was used to complement interviews and gather a broader range of responses. It provided the team with quantitative and qualitative data. The survey consisted

[1] One session was conducted on Google Hangouts due to technical difficulty encountered by the interviewee. This session was therefore, not recorded due to data governance issues.

of 19 questions (a mix of open-ended and closed-ended questions) and was designed to take no more than 15 minutes.

The survey was hosted by the BSI. The purpose was to understand the innovation process better and at what stage in the product development standards are used. The survey focused on key areas such as the safety and security of connected and intelligent medical devices across the supply chain, manufacturers' experiences with standards and regulations, and the main challenges that manufacturers are facing.

A total of 50 survey responses were gathered. Respondents represented a broad range of organisations, including SMEs, corporations, trade associations, healthcare providers, consultancy and other relevant organisations. They also work with diverse technologies, representing the diversity in the field of intelligent, connected medical devices.

The survey covered topics related to organisational and regulatory challenges as well as emerging risks and issues. Please see Annex 4.

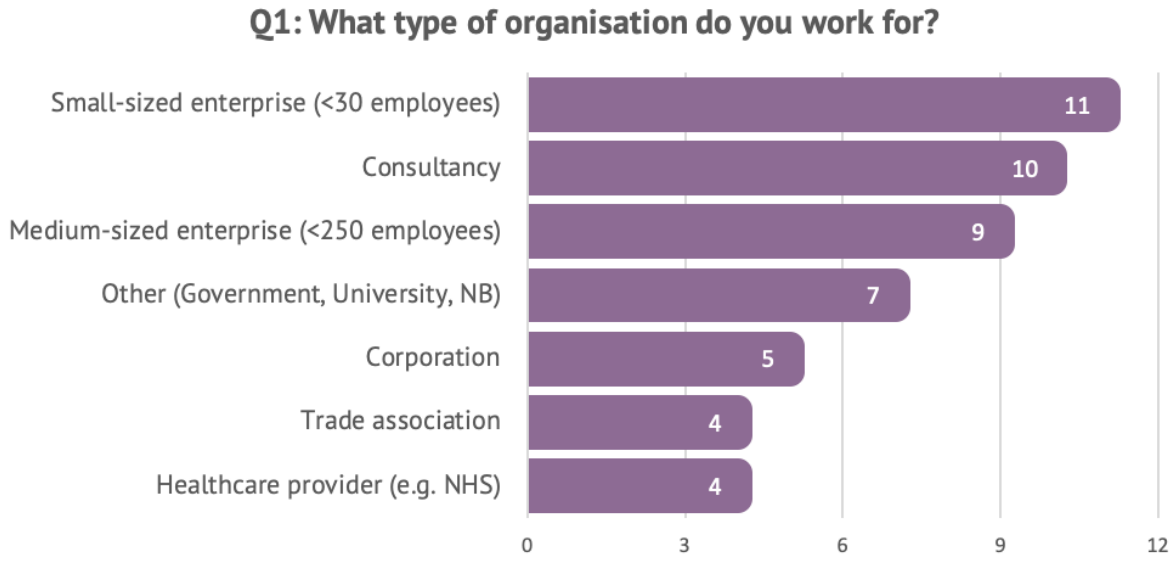


Figure 2: Breakdown of survey respondents by organisation type

Respondents that chose 'Other' comprise universities (2), the Government (1), student (1), a Notified Body (1), regulator (1), and health technology network (1).

The quantitative results were summarised and analysed, while the qualitative responses (responses to open-ended questions) were thematically coded using the same method as the interview analysis, to ensure consistency. Some inconsistent data was tidied by the team (for instance when one responded selected 'no' in the question of whether they use standards,

while later discussing their use of standards). Every response which contained ambiguities was cross-checked with several team members to avoid any bias.

3 OTHER – OBSERVATION THROUGH INDUSTRY MEETINGS, WEBINARS, AND CONFERENCE PARTICIPATION

BSI Standards Conference

We co-hosted an online breakout session with the BSI during the BSI Standards e-Conference on 23 April 2020. The conference concerned BSI's work and standards in general and it has attracted over 1000 attendees representing various industries.

The session lasted for 45 minutes and provided us with an excellent opportunity to engage with stakeholders. It also allowed us to validate our research objectives and better understand the challenges involved in regulating connected, intelligent medical devices.

The recording from the session is available here: https://www.bsigroup.com/en-GB/our-services/events/2020/bsi-standards-conferences/BSI-standards-conference-spring/standards-e-conference-recordings/

BSI Committee Meetings

We were able to attend two relevant BSI Committee meetings (I) biological evaluation of medical devices on 10 March 2020, and (ii) artificial intelligence on 26 March 2020. BSI Committees have an important role in the standardization process and participate in standards-making at the international level. Observing the meetings allowed us to understand better the standardization process and BSI's role in it.

Other

The initial intention of the group was to participate in and present the research at numerous industry meetings. Unfortunately, the COVID-19 pandemic considerably hindered the group's ability to do so.

We will be virtually presenting the research findings at the IMPACT 2020 cybersecurity conference on 29 September 2020.

With physical industry events cancelled, the group also participated in a broad range of webinars and online events. They exposed us to diverse issues in the field and were useful in validating the initial findings as well as highlighting new areas to explore.

Some of the events attended include:

- Artificial intelligence in radiology: what is the potential (23 April 2020)
- CogX (8-10 June 2020)
- ISC Online Session: Cybersecurity & Medical Technology (17 June 2020)
- FW Live: Understanding Medical Practice Changes in an Increasingly Virtual World (25 June 2020)
- Navigating the Wild West of Digital Health (30 June 2020)
- Tea & Tech: Medtech - Don't Let a Medical Condition Interfere with Your Life (1 July 2020)
- TINs Seminar: The Mechanics Behind the Rapid Translation of the CPAP Device (1 July 2020)
- Getting paediatrics apps into clinical pathways (ORCHA) (1 July 2020)
- Tackling cyber-threats in health and care: learning from Covid-19 (15 July 2020)
- Regulation Hackathon - data-driven technologies in healthcare (22 July 2020)

4 METHODS OF ANALYSIS

With data collected through the survey, we used quantitative analysis methods (for multiple-choice, closed questions) and qualitative methods such as content and thematic analysis (for open-ended questions). The open-ended questions were coded using the same method as the interviews.

With data collected through interviews, we conducted narrative and thematic analysis to determine the main patterns.

Based on the primary data collected, as well as secondary research, particularly the horizon scanning exercise, a 'drivers of change' analysis was conducted to map the main trends shaping the field. This has informed our understanding of the dynamics of change and enabled us to provide BSI with recommendations on the evolution of its practices.

ETHICS APPLICATION

The UCL Research Ethics Committee granted ethics approval before the primary data collection commenced. All research activities were conducted in accordance with high ethics and data protection standards. Participants took part in the research voluntarily and provided informed consent – they were informed about the purpose of the research and how any data would be stored and processed.

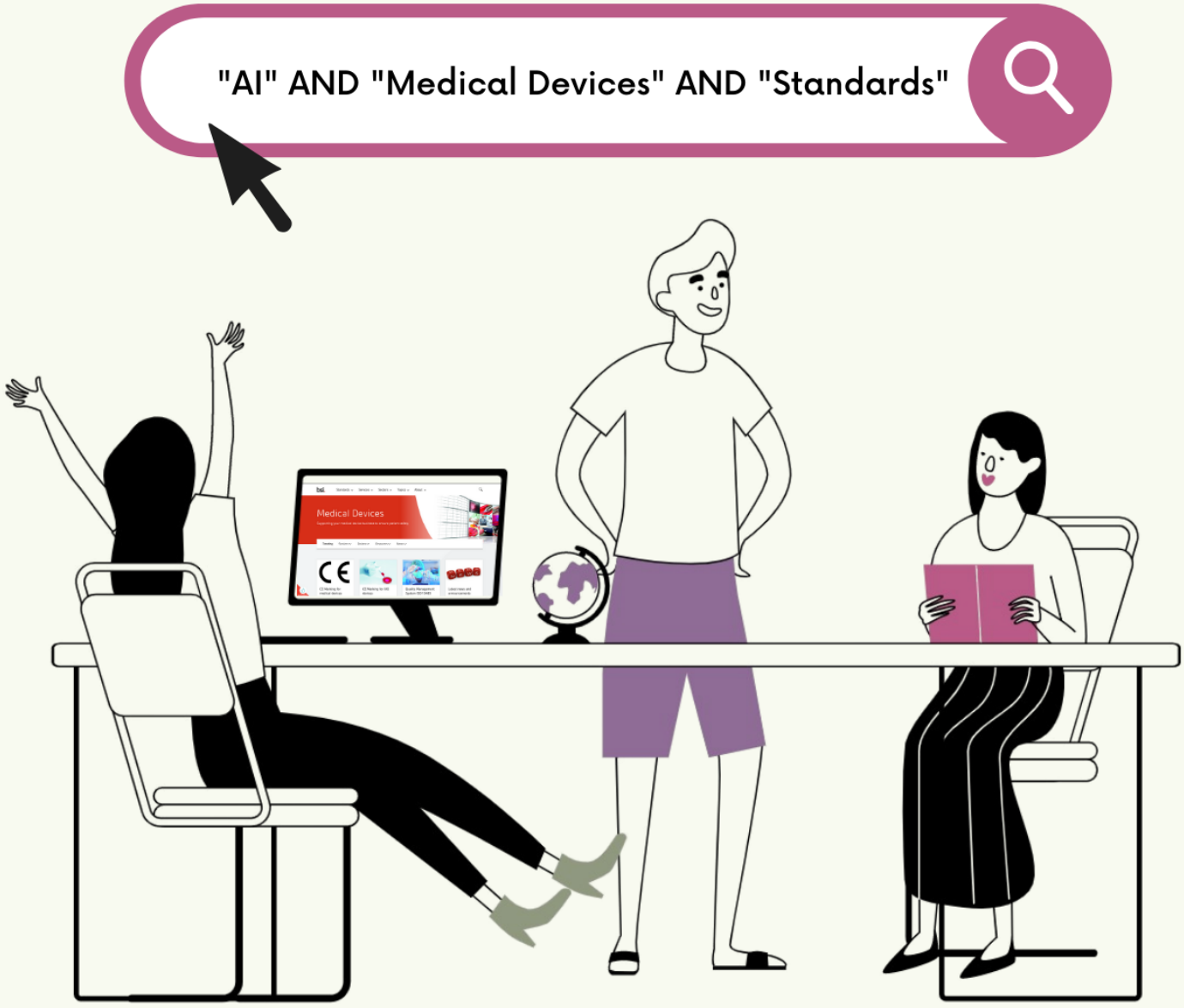
BIBLIOGRAPHY

1. Amanatidou E, Butter M, Carabias V, Könnölä T, Leis M, Saritas O, et al. On concepts and methods in horizon scanning: Lessons from initiating policy dialogues on emerging issues. Sci Public Policy. 2012 Mar 1;39(2):208–21.

2. DeLurio J, Hulshizer R, Robertson D, Wilkinson B, Schoelles K. Horizon Scanning Protocol and Operations Manual. September 2015 Revision. [Internet]. (Prepared by ECRI Institute under Contract No. 290-2010-00006-C.) AHRQ Publication No. 15-EHC035-EF. Rockville, MD: Agency for Healthcare Research and Quality; 2015. Available from: www.effectivehealthcare.ahrq.gov/reports/final.cfm

Regulatory and Standardization Challenges for Connected and Intelligent Medical Devices

Annex 2: Literature Review



UCL In Partnership with bsi.

1 INTRODUCTION

While the literature on medical devices is vast, the specific topic of regulatory and standardization challenges of connected and intelligent medical devices is relatively under-researched. Moreover, the term 'connected and intelligent' medical devices is rarely used, with most studies focusing on either 'connected' or 'intelligent' devices. These issues necessitated a careful, nuanced analysis of the source material, in particular understanding which specific technologies were discussed.

The literature review focused on exploring the challenges created by connected and intelligent devices to answer research questions guiding the project. These were related to: (i) regulations, (ii) standardization, (iii) patient safety, (iv) security, (v) negative interactions between software and the IT environment, and (vi) innovation. Overall, there is a particularly large body of research on patient safety, cybersecurity and innovation.

The primary focus was on journal articles and regulatory material (legislation, standards, policy documents). Given the novel character of the field, grey literature was also consulted. Further details on the methodology are included in Annex 1, section 1.1.

2 REGULATION

Research question: What are the regulatory gaps regarding connected, intelligent medical devices?

Overall, there is very little writing on the regulation of connected, intelligent medical devices. Studies tend to be general, discussing medical devices broadly, or focus on the specific technologies involved, such as software, artificial intelligence (AI) or wearable devices.

2.1. REGULATORY LANDSCAPE

New European regime

The replacing of the Medical Device Directive (MDD) and the In Vitro Diagnostic Medical Devices Directive (IVDD) with the Medical Devices Regulation (MDR) and the In Vitro Diagnostic Medical Devices Regulation (IVDR) has attracted extensive coverage in literature, with numerous summaries of the main obligations available.

Regulatory change was needed in the European Union (EU) for a range of reasons. In the aftermath of safety scandals related to hip and breast implants, the legislative intent was to

increase the safety of medical devices on the market.[1] In addition, technological advancement was a key driver behind the legislative change.[2,3] Indeed, the European Commission recognised that since the MDD, medical technology has significantly developed, for instance through information and communication technologies, personalised medicine and evolving models of healthcare delivery.[4] This necessitated changes to the framework, and a new approach to what is considered a medical device.[5]

The MDR and the IVDR broadly continue the previous framework but introduce certain important changes and additional requirements in numerous areas.[1] Some of the key changes aim to increase safety, such as onerous post-market surveillance requirements, tighter clinical trials obligations, and improved traceability.[2] Moreover, the new framework aims to increase transparency to enable consumers to find relevant information.[2] For instance, under Article 32 of the MDR, the EUDAMED database will include safety and clinical performance information for certain high-risk devices. Reflecting the intention to modernise the framework in the light of technological advancements,[1] there is an increased focus on software. As an example, the MDR includes specific provisions for software, on classification (Annex VIII, Rule 11) and performance (Annex I, Section 17). Furthermore, new requirements around data protection, cybersecurity and the interactions between software and the broader IT environment, address the increasing connectivity of medical devices.

Overall, the new regulatory framework provides more clarity and is more appropriate at dealing with devices relying on software. However, important gaps and unaddressed issues remain regarding connected, intelligent medical devices, as further discussed in 1.2 below.

International approaches

The literature conveys the importance of international harmonization of medical device regulation. Some of the key benefits of harmonization concern fewer barriers to trade, lesser regulatory burdens for manufacturers and faster market access for patients.[6,7]

Overall, there is a high degree of international convergence. At the EU level, the framework will rely on regulations following the end of the transition period, which are directly applicable in all Member States. Therefore, it will support harmonization across the internal market. Beyond the EU, the International Medical Device Regulators Forum (IMDRF), which has replaced the Global Harmonization Task Force on Medical Devices, is crucial in supporting harmonization. An important objective of IMDRF is to respond to the technological advancement in the field of medical devices, such as the growing importance of software.[8] This highlights that digitalisation has been transforming the field of medical devices, necessitating new regulatory approaches.

However, despite these international initiatives, there remains a degree of divergence and

certain areas would benefit from greater harmonization.[9] For instance, differences between the EU and US frameworks arise around definitions, classifications and compliance procedures.[10–12] Although both regimes focus on the intended use of a device, it has been highlighted that the US Food and Drug Administration (US FDA) understands the intended use with reference to the "objective intent".[13] This differs from a more subjective approach in the EU and means that different products may be considered a medical device under these regimes. Moreover, there are different classification categories and procedures. For instance, the MDR recognises four risk classes, in comparison to three under the US FDA's framework.[9] Additionally, demonstrating conformity with the requirements in the US requires compliance with US FDA's detailed, specific guidelines, whereas in the EU the focus is on harmonized standards.[9]

Specifically, in the context of connected and intelligent medical devices, comparisons are often made between the EU and the US, with some studies suggesting advantages of the US approach. Most notably, Quinn argued that the US FDA adopted a more adaptive, risk-based approach to innovative products, such as mHealth apps, which makes the US framework better placed to deal with technological innovation.[14] According to Quinn, the US FDA engages in a case-by-case analysis and it has the discretion not to regulate low-risk devices.[14] This is set out in Section 3060 of the 21st Century Cures Act, which states that software is regulated as a medical device if the US FDA considers that it is "reasonably likely to have serious adverse health consequences". No such discretion is given to regulators in the EU. However, there is lack of consensus in the literature on how substantive the difference is between the EU and US approaches. Ordish et al. highlighted that in practice, despite differences, similar conclusions may be reached under both frameworks.[13]

However, the US FDA in recent years has been active in issuing regulatory guidance, for instance, concerning digital health, AI, and wearables. In particular, the US FDA's *Pre-Certification Programme* and *AI Framework*, are considered important in conceptualising software and AI, and addressing regulatory gaps created by technological change. Currently, in comparison, there is little guidance available on these topics in the EU, and there are no specific provisions relating to AI in the MDR.[8] This highlights a degree of divergence between both systems, which may become an area of future regulatory activity. Furthermore, these different approaches offer the opportunity for the EU and US regulators to engage in policy learning on the appropriate approach to emerging technologies.

2.2. CRITICAL ISSUES

Software

Due to its growing application in the medical field and the significant impact of the MDR/IVDR in this area, challenges around software emerge as a key theme in the literature.

Importantly, medical device software captures a broad range of technologies, from simple programmes to highly complex AI applications.

Definitions

Rule 3.3 in Annex VIII of the MDR distinguishes between (i) software that is independent (i.e. software as a medical device (SaMD)) and (ii) software that drives or influences the use of a device. Importantly, these two types of software create distinct challenges. Software that drives or influences the use of a device presents specific difficulties due to potential negative hardware-software interactions (see section 5 below). Regulatory guidance has focused thus far on SaMD. Some of the most notable documents include guidance from the IMDRF (*Possible Framework for Risk Categorization and Corresponding Considerations*)[15] and the European Commission (*MEDDEV 2.1/6 Guidance*)[16].

The MDR/IVDR broadened the definition of a medical device, which, according to some studies, was necessary because of the technological change in the field.[17] Under Article 2(1) of the MDR, the full definition is:

'medical device' *means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:*

- *diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,*
- *investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,*
- *providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,*

and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

Importantly, regulations now cover devices designed for the purpose of 'prediction and prognosis' of a disease. This is crucial in the context of software, as the new regulatory regime will capture a broader range of applications and generally provides more clarity compared to the previous framework.[18] However, there remains a degree of difficulty in deciding what classifies as a medical device, especially in the context of digital devices (see 'wellness devices' section below for more detail).[13] Although this broader definition is beneficial from the perspective of patient safety, it creates significant challenges for

manufacturers. Following the end of the transition period[1], numerous organisations will be brought into the framework for the first time, often with little guidance or resources to address compliance burdens. As the literature suggests, some organisations may be unaware that the regime captures them.[13] This has potential consequences for patient safety, as uncertified devices may enter the market.

Classification

One of the key implications of the MDR is that software will generally be classified as class IIa or higher under Rule 11, Annex VIII MDR. The classification relies on the severity of the potential consequences.[8] This up-classification has important implications for software developers, meaning that they must comply with more onerous requirements.[18] Importantly, the European Medical Device Coordination Group (MDCG) issued *Guidance on Qualification and Classification of Software*[19], which clarifies that Rule 11 intends to mirror IMDRF's approach to risk classification, contained in *Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations*.[15] MDCG's *Guidance* is, therefore, important in promoting international regulatory harmonization. However, there is a slight divergence in terminology between the documents. MDCG uses the concept of 'medical device software', covering SaMD and software influencing the use of a device, whereas IMDRF's *Framework* focuses specifically on SaMD.[8]

Specific pre-market and post-market considerations

Increased use of medical device software creates specific compliance and regulatory challenges, which are not present in the case of traditional devices. These complexities are evident at the pre-market and post-market stage.[20]

The General Safety and Performance Requirements in Annex I of the MDR include provisions specific to software design and manufacture. Some of these provisions are new compared to the MDD. For instance, they require software repeatability, reliability and performance. This new requirement recognises the dynamic nature of software.[8] Moreover, the MDR adds specific requirements regarding cybersecurity, for instance, by highlighting that manufacturers have to consider "state of the art" with respect to information security. There is also an increased focus on the interactions with the broader software environment, further discussed in 6.2 below.

At the post-market stage, one of the key issues is that software may need to be updated, which creates challenges in the context of quality management and post-market surveillance. For instance, this raises the question when recertification[13] or a new Unique Device Identifier may be needed.[21] This is further discussed in the context of AI below.

[1] The transition period for the MDR has been moved from May 2020 to May 2021. The transition period for IVDR will expire in May 2022.

Artificial intelligence

There is a consensus in the literature that AI and machine learning (ML) offer immense opportunities in healthcare. However, these technologies are still at the early stages of development and their potential applications are likely to evolve.[22,23] The literature underlines significant hurdles to the adoption of AI, especially specific regulatory and implementation challenges.[18]

In the EU, the regulatory landscape on AI/ML remains immature, with important unresolved issues.[13] Currently, there are no specific AI/ML provisions in the EU, and under the MDR AI/ML has approached the same way as software.[8] However, the European Commission's *White Paper on Artificial Intelligence*[24] signals a potential change in the regulatory landscape. The *White Paper* recognises that healthcare is one of the priority areas for AI adoption and procurement. Furthermore, it notes that the Commission is investigating specific safety and liability challenges in the healthcare context. Therefore, it is reasonable to expect further work in the EU in this area, which will likely affect the field of medical devices.

It has to be underlined that the difficulty of regulating AI arises both *ex-ante* and *ex-post*.[25] The literature indicates that the main regulatory gaps emerge around: accountability, transparency and opacity, as well as the self-learning character of this technology.

Concerning accountability, the main question is who should be responsible for actions and the performance of a medical device, and its potential errors after the market entry. This challenge is likely to grow as AI systems become more autonomous, particularly unsupervised AI. Under the MDR, a manufacturer has the primary responsibility for the device, but this does not fully reflect the complex ecosystem in which AI-driven medical devices are used and a broad range of users (patients and clinicians).[21] Errors may be attributable to the deployment and use of a device (such as interpretation of results, low quality of input data), rather than the product itself.

Moreover, the literature underlines that AI changes the relationship between clinicians and devices, especially in the context of clinical decisions support systems. This introduces risk of, for instance, automation bias, and requires greater technical expertise from clinicians.[26] Furthermore, medical practitioners' work may change, with an increased focus on data and information management.[26] Accordingly, there are numerous calls in the literature for additional training and guidance for medical practitioners dealing with AI, to enable them better understand the limitations of these algorithms.[26] This is especially important in disciplines which are likely to be heavily affected by the growth of AI, such as radiology.

Challenges also arise around transparency and opacity of AI algorithms. For instance, it has been noted that the MDR's obligations of repeatability, reliability and performance could still

be met by opaque algorithms.[13] This is considered problematic because the ability to understand an algorithm is relevant to the assessment of device safety, risk and effectiveness.[13] Moreover, transparency, in terms of patients' ability to understand the treatment and provide consent, is fundamental to the patient's trust in the healthcare system and using the prescribed treatments.[21] Some researchers have turned to finding practical solutions to the problem, underlining that policy decisions have to be made around the levels of transparency required to provide patients with sufficient information and how this can be achieved.[21]

Although this question arises with medical software in general, AI-applications, due to their self-learning character, highlight the challenge of dealing with connected, intelligent medical devices, which, unlike traditional devices, are not static but have a dynamic character. Software and AI applications are usually developed through an iterative process, and continuous updates are required once placed on the market. This means that their performance and characteristics may change in the post-market stage, which, as noted above, creates challenges in the context of post-market obligations and ongoing monitoring.

Overall, it has to be underlined that the MDR does not include provisions specific to intelligent devices, meaning that important aspects of AI devices' safety and performance are not addressed. For instance, there are no provisions on data quality or potential encoded biases. As a result, this creates difficulties around assessing the safety and effectiveness of intelligent devices.[13] Further details are provided in section 4.2 below.

Wellness devices

There is also a large body of literature focusing on wellness devices, especially wearables and mobile apps. Wellness devices are specifically excluded from the medical device regime (Recital 19 MDR/ Recital 17 IVDR), which creates a large regulatory gap in this area.

The exclusion of wellness devices from the framework is problematic. There is a convergence between health and wellness, meaning that the distinction between wellness and medical devices is becoming blurred.[14,20] For instance, wellness devices are increasingly accurate, because higher-quality sensors and technology are commercially available.[13] According to Ordish et al., this removes the distinction between consumer and medical devices.[13] Moreover, the popularity of wellness devices is growing and they are applied in a broader range of contexts.[14] Quinn underlined that strict reliance on "the intended purpose" when defining medical devices in the EU, contributes to the issue.[14] This is because whether a product is regulated as a medical device or not may depend on the way it is marketed, rather than its risk profile or specific functionality.[14] At the same time, in the case of mobile apps, studies found numerous issues with their quality.[27] The fact that wellbeing products are not regulated is problematic as digital devices are increasingly used directly by

patients/customers, who do not have any medical training and may potentially misuse them.[13] For instance, they may rely on information provided by apps or wearable devices to make health-related decisions[14], such as whether to go to the clinician or not, which may have significant health and safety consequences. Accordingly, the exclusion of these devices from the MDR framework reveals potential shortcomings of the regime in protecting patients' safety.[14]

At the same time, some studies note that the Notified Body's capacity has dramatically decreased under the new medical device regime. As Notified Bodies have to be recertified under the new regulations and subject to more stringent designation requirements[17], the number of designated bodies has significantly decreased. Simultaneously, Notified Bodies under MDR/IVDR have a considerably broader role and are responsible, for instance, for unannounced audits. All these factors create a capacity issue. Importantly, certain papers suggest that the issue concerns not only resources but also expertise. Since digital products require different skills from regulators to properly test and analyse them, there is a shortage of experts.[13] Overall, this indicates that including an even broader range of digital devices under the regime would overburden the capacity of Notified Bodies.

Data management

Data management and confidentiality are crucial areas in the context of connected, intelligent medical devices. However, it is not addressed in sufficient detail in the MDR/ IVDR. Questions of data management and security are relevant across the entire lifecycle of a device, highlighting the importance of these considerations at the design level and once devices are placed on the market.

Annex I of the MDR, has important implications for data management. For instance, Requirement 17.2, requires software-driven devices to be developed in accordance with the "state of the art, taking into account the principles of the development lifecycle, risk management". Moreover, Requirement 17.4 underlines the importance of "IT networks characteristics and IT security measures, including protection against unauthorised access". This underlines the importance of cybersecurity and data protection. More generally, Annex I imposes requirements around risk management which are relevant for manufacturers from a data management perspective, for instance requiring them to evaluate and control the risks occurring during the intended use and "reasonably foreseeable misuse". However, it is important to note that the legislation remains high level and non-specific.

Importantly, the European Commission has been working on the Privacy Code of Conduct for mHealth. However, progress on this document has paused following the introduction of the General Data Protection Regulation (GDPR).[28]

In the EU, a medical device is subject to the GDPR if it collects personal data. This means that manufacturers of such medical devices need to ensure compliance with data protection regulations, which further contributes to the regulatory burden.[8] Under the GDPR, health data is considered a special category of data. This means that processing it is illegal unless, under Article 9(2) of the GDPR, there is explicit consent or data is used for the provision of "medical diagnosis, the provision of health or social care or treatment or the management of health". The GDPR has important implications for various medical device lifecycle stages, design and safety and performance requirements, data storage and transfer, or post-market surveillance.[8] Moreover, the GDPR imposes other obligations, such as the data minimisation principle or the right to be forgotten, which create challenges, new questions and uncertainties for device developers. Importantly, exploratory research in the field of medical apps indicates that non-compliance with the GDPR may be common, especially regarding transparency around data collection and its purpose.[29]

Studies indicate that solutions improving data management are necessary to maximise the benefits offered by new technologies and build trust between clinicians, patients and digital medical solutions.[30] These comments arise especially around AI technologies since a lack of agreement around data sharing, storage, and security are among crucial hurdles to the development of AI in healthcare.[26,31,32]

Changing nature of the medical devices field

Overall, the literature review clearly indicates that the digitalisation and the emergence of connected, intelligent medical devices are fundamentally changing the field of medical devices – this, in turn, disrupts the regulatory frameworks.

One of the key transformations is the blurring of the boundaries between various domains – medical devices, healthcare provision, software technology, pharmaceutical industry and wellness. Each of these domains is regulated differently, which increases complexity and creates challenges for regulators as well as device users and manufacturers.[33] These processes highlight the importance of analysing the entire ecosystem and the context in which medical devices are used.

A broader definition of a medical device in MDR means that new types of organisations are brought under the regime. They may differ from the traditional device manufacturers, because of different capacities and resources. In particular, this concerns software developers and SMEs. Furthermore, hospitals developing in-house support systems for their needs may also be captured by the MDR/IVDR.

The end customer of medical devices is also changing. There is an increased focus on business-to-consumer interactions, as devices are increasingly used by patients, i.e. people

without specialist training.[8] As a result, market participants are no longer only "well-resourced" specialist organisations.[14] Clinicians' interactions with medical devices are also changing and influencing their relationships with patients.[30] These observations may highlight the need to incorporate new considerations in the regulatory and standardization frameworks, for instance, around usability. Moreover, some researchers recommend solutions focused around the collaboration between multiple stakeholders, to better understand the ethical and regulatory issues arising across the supply chain.[30]

2.3. KEY FINDINGS

Based on the literature review, the following regulatory gaps and challenges were identified:

- The new regulatory framework captures a broad range of software-enabled applications. Generally, it classifies them into medium- and high-risk categories, meaning that manufacturers must comply with onerous requirements despite potentially not having resources and capabilities to do so. This may have adverse consequences for innovation and competition in the market, by placing significant burdens on smaller manufacturers. Moreover, dependence on software creates specific challenges for manufacturers in terms of pre-market and post-market requirements. In particular, due to its non-static nature, software underlines the importance of ongoing monitoring.
- The MDR/IVDR framework does not capture some of the characteristics and complexities of connected, intelligent medical devices. Regulators' attention is needed across multiple areas, such as the iterative nature of software, transparency, accountability and data management. This is particularly important as the use of connected, intelligent medical devices is likely to grow and further evolve.
- The EU's new regulatory regime does not sufficiently capture the potential risk that the growing number of wellness devices may create for user safety.
- Regulators should consider the changing nature of the field of medical devices, especially the blurring of the boundaries between different disciplines, and the fact that a broad range of individuals and organisations are increasingly participating in the market.

3 STANDARDS

Research question: What are the standardization gaps regarding connected, intelligent medical devices?

The literature mainly focused on the role of standards, the classification of standards and key standards in the United Kingdom. Another important theme is the role of standards in

balancing patient safety with competing interests, including device utility and product innovation. However, there was a lack of articles on the standardization of connected, intelligent medical devices focusing on a complete product lifecycle approach and interactions within their environment. This highlights a critical gap in standards which are crucial in providing guidance to industry stakeholders on how to address new, complex challenges surrounding patient safety and device security.

3.1. ROLE OF STANDARDS

Standards are "an agreed way of doing something", and cover a wide range of activities from manufacturing products and process management to service delivery.[34] Standards in the medical device sector serve several purposes. They aim to enhance the safety, reliability and performance of products or services.[35] Standards define the criteria for a minimum viable product, provide quality assurance on product functionality and establish accountability[35]. Standards complement regulations by elaborating methods and evaluation criteria, which may be too complicated within regulations[36]. This is because standards are typically easier to update, and revise compared to regulations.

3.2. CLASSIFICATION OF STANDARDS

There are several ways to classify standards applicable to the medical devices sector,[37] including the following:

- **International**[38] **/ regional standards**[39–41]
  Standards in this category represent a consensus across various national standards bodies, on a regional or an international level. These standards are facilitated by organisations such as the International Organization for Standardization (ISO) and the European Committee for Standardization (CEN). National standards bodies naturally have an incentive to participate in the development of international standards to ensure that their national interests are represented.

- **National standards**[37]
  These are standards which have been approved by a formally acknowledged national standards bodies, such as the BSI. Formal standards are drawn up through the process of building consensus among experts, based on specific principles determined by the national standards-setting organisation. These experts are typically brought together in technical committees to produce a draft set of standards. The technical committees typically comprise representatives from industry associations, academia, research institutes, government agencies and consumers. The draft standards are then circulated for public consultation. After that, the committee decides which comments

to incorporate and finalises a set of standards for formalisation. BS 70000 is an example of a British Standard for medical devices.

- **Health system standards**[42,43]
  These standards are generally accepted requirements complied by members of a specific industry and may not necessarily be endorsed by national standards bodies. For example, within the National Health Service (NHS), the Data Coordination Board (DCB) is responsible for developing and approving standards.[44] Some of the areas covered include information governance, data collection and data extraction. Subject matter experts appraise DCB standards. Compliance with some of these industry standards may help meet the regulatory requirements. For instance, health IT systems procured by NHS Trusts must comply with the DCB0129 standard under the Health and Social Care Act 2012.[44]

3.3. KEY STANDARDS

Standards may be further categorised into basic, group/horizontal, vertical and process standards, to indicate the sector, processes or devices for which they are applicable. The definition of each category, based on a BSI publication[45], is provided below:

- Basic: states fundamental concepts and specifies generic requirements. As such, these apply to a wide range of products, processes or services across multiple sectors.
- Group/horizontal: specifies safety and performance criteria which are relevant to a group of similar products processes or services.
- Product: specifies safety and performance criteria for a specific type of product, process, or service, typically referencing basic and group standards.
- Process: specifies requirements for elements of a process used to develop, implement or maintain a stage of a product or service lifecycle. A process standard may be a basic, group or product standard.

From an analysis of standards published by the BSI[46] and NHS Digital[44], a list of applicable standards related to the development and use of connected and intelligent medical devices in the United Kingdom was compiled. They are summarised in four broad categories below:

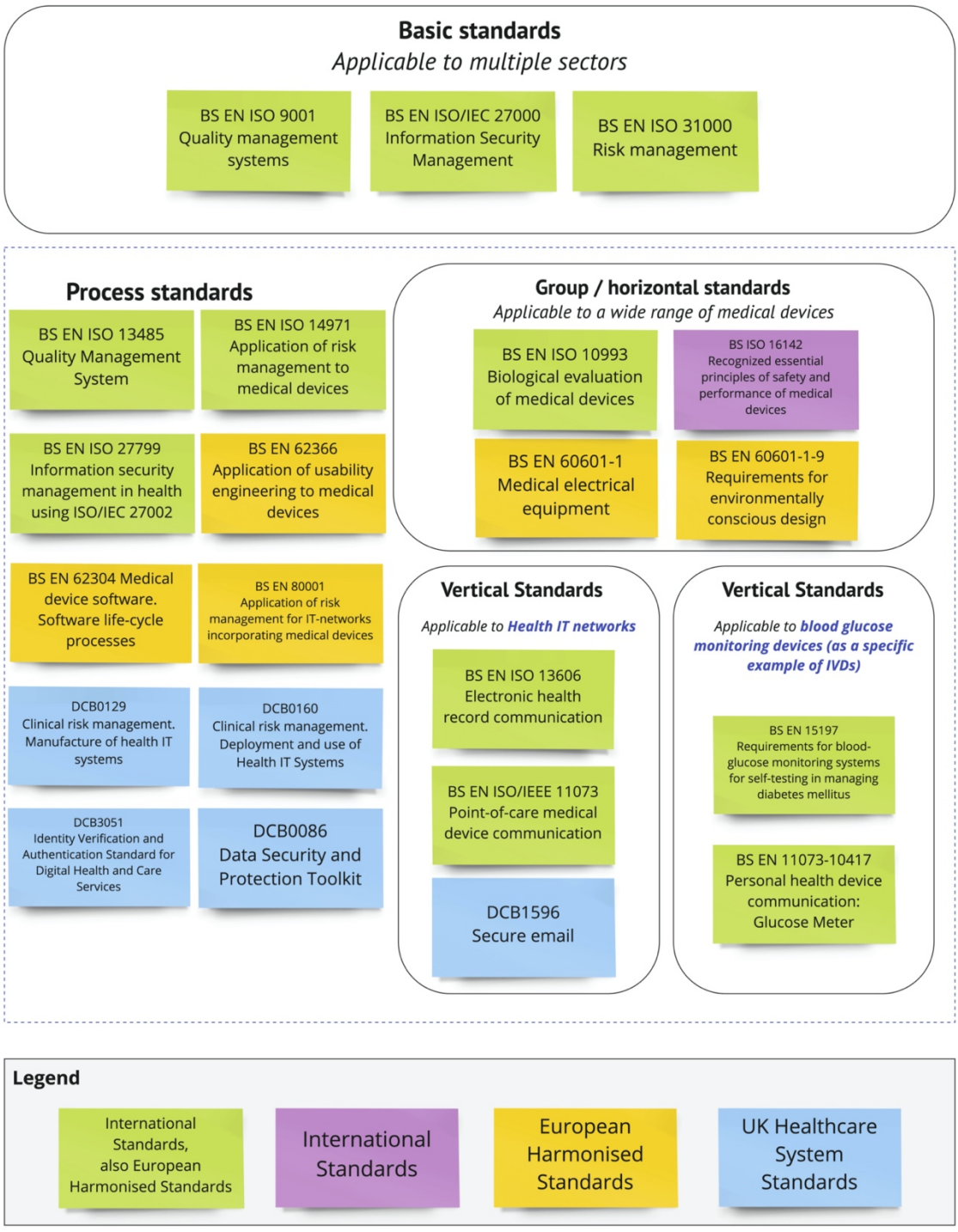


Figure 1. Key standards applicable to connected and intelligent medical devices in the UK.

3.4. STANDARDIZATION CHALLENGES

Risks and challenges surrounding patient safety and device security arise from the connected nature of devices, the rapid pace of innovation[47], new product use cases[48,49], as well as the globalisation of the supply chain.[47]

Existing standards, including those listed in section 3.3 above, seek to address these challenges to patient safety and device security. They offer best practices that ensure quality and reduce risks such as unauthorised access to data and malfunctioning of these devices, which may, in turn, impact the broader healthcare ecosystem. As explored further in sections 4 and 5 below, improved patient safety requires ensuring both the safety and security of connected, intelligent medical devices, as the unintended operation of a device could result in patient harm.

Tension between device security and patient safety

However, there are also tensions between device security and patient safety, as highlighted by Halperin et al. in an article on the security and privacy for implantable medical devices (IMDs).[50] This could arise if the design of security measures interferes with the intended operation of the device, therefore causing patient harm.

For instance, if a manufacturer complies with BS EN ISO 27799, it would design a wearable medical device with strong encryption techniques. This is aimed at preventing unauthorised entities from accessing confidential patient data. However, it may prevent the detection of IMDs in the patient and timely access to patient information in emergencies, such as when a patient is unconscious and unable to grant authorisation. In another scenario, if there is a critical need to access the IMD, for instance to deactivate a malfunctioning IMD which is causing the medical condition, the stringent security measures could result in patient harm instead of ensuring patient safety. In another example, the authors highlight how the presence of robust security mechanisms may be a vector of denial of service (DoS) attacks, through repeated attempts by malicious entities to authenticate. This could affect device performance and, consequently, adversely impact patient safety.

There are several suggestions on how to resolve these tensions, including:

> Third-party governing access control[50]
> Introduce an intermediary. For instance, emergency teams could have external programmers to determine device manufacturer and patient's primary care facility, and for these parties to authorise access to medical devices.

Means to revoke unauthorised access[50]

The default setting would be open access, but any unauthorised access is revoked when detected. One proposed method of detecting unauthorised access was to have secondary alerts to patients when certain device functions are activated.

Secured on-device audit logs[50]

This would record modifications of device settings and data access. However, there is a need to balance this with device performance and potential DoS attacks by malicious entities.

Oath taking by various stakeholders[51]

Subjecting manufacturers and adopters of connected medical devices to an ethical oath of duty. This was proposed by the "I am The Cavalry" group, drawing reference from the Hippocratic Oath which all physicians have to take as a pledge to provide care in the best interest of patients. For the proposed Hippocratic Oath for Connected Medical Devices, there are five ethical principles which manufacturers, organisations and clinical end-users providing care through these devices should adhere to. This aims to build an ecosystem of secure medical devices, by favouring manufacturers who adhere to the Oath. It is believed that manufacturers can be held accountable to their commitments, as this information could be made available publicly (e.g. on manufacturers' websites).

In essence, to ensure connected medical devices are fit-for-purpose, it is crucial to recognise the trade-offs between security and safety, and determine the optimal balance based on the relative risks and vulnerabilities. While existing standards address individual components of connected and intelligent medical devices, there appears to be a challenge in terms of resolving possible tensions between different sets of applicable standards.

Global consensus standards

Different safety risks are present at various stages of the device supply chain.[47] In the world of connected and intelligent medical devices, where a compromised device "can cause significant disruption to the delivery of healthcare services"[52] and therefore impact patient safety, it is even more crucial than before to ensure the cybersecurity of these medical devices across the entire supply chain.

A key trend is the globalisation of the medical device supply chain. Global consensus standards are required to ensure consistency in the security of medical devices. However, there are several challenges. There are contextual factors which result in differing regulations imposed on connected and intelligent medical devices. In addition, there could be a varying interpretation of regulations and requirements, and possibly even different uses

of technical terminology. A study highlighted that different provinces in China had different standards applicable to medical devices and, therefore, encountered difficulties in supporting the convergence of standards across its provinces[47]. It can thus be deduced that achieving global consensus on standards would be even more complicated.

Given that international markets are important for the medical devices industry, the contextual factors surrounding standards may be perceived by some as a trade barrier[37]. Although standards essentially aim to serve the public interest by ensuring patient safety and product efficacy, the "fundamental differences in safety philosophy, the base of experience, or existing medical practices"[37] may lead to a bias towards locally-manufactured products.

Unlike traditional medical devices where data was mainly generated and viewed on a single device or customised research application, connected and intelligent medical devices are expected to interact with other medical devices and healthcare networks.[53] The need for interoperability across device manufacturers further highlights the importance of global consensus standards. There have been several suggestions on how these challenges may be addressed, such as the following:

Open standards and open-source medical devices[54]

This is seen as a means to avoid monopoly by certain technology of firms, seen in proprietary devices. This should improve expertise, promote collaboration with other regulatory authorities, enhance operational efficiency and offer access to new markets. Ultimately, such an open framework will benefit patients through improved access to safe and high-quality medical devices.

Promote cooperation between stakeholders[53]

The lack of interoperability between medical devices could have unintended consequences on patient safety. For example, a patient may be harmed if a medical device used for diagnostic purposes does not transmit accurate and readable information to another device used for the administering of medical treatment.

Currently, there are standards related to the areas of patient safety and data security. However, they apply to specific parts of the medical device ecosystem and there is a gap in a "blueprint" that will connect this "patchwork of standards".[53] Weininger et al explore various options to promote cooperation between manufacturers.[53] The authors recognised that there is a need for regulatory drivers to complement clinical needs. It was suggested that manufacturers could be mandated by regulations to allow electronic health record portability, with further guidance on the agreed intended use cases and data structure provided through standards. The provision of

financial incentives and support, in the form of providing vendor-neutral interoperability testing facilities, were also proposed to promote interoperable healthcare platforms.

As these efforts could be hindered by competing interests of different standards development organisations (SDOs), the cooperation between SDOs was also highlighted.[53] It was suggested that SDOs make use of blueprints or roadmaps to highlight the current state of safety and security management, explicitly state what needs to be developed and clearly define the role of various stakeholder groups in achieving the end goal of interoperability.

Trade-off between innovation and patient safety

The medical devices industry has benefitted from innovations which have helped to improve patient safety and quality of life.[47] Nevertheless, innovative technologies pose novel challenges to patient safety, as these risks may not be easily anticipated during the development stage of the product lifecycle.

Compared to other industries, recalling a medical device that is already placed on the market presents higher safety risks. For instance, where a faulty IMD is detected in the post-market phase, there are new risks if the patient must undergo additional procedures to retrieve the faulty device.[47]

In this context the role of standards is to ensure that the product has met safety requirements before commercialisation. However, it has also been argued that while standards are intended to promote better product quality, there are limitations on the extent to which this goal could be achieved. This is because manufacturers could perceive standards as an additional cost and they would only put in minimal effort to meet the standards, especially if these standards are voluntary[47]. The selection of lower-cost products as part of the medical devices supply chain could, therefore, result in a sub-optimal ecosystem, comprising minimum viable products rather than high-quality products[47].

Another safety issue brought about by technological advancement is the ease of producing counterfeit products, which may be designed almost identically to genuine products, making it difficult even for medical professionals to distinguish authentic and counterfeit products.[47] This results in additional risks to patient safety as these counterfeit products may not have met relevant safety standards. In this case, a different kind of standard (for instance, tamper-proof and unique product markings) may be required to distinguish between genuine and counterfeit products.

3.5. KEY FINDINGS

According to the existing literature, there are several key standardization gaps and challenges arising from the increased use of connected and intelligent devices.

- There is a need to understand the risks associated with these devices holistically, in order to obtain a balance between potentially conflicting requirements. Existing standards address specific components of these devices. However, there is an unresolved tension between different sets of standards which apply to a single medical device.
- Global consensus standards are increasingly important. However, there remain several barriers in achieving consensus. Connected and intelligent medical devices differ from traditional medical devices, in terms of their connectivity and interoperability with the broader healthcare ecosystem. Moreover, globalisation of this supply chain compounds the need to ensure that consistent standards are applied across the entire lifecycle. Nevertheless, various contextual factors impede achieving global consensus of standards.
- Innovative technologies may challenge the effectiveness of standards in ensuring patient safety and product quality, as "some safety hazards posed by complex new technologies may be difficult to anticipate during development and may not be realised until the device is actually in use" [47]. The current standards-making process may also result in an ecosystem of minimum viable processes or devices instead of high-quality ones.

Nevertheless, the complexity and challenges of various regulations and standards in the field of connected health should be viewed as an opportunity to provide conformity assessment tools and regulatory guidance.[18]

4 SAFETY

Research question: What are the challenges to the safety of connected and intelligent medical devices?

Overall, there is a significant number of studies on the safety of connected and intelligent medical devices. A significant portion of the literature provides an overview of the critical safety issues arising from such devices, and several works present the technical challenges posed by SaMD. Discussion of the main challenges to the safety of connected, intelligent medical devices revolves around human factors, evidence of efficacy, and cybersecurity, as well as privacy and data management. Importantly, connected and intelligent medical

devices are generally depicted as safety-critical cyber-physical systems. These systems integrate cyber elements (embedded sensors, computing components) with physical processes, the physical environment and human activities that include various safety-critical functions.

4.1. HUMAN FACTORS

The discussion of human factors centres around three main themes, covering usability and interpretability, user interactions and operational challenges of connected and intelligent medical devices.

Usability and interpretability

This sub-theme appears in most studies reviewed. It focuses on the difficulties that end-users may encounter in understanding and interpreting the results of connected and intelligent medical devices.[55,56] These challenges arise out of the high degree of complexity of connected and intelligent medical devices and the non-technical origin of end-users. End-users, in this context, include doctors, nurses, administrators and patients. One study indicates that the difficulties stem from the inability of users to conceptually model the information presented on the device's interface, and their limited understanding of the way the system works.[57]

Equally, Sujan et al. attributes this issue to the current regulatory framework.[58] In this case, an unintended consequence of the MDR is that manufacturers of connected intelligent devices given the responsibility of establishing acceptable levels of risk.[58] However, the study notes that manufacturers have limited control over how their devices are used in the end-use environment, and over compliance with safety-critical assumptions on aspects such as user training and device upkeep.[58]

On a similar note, where an incident involves a connected and intelligent device, Blandford et al., argues that the incident is classified as either a user error or a device error.[59] However, this simple attribution does not consider issues related to the appropriateness of the design, and the existence of a gap in the design, subsequent use and maintenance of software-based medical devices. Like other studies, it recognises that connected, intelligent medical devices may not be user-friendly.[49,57,59–61] It also recognises the challenges posed by the ability to effectively manage and regulate the post-market oversight of medical devices.

Concerning intelligent devices, the ease of use and interpretation also has implications for patient safety. In this context, the deployment of AI and ML applications for diagnosis raises concerns about the ability of end-users to understand how a neural network reaches its conclusions about a specific problem.[61–63] The use of deep learning to predict the likelihood

that a patient will suffer from a particular disease is an example of this. The problem is aggravated by the fact that it is rarely possible to interpret the layers of learned and non-linear features in AI applications because their meanings depend primarily on intricate interactions with the uninterpreted features of other layers.[61]

In addition, the literature discerns that the issues of usability and interpretability have broader implications. These include the inability of clinical end-users and patients to trust an algorithmic black box, which could lead to low uptake of these devices.[63–65] Moreover, uncertainties remain as to how clinical end-users can meet the GDPR's "right to explanation" for decisions made by AI-driven software and devices in healthcare.

User interactions

In general, manufacturers of connected, intelligent medical devices are expected to take into account the various ways in which potential users interact with their device.[55,57] However, devices may be used in ways and for purposes that were never intended by the manufacturer. Such use could potentially erode safety mechanisms built into the device.[59]

In a clinical setting, the use of devices for unintended purposes may be the result of workarounds, i.e. the use of other tools to achieve an objective when the right tool cannot be found. However, the implications of such workarounds in clinical environments have received limited attention in the literature. As it stands, critical safety issues can arise if the use of medical devices is misaligned with their intended purpose.[59] Hence, the ability to safely assume that a device is fit for use resides in the interaction between the end-user, the device and the use environment.

Operational challenges

Another sub-theme that emerged from the literature review is the operational challenges raised by the integration of connected, intelligent medical devices and software in healthcare systems. While it is generally acknowledged that utilising these devices could enhance patient safety and patient care, their deployment in a highly intensive and safety critical environment might be too overwhelming for hospital staff. Many staff are already overwhelmed by the increased demands. As a result, the incorporation of IoT in medical devices is setting new expectations for hospital staff without the organisational and financial support needed to facilitate this transition.[49,59,60,62]

Additionally, such technological advances are leading to increasingly complex and multifaceted errors, which must be conceptualised, critically analysed and mitigated through a robust oversight structure. These operational challenges could result in the emergence of new safety risks with implications for patient safety. Furthermore, issues pertaining to how

to incorporate algorithmic-driven devices and software into clinical workflows appear to be another operational challenge.[49,60,63]

Changing patient-clinician relationship

A central theme that has emerged in the literature focuses on the implications of the use of connected and intelligent medical devices on the patient-clinician relationship. Importantly, the deployment of these technologies raises the issue of trust, as the use of such devices could completely change the communication dynamics in the healthcare system.[61,66,67]

However, there is a divergence of opinion as to whether this would have negative or positive implications for patient safety and care. One study postulates that the introduction of AI-based medical devices and software could erode confidence in the healthcare system in the event of an error.[66] Other studies contend that it would allow physicians and hospital staff to refocus on communication and interaction with patients.[67–69]

4.2. EVIDENCE OF EFFICACY

Another key theme within the literature is evidence of efficacy. There is a consensus that connected, intelligent medical devices currently lack adequate evidence that demonstrates their efficacy.[58,60,62,70–74] This is generally believed to be a regulatory and standardization gap with grave implications for patient safety. This is because the deployment of these devices has the potential to introduce new safety risks that are unaccounted for by their manufacturers. In this context, inadequate evidence of efficacy is a critical issue that appears throughout the product's lifecycle.

It is recognised in the literature that the issue stems from the regulatory framework that delegates responsibility for determining the acceptable level of risk to manufacturers.[61,66,74] Yet, as noted above, manufacturers have limited control over how the device is used in its end-user environment. The complexity of safety assurance is compounded by the integration of various intelligent and connected devices and software in the final environment. Given this, the literature notes that the MDR neglects other subjects that are involved in the device use process in healthcare.[21,65,75] This is particularly critical for traceability – the allocation of accountability, and investigating errors related to the use of the device. In this context, in most healthcare settings, the user is a doctor who uses intelligent devices to make a diagnosis or therapeutic decisions. In this case, the physician's behaviour is covered by separate liability rules for medical errors. However, in the case of AI-based medical devices, there is a strong link between poor design of the device and what is traditionally classified as a user error, making the allocation of responsibility harder.

Additionally, the literature points to an evident tension between the clinical validation requirement of the MDR and the GDPR.[58,60,66,76] A crucial element of the MDR is the evidence-based approach to clinical validation, in conjunction with comprehensive post-market surveillance. Under the MDR, clinical validation must be based on a systematic analysis of clinical data that proves the efficacy of the devices. Post-marketing surveillance includes an evaluation of the entire chain of development, production and field application of the devices. To achieve these two objectives, comprehensive data collection and analysis is necessary to ensure robust evaluation process. However, the GDPR sets high restrictions on data collection. As a result, difficulties in data access create significant barriers to the implementation of an evidence-based approach to clinical validation and post-market surveillance of AI-based devices. Overall, this indicates a substantial discrepancy between the high requirements laid out within the MDR and the challenge regarding its practical implementation.

Hence, addressing clinical validation and post-market surveillance would require regulators and manufacturers to work together to develop a list of permissible alterations and changes that AI-based devices can use to adapt to new information in real time.[72,74,77,78] This should be in addition to integrated and periodic audits that use data from ongoing implementation to evaluate the results at a pre-determined point in time as part of a continual approval process. Further, clarification is pertinent to developing appropriate ways for the evolution of requirements and best practices.

On a similar note, algorithmic bias is an ethical concern arising from the lack of evidence of efficacy. Studies have shown that differences in model performance can have important consequences for the health of marginalized groups.[64,66,79] It can also exacerbate health inequalities and increase mistrust of medical institutions. The problem lies in the encoding of human biases in the training dataset that currently serve as a base for intelligent and connected medical devices and the development of their model.[79] As such, information asymmetry has serious implications for rectifying these problems early in the device development. For this reason, studies advocate a regulatory approach to algorithmic bias, with one study proposing that algorithmic bias should be regarded as a patient safety and quality improvement matter.[79] This regulatory approach would aim to prevent unintended harm and increase the delivery of healthcare services in a fair manner.

4.3. CYBERSECURITY, DATA PRIVACY AND MANAGEMENT

There appears to be a general conflation between safety and cybersecurity in the literature. Cybersecurity vulnerabilities are depicted as safety hazards with implications for privacy and confidentiality. This is due to the increasing connectivity of these devices with a majority of medical devices using Bluetooth, wi-fi, radiofrequency and other technologies to

communicate.[80,81] As explained in more detail in the section on cyber security below, the increasing connectivity of these devices may cause adversaries to exploit these networks to launch highly sophisticated cyber-attacks. . As medical devices become more dependent on information technology, the nature of the risks to patient safety is changing as security vulnerabilities can have an impact on the well-being of patients.

These problems are compounded by a lack of awareness of cybersecurity among end-users as well as manufacturers who do not follow a 'security by design' approach to ensure the integrity of their devices. Furthermore, clinical testing and validation of connected, intelligent medical devices address patient safety concerns directly. Consequently, any security vulnerabilities that do not result in physical harm could potentially be overlooked.[81–84] This is particularly concerning as the breach of a patient's right to privacy can also lead to other forms of harm, including reputational, financial and psychological harm.[81,85]

The GDPR is considered a step in the right direction. However, regarding its implementation, ambiguities and transparency problems remain.[86] For instance, questions on how data privacy and protection can be maintained without stifling innovation and research remain unanswered. Further, there appears to be no consensus regarding data sharing and storage, with these issues set to be exacerbated by the current innovation trends as a result of the COVID-19 pandemic.

4.4. KEY FINDINGS

Based on the literature review, several safety-critical issues have been identified.

- Connected and intelligent medical devices are giving rise to new security and safety risks. To mitigate them, it is pertinent that manufacturers apply a safety by design and security by design approach to the medical device development process.
- Connected, intelligent medical devices can be used in ways unintended and unaccounted for by manufacturers. These interactions could circumvent safety mechanisms that have been put in place.
- The embedding of AI and ML could result in changes to functionalities between the pre-market and the post-market phase. Hence, the functionality of an intelligent device is dynamic and needs to be accounted for by regulations and standards
- Usability and interpretability issues require connected, intelligent medical device manufacturers to account for cognitive ergonomics and user experience at the design stage, to enable effective interaction between device and end-user.
- The deployment of connected intelligent medical devices in healthcare transforms the relationships between devices, clinicians and patients.

- Connected, intelligent medical devices lack adequate evidence of efficacy, which has grave implications for patient safety. In this context, there are evident tensions between the MDR and the GDPR with regards to data access.
- There appears to be a tension between the utility of connected, intelligent medical devices and patient safety.

5 SECURITY

Research question: What are the challenges to the security of connected, intelligent medical devices across the supply chain?

Overall, the literature on the cybersecurity of connected, intelligent medical devices is vast. While there are some general studies, the majority focuses on challenges and technical solutions for securing connected and intelligent medical devices. Fewer studies concentrate on the human aspects involved in ensuring the security and safety of those devices. The following section is divided into challenges (5.1) and solutions (5.2).

5.1. CYBERSECURITY CHALLENGES OF CONNECTED MEDICAL DEVICES

Cybersecurity attacks

The literature recognises that most cybersecurity vulnerabilities of medical devices arise from the connectivity and wireless communications, which can be interfered by hackers.[87] For instance, a cardiac implantable electronic device that communicates with hospital networks, especially via the internet, is vulnerable to attackers who could interfere with the communications, eavesdrop and gain access to these devices (Figure 2).

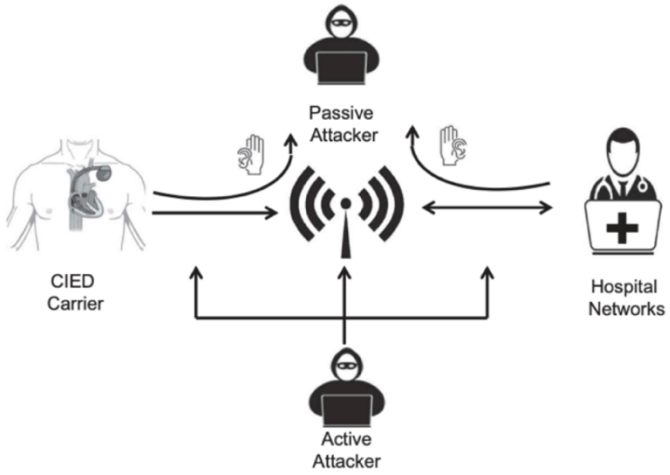


Figure 2: Passive interference and active attacks on medical device communications within a hospital network[87]

Such attacks can be classified into three categories, depending on how advanced they are:[88]

- Simple attacks are singular attacks such as DoS, eavesdropping or battery depletion attacks.
- Advanced attacks are a sequenced combination of simple attacks.
- Advanced complex attacks combine simple attacks while also taking anti-forensic action to cover up digital traces of an attack.

Several studies successfully demonstrated vulnerabilities in medical devices by simulating attacks through ethical hacking and penetration testing.[89–92] Numerous papers in this field refer to the pioneering study by Halperin et al., which demonstrated that medical devices could be easily hackable.[89] They demonstrate how the vulnerabilities arising from the embedded connectivity can put patient safety and privacy at risk. Vulnerabilities in Interoperable medical devices, devices that are able to seamlessly exchange data with other devices, can act as gateways that can compromise the whole IT network[93,94]

There are two types of attacks – active and passive. One study simulated an active DoS attack through an injection of signals via electromagnetic signals at high-frequency.[91,92] This prevents any wireless communication with the device because it is drowned with high-frequency signals. Thus, the availability to communicate with other devices is compromised and the device would be unresponsive and restricted in its functionality.

The other two studies followed a passive attack simulation that usually involves eavesdropping, which is the illicit interference of communication signals.[89,90,92] Here, a hacker may interfere with communication protocols between a medical device and a hospital network (Figure 2). If these protocols are not encrypted, the hacker can openly view the transmitted information. If the information is encrypted, meaning encoded information, then a hacker usually cannot immediately decipher it. However, encrypted protocols can be reverse-engineered. This allows a hacker to determine command patterns. With this information, an attacker can acquire valuable intelligence on device vulnerabilities, processes and patient data. This could eventually lead to the attacker gaining access to the device.

As a result, the confidentiality, availability, integrity of the device is compromised, which are key requirements needed to ensure that a device is secure. This can have severe consequences to patients. With device access, a hacker could launch an attack, such as a replay attack where a command to set off a pacemaker is repeatedly sent. Besides potentially killing a patient, these commands can deplete the battery of a medical device. If the battery is empty, patients would not have access to the lifesaving functionality of pacemakers and an operation would be necessary to replace the battery.

Medical devices using AI can exacerbate these cybersecurity vulnerabilities of connected medical devices by multiplying risks.[95] Successful AI hinges upon the integrity of data, in the form of large and high-quality applicable data sets. However, if hackers manage to obtain access and alter data that an AI relies upon, the AI algorithm will reinforce this modification by deriving a faulty conclusion and providing incorrect instructions to users. This could have fatal consequences for patients. For instance, if an AI-powered insulin pump derives a faulty conclusion from altered blood sugar data to inject more insulin, the overdose may kill a patient.[92]

Nevertheless, despite reoccurring vulnerabilities in "hundreds of thousands" connected and intelligent implantable medical devices, "no reports of patient harm have ever been recorded".[96] However, the literature suggests that the barriers to launching simple attacks on connected medical devices are low.[89–92] Affordable and widely available commercial equipment can be acquired by an inexperienced attacker to launch attacks despite not having physical proximity or access to a device.[90]

Considered further below are technical solutions explored in the literature that aim to mitigate these vulnerabilities. However, these solutions create challenges in themselves because they usually involve various trade-offs.[97] There are three common ones. Firstly, stringent security measures can make it difficult to access devices. This is particularly critical in emergencies where patients are unconscious and medical staff do not have credentials to gain access. Moreover, ensuring security whilst maintaining minimal energy consumption is problematic. Strong security solutions tend to be complex and energy-consuming. For example, pacemakers that use encryption for communications would have to undertake decryption activities that are energy depleting. This would be problematic since surgeries would be more frequent to replace pacemaker batteries. Finally, there is security against human-oriented design which is explored in the section under human preferences.

Human factors

Stakeholder interactions and communications

Stakeholder interactions are a major theme within the literature. Studies underline that there is a complex web of stakeholder dynamics (Figure 3).[48,96,98]

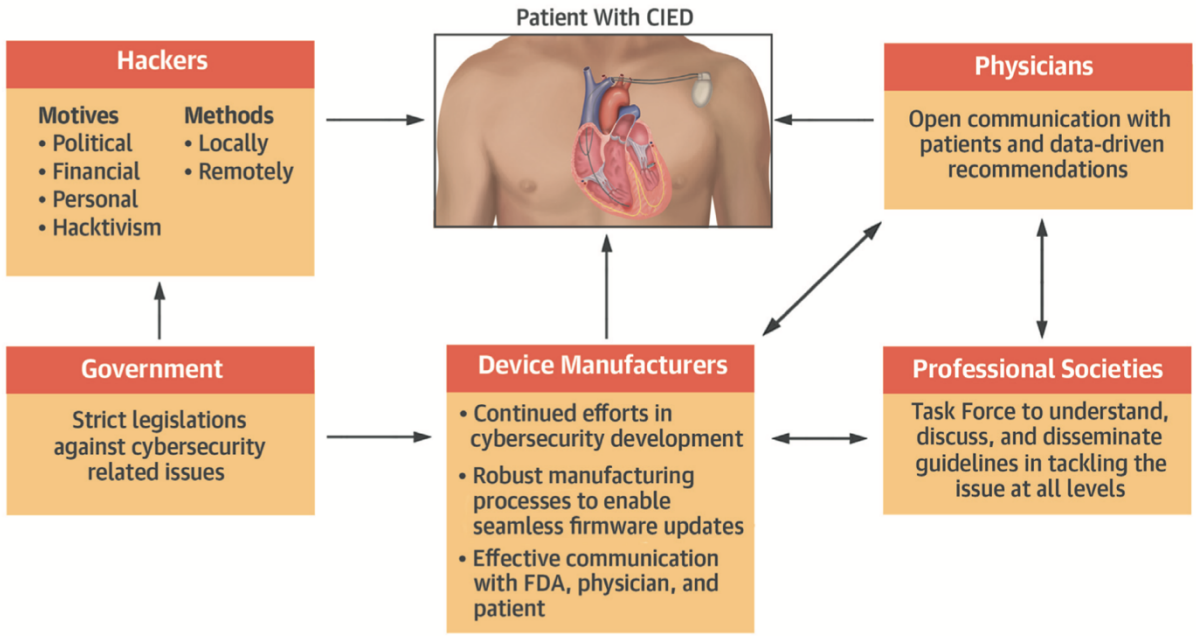


Figure 3: Stakeholder interactions within the medical device cybersecurity area[98]

To streamline these communication process, in 2017, the Heart Rhythm Society developed communication strategies with a range of stakeholders, including the US FDA.[48] It includes a recommended communication chain between stakeholders that outline a patient-centred communication process to address any medical device security vulnerabilities that arise and affect the public (Figure 4).

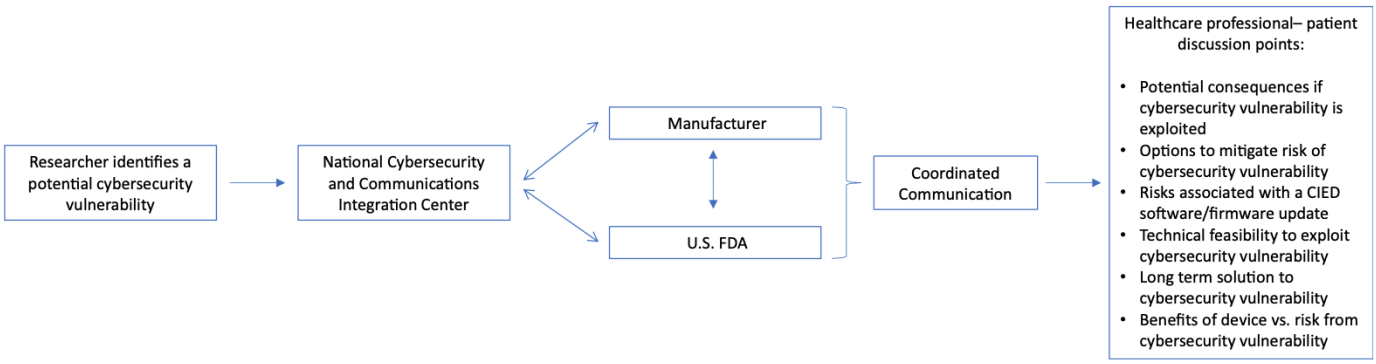


Figure 4: Medical device cybersecurity vulnerability notification chain[48]

The main communication focus was on patients.[48] Patients may experience mental distress depending on the timing and the method of information delivery of a vulnerability. This could even lead to a public hysteria, for instance if a hacker releases information via social media on a device security vulnerability.[48]

It is recommended that patients and healthcare professionals have open and regular communications to mitigate such a threat.[48] Such a communication style is essential to ensure that patients trust connected and intelligent medical devices.[99] This is key for their

security and safety, and is especially important when updates are necessary to patch security vulnerabilities. For instance, according to one study, a pacemaker manufacturer estimated that a security update process presented a 0.003% risk of complete loss of function.[96] While this risk was considered low, it still affected patient choice and discouraged some patients from updating their device.[100] Various factors appear to influence the openness of a patient to update their device, such as age, gender, residence location and the novelty of the device.[100] In-person communications between medical staff and patients through an open conversation on the potential consequences and dangers of security vulnerabilities and benefits of updates are recommended to address such concerns (Figure 4).

Overall, the literature has demonstrated that strategic stakeholder collaboration is essential to maximise device security and patient safety.

Human preferences

Another critical research strand within the literature examines the human factors regarding various physical cybersecurity protection mechanisms. A key study by Denning et al. advocates a human-oriented design for access and protection mechanisms of implantable medical devices.[101] The research emphasised that the individuality of each human needs to be recognised within security mechanisms. This is because not every security approach will be suitable for all patients.

While technically capable, the desirability of access methods may depend on various human values and preferences. These include privacy, usability, physical or mental concerns, self-image, perceived security and freedom from undesirable cultural and historical connotations.[101] For instance, some patients may feel uncomfortable having a visible QR code tattoo that allows for vital access to a medical device during emergency situations.

Therefore, manufacturers need to consider human factors, such as patients' values and preferences and test the different access methods while designing the security mechanisms of medical devices. This should occur from the earliest stage of the medical device lifecycle to secure them in a way that fulfils technical requirements and respects patients' needs and values.

5.2. SOLUTIONS AND MITIGATION PATHS

Most of the literature focuses on the technical ways of securing connected medical devices and mitigating their cybersecurity vulnerabilities. There is a wide range of techniques to achieve this, which these can be split into pre-market and post-market considerations.

Pre-market protection

Physical-layer-security methods focus on the physical aspects of protecting medical devices against intrusion.[102] Here, the protection of communication signals of connected medical devices is the key aspect. By using a certain communication frequency, passive attacks such as eavesdropping can be mitigated. For instance, one study calculated that, with the medical implant communication systems frequency band, a connected cardiac pacemaker has a one in a billion chance of being successfully eavesdropped.[102]

Authentication and access management are also crucial protection mechanisms explored in the literature. These types of solutions tend to be frequently based on biometrical authentication, such as heart signals.[103] They are usually combined with other secure access mechanisms such as radiofrequency identification to achieve a secure authentication.[97]

Software systems that protect a connected medical device are another crucial theme in the literature. There are multiple ways software is used to protect devices, such as software verification solutions that continuously review and test the software code to identify any vulnerabilities and suggest suitable updates.[104]

However, within the literature, most software systems focus on monitoring and anomaly detection.[105–109] These systems detect irregular or unexpected activities. Normally, this is achieved by identifying deviations from a norm of expected events. For instance, if patient data is accessed outside of an expected location or time, this would be notified.

There are various methods to detect anomalies, such as time-based methods.[108,109] This method compares time deviations to execution times ranging from best to worst-case times. If a time to execute a command is outside of this time range, an anomaly would be detected.

Another method identified in the literature involves comparing actual events to a database of expected events.[105–107] Such a database could include historical data of patients, potential threat scenarios or a history of commands. Such a sanity check aims to limit unusual activity.

Importantly, while AI can amplify cybersecurity vulnerabilities, it can also be part of the solution.[95] AI may be able to effectively execute most of these protection mechanisms, such as monitoring and anomaly detection. For example, an AI algorithm may be programmed to identify any dataset changes or unauthorised accesses in real-time.

Risk management approaches usually inform these software systems. The depicted framework shows an example of a model that aims to protect a medical device by using a dynamic risk and automated threat management method (Figure 5).[110]

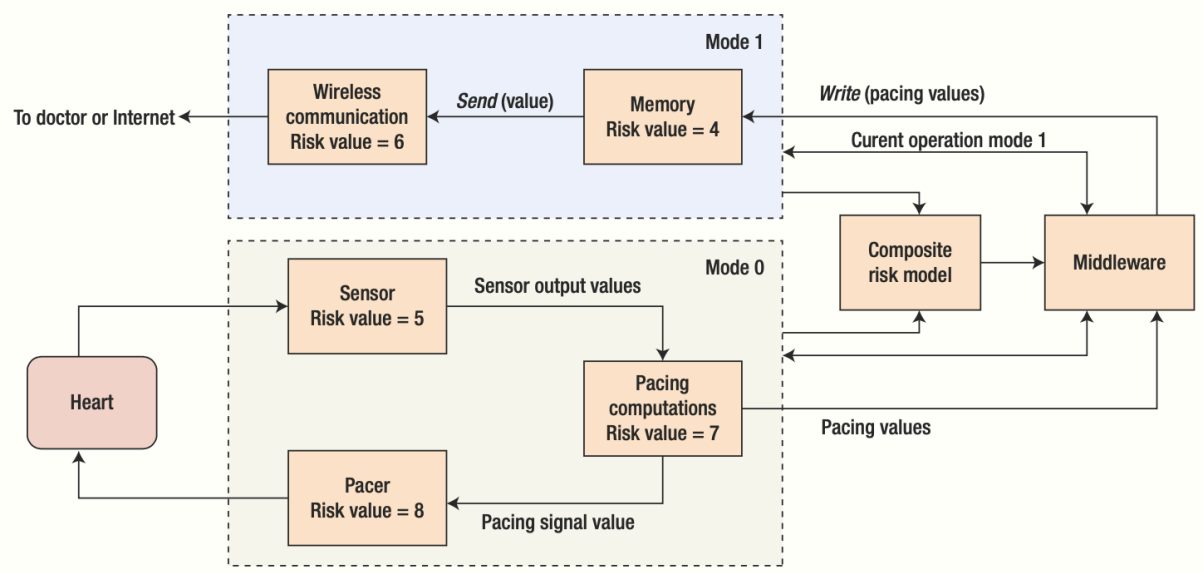


Figure 5: Example of a connected pacemaker risk model[110]

Post-market

At the post-market lifecycle stage of connected medical devices, forensics and reuse are essential to ensure safety and security. One study examines the post-mortem examinations and reviews the ethical data considerations of the reuse of connected medical devices.[88] The proposed digital system aims to support the integrity of devices by protecting them against advanced complex attacks with anti-forensic measures. The intelligence from such systems aims to inform stakeholder decision-making. For instance, despite anti-forensic measures, through an attack reconstruction and incident analysis, a regulator could determine whether a cybersecurity attack is behind a faulty device that caused a death. After completion of the post-mortem analysis, ethical and data considerations on the recycling of medical devices are critical.

Moreover, to achieve secure devices, manufacturers need to include security measures from the beginning of the medical device lifecycle, as reflected in the security by design approach. However, a study analysing the US FDA's product summaries for regulated SaMD in the US found that only 2.13% mentioned cybersecurity.[111] This may suggest lack of awareness of security measures or that security principles tend to be neglected in the medical device lifecycle.

However, security considerations from the beginning of the medical device lifecycle are crucial to guarantee a secure and safe medical device and to establishes trust between patients and the device. This security by design approach is one of the core principles in the recently published IMDRF and MCGM cybersecurity guidance papers.[112,113] Both offer key principles and practices to ensure the cybersecurity of medical devices, pre-market and post-market considerations and a brief overview of the standards landscape.

5.3. KEY FINDINGS

Overall, the main points emerging from the literature on cybersecurity of connected, medical devices are:

- Wireless communications of connected and smart medical devices expose them to cybersecurity vulnerabilities and can act as gateways to the healthcare network.
- Intelligent medical devices, such as AI can amplify cybersecurity vulnerabilities.
- There are low barriers to hack connected medical devices.
- There is patient inertia to medical device security updates.
- New cybersecurity threats are constantly emerging.
- There are numerous techniques that can help address these emerging vulnerabilities, both at the pre-market and post-market stage. As the literature highlights, it is crucial that manufacturers consider cybersecurity from the early stages of the medical device lifecycle and apply security by design principles.

6 INTERACTIONS BETWEEN SOFTWARE AND THE IT ENVIRONMENT

In general, there is minimal literature dealing with the risks posed by possible negative interactions between software-driven medical devices and the IT environment, and little guidance from public authorities on this topic. In addition to the literature dealing with the topic being limited, there is a lack of consensus on the key terms such as 'IT environment' or 'negative interactions', as well as a clearly attributed disciplinary area that provides a conceptual underpinning to the issue under review.

Due to the minimal literature, this research question will be explored further through horizon scanning and interviews.

6.1. REQUIREMENTS FOR MANUFACTURERS

To make the risks posed by medical device software more explicit, Annex I of the MDR sets out specific requirements regarding the manufacturing and designing of devices. Section 14.2(d) of Annex I states that "devices shall be designed and manufactured in such a way as to eliminate or reduce as far as possible… the risks associated with the possible negative interaction between the software and the IT environment in which it operates and interacts."

This requirement has been first explicitly introduced in the MDR and IVDR and, so far, little commentary has been provided by public authorities. The MDCG published the *Guidance on Cybersecurity for medical devices*.[112] However, it does not refer to the IT environment, but the operating environment, which is defined as "the sum of IT assets (software, hardware,

network components) within which the medical device operates and with which the medical device interacts."[112] This divergence from the wording in the legislation in itself highlights the absence of homogenous terminology. Importantly, the document frames negative interactions as a cybersecurity issue. At the same time, the broad definition of the operating environment indicates that negative interactions concern a broader set of issues, not only security.

It is acknowledged within the limited literature that address these risk *implicitly,* that medical devices are becoming increasingly dependent on software for improved patient care and to create efficiencies in the healthcare system.[59,114,115] Tied to this by-line is the view that more needs to be done to ensure safe interactions between software-driven medical devices and information systems and sources.[116,117] This includes, for example, interoperability issues between the hospital information systems and sources as well as issues that arise when the device has wireless connectivity.[118–121] In addition, it also recognises the need for manufacturers to consider various user interaction scenarios – both positive and negative ones. This would enable manufacturers to address issues of incompatibility and human errors at the outset.

Hence, addressing these risks requires connected device manufacturers to consider interactions with the IT environment where the software is used, and not only the integrity of the device[55,122,123]. This is primarily due to the fact that software deployment and subsequent use add complexity to the design of devices.[123–125] Ensuring the continued safety of medical device software requires manufacturers to take into account defects or deficiencies that could potentially create new hazards.[118,126,127] The key recommendations identified within the literature centre around the importance of standards in ensuring the safety and effectiveness of medical device software as well as regulatory policies that mandate incorporating best practices and safety guidelines to mitigate these interactions.[114,116,124,128]

6.2. POSSIBLE NEGATIVE INTERACTIONS

In the limited literature, three key types of negative interactions between the IT environment and software have been identified. They have been linked to cybersecurity, human-computer interactions or usability issues, with a significant focus on human factors.

Information source interactions

An emerging risk specific to connected, intelligent medical devices centres around possible negative interactions between software and information sources. This risk is reflective of a broader trend – increased deployment of varied software, greater connectivity, greater interdependence and more data are shaping many aspects of medical device development.

This innovation, centred around connected and intelligent medical devices, brings new challenges, leading to the emergence of new safety and cybersecurity risks that were not originally considered by manufacturers. Traditionally, medical device software was connected to an isolated network that consisted of proprietary technologies, which were exclusively managed by the supplier of the medical device.[55,126] However, the technical expertise required for various components of connected, intelligent medical devices have created a fragmented medical device innovation ecosystem. As such, the issue of incompatibility with various systems and information sources with no single manufacturer requires an understanding of how incorporating a medical device into its IT environment may introduce additional safety and security risks.[114,121,129]

At a microscopic level, as many medical devices are now Internet-enabled, data storage through the cloud or servers requires manufacturers to ensure the interoperability of their devices to the end-use environment such as the hospital IT environment or in the context of a smart patient home.[116,124,126,127] In addition, it requires an understanding of how connected and intelligent medical devices interact with other devices or products, and ensuring that these interactions are undertaken in a non-negative manner.

User interactions

Connected, intelligent software leads to a high degree of complexity, which is further deepened by the characteristics of the medical device field. In this context, human error is linked to the non-technical origin of most users, including doctors, nurses, administrators and patients.[116,117,123,130] As a result of these complexities, the literature generally emphasises that manufacturers need to consider various forms of user interactions with medical software from the design stage.

To guarantee safety by design, manufacturers must, therefore, identify, understand, control and prevent failures that result in risk when humans use these technologies. This can be undertaken through the application of relevant standards on medical software, which provide a risk management framework and help account for various risks.[119,123,131] In addition, recommended activities include scenario analysis for critical evaluation of potential use errors and the application of usability engineering methods in medical device design and development.[123]

Hardware interactions

Another possible negative interaction stems from malfunctioning of the interface between hardware and software in the connected, intelligent medical device.[121,123,125,132] This is typically as basic as incorrect plugs on the devices power cord to the implications of hardware failure on software in the device. In addition, literature centred around this interaction also considers the impact of human errors.

Addressing human errors and hardware-software interactions primarily centres on understanding usability in practice. This is because devices may be poorly designed for the way the user interacts with this device. In some cases, devices may be utilised in ways that they were never intended to be used.[120] Hence, it is generally indicated that mitigating this interaction focuses on ensuring that manufacturers align the device design with all possible use scenarios. This could be undertaken with the utilisation of interaction design testing in the development of medical devices and SaMD. [119,123,124]

6.3. KEY FINDINGS

- Negative interactions between software-driven medical devices and their IT environment often derive from user interactions.
- Other negative interactions also arise from hardware-software interactions and medical device-information source interactions.

7 INNOVATION

Research question: What are the main trends and innovations emerging in the field of connected, intelligent medical devices?

As the medical device industry is becoming increasingly digitised, innovation accelerates and new capabilities, products and business models emerge. The industry is characterised by heterogeneity, and covers a wide range of products and technologies; ranging from nanotechnology to engineered cells and more traditional devices such as bandages.[133] In turn, products are used and deployed in a variety of places such as private homes and hospitals.[134] The concept of innovation captures both the development of new products as well as modifications to existing devices. The literature on innovation can be found in multiple disciplines, ranging from healthcare and computer science to business administration and finance, reflecting a highly interdisciplinary topic. The innovation ecosystem consists of investors, innovation catalysts such as start-ups and SMEs, regulators, hospitals and patients.[135]

7.1. INNOVATION DRIVERS

Small and medium-sized enterprises

A central theme in the literature is the importance of SMEs and start-ups, with technological innovation being dependent on entrepreneurial initiative and innovators taking risks.[136] Indeed, the global medical device industry is diverse, and characterised by a large number of small and high-technology firms, with a wide range of products.[137] Cooperation with other organisations is seen as crucial in helping SMEs successfully innovate due to the complexity of products, extensive resource requirements and the length of the development process.[138,139] The shape and acceleration of the product lifecycle and innovation within firms are influenced by factors such as the advantages of new products over the existing ones, for instance regarding costs, commercial attractiveness, intellectual property, and barriers to entry.[140]

Technology

The second key innovation driver identified in the literature concerns technology. It is highlighted that information technology remains a key driver of innovation in healthcare.[137,141] The direction of technological innovation is driven by a complex interplay of supply and demand-side factors.[142] However, it is important to note that the sector remains patient-driven rather than technology-driven and technologies that address a specific patient need to be adopted and last in the long run.[135] The use of advanced technologies in the medical device industry, such as AI is increasing, as reflected in recent literature.[31,143]

Overall, the innovation process is not linear, but it is iterative and driven by the convergence of various disciplines.[144] By combining cutting-edge academic research in various fields as well as knowledge from the healthcare industry and medical device manufacturers, new and innovative theories and technologies emerge that can improve device functionality.

7.2. EMERGING TRENDS

Advanced technologies

The literature recognises that the field of medical devices is quickly evolving, fuelled by the rise of digital technologies. There is an extensive body of literature on the use of advanced technologies such as AI, suggesting that these technologies will play a crucial role in the products of tomorrow.[25] Other trends include cross-over collaboration with other industries, such as integrating medical devices with software apps or developing wellness wearable devices to detect depression. Recent developments and trends include wearables as a tool for more personalised healthcare.[145,146] Change is also driven by AI, self-tests and health-monitoring, illness detection and clinical decision support system – reflecting the heterogeneous nature of the medical device industry.[137]

Personalised care

A general trend is an increase in personalised care and portability. As the healthcare industry is moving further towards personalised care, more advanced monitors, sensors, and wearables are released to market as they offer the possibility for healthcare monitoring, personalised treatment and early diagnosis. These products are geared toward a consumer-driven model for health care, enabling patients to be more independent of their physician.[147] These devices cover a wide range of purposes and functionalities, including fitness devices, monitoring devices, or wearable patch physiological monitoring devices. Further, some literature exists in the area of using monitors and more advanced devices for monitoring to aid sleep disorders and elderly care as a result of an ageing population.

Although the literature highlights a range of important emerging trends, it also has important limitations due to the fast pace of innovation in the field. As a result, this project also explores the topic of emerging trends through other research methods, especially horizon scanning and interviews.

7.3. KEY CHALLENGES

The healthcare industry: a highly regulated arena

The medical device industry is highly regulated. The influences and limits of national and international regulations add complexity to the innovation cycle. The literature suggests that although the medical practice is changing rapidly due to digitisation, the preference is remains towards the status quo.[148]

Medical device manufacturers need more resources and capital to be able to sustain such a capital-intensive business and rigorous processes. As noted, SMEs are crucial for innovation and product development in the field. However, they often lack resources, which creates a challenge for their innovation journey.[137] Regulations often add to this burden by requiring more technical expertise to comply. While a new device may have improved capabilities, proving safety and efficacy to ensure regulatory compliance remains a challenging and costly process for firms, especially smaller firms. Importantly, the process also takes a long time. The average time to develop a medical device varies from one to two years for incremental devices and up to seven years for more complicated and advanced devices, depending on the risk class and classification.[137] While technology lifecycles are shorter than pharmaceutical lifecycles, because technological innovation is structured around iterative processes and often involves smaller improvements to existing products[119], this is a significant time requirement for newly established firms with limited resources.

Thus, innovation in medical devices and increased deployment of advanced technologies requires a regulatory system that accepts quick iteration, as it is difficult to predict how

devices and technologies will be used when placed on the market. Thus, companies need to be able to make adjustments fast, which is hard to balance with lengthy regulatory processes.

Commercialisation and access to funding

Common innovation challenges identified in the literature include lack of funding, identifying product-market fit, customer acquisition, meeting regulatory demands, competitive advantages, business strategy, and commercialisation of research. Other challenges involve determining what the patient or the clinician want, cost of research, funding, and the requirement to show improvements to care in order to be adopted by health services.[142]

To successfully commercialise and develop new products, large amounts of capital are needed. As capital is crucial for development and growth, the amount of capital in the healthcare system indicates what type of innovation is supported, and to what extent.[149] As medical devices operate in high risk-arenas with many uncertainties, raising enough funding can be complicated. The commercialisation of emerging technological innovations for medical devices requires time and these lengthy processes can potentially prevent market entrance. These processes increase the amount of resources and investment required for a successful product launch. [137]

Assessing the value of innovative high-risk devices

Access to health technologies, including medical devices, is a critical issue for both developed and emerging economies. For hospitals and other organisations, making evidence-based choices about what technologies should be available on the market is a complex task.

One of the common frameworks for informing such decisions is the health technology assessment.[150] The adoption of new medical devices can sometimes be limited by the existence of published evidence and thus making any assessment more complex.[151] Under this framework, costs and benefits of new technologies are evaluated using health-economic criteria to assess which technology is the most suitable given a clinical scenario. New products need to meet certain evidence requirements and fulfil criteria, such as being more cost-efficient than other alternatives. As such, it is important for innovators and organisations to ensure their products meet such evidence-criteria for their products to be adopted. Technology adoption tends to be less controversial when there is a well-defined clinical need, and it is hard to balance user needs with some adoption requirements.[151]

7.4. KEY FINDINGS

- Strict regulatory requirements create high barriers to entry and constraints on companies. They require longer innovation cycles, more capital, expertise and resources.
- SMEs and entrepreneurs are crucial in the development of innovative products but are easily constrained by regulatory burdens.
- The literature strongly indicates that advanced technologies such as AI will drive innovation in the field. Other key drivers include regulatory developments, research, and expanding financial investments.
- Importantly, innovation is an iterative process, which is driven by patient and healthcare needs.

8 CONCLUSION

Several main themes are emerging from the review of the literature on the regulatory and standardization challenges of connected medical devices.

Overall, the MDR/IVDR framework provides for an improved, more comprehensive oversight of digital medical devices compared to the MDD/IVDD framework, especially because of the increased focus on software. However, important shortcomings persist. The literature suggests that the regulatory frameworks were not designed with connected and intelligent devices in mind and they are failing to keep up with innovation. This leads to the emergence of regulatory gaps, evident, for instance, around AI and wearable devices. Moreover, the MDR/IVDR framework does not account for broad changes occurring in the medical field, such as the changing relationships between devices, clinicians and patients. Given the pace of technological change, it is likely that further regulatory gaps and grey areas will emerge, with a risk to patient safety.

Similarly, there are some evident standardization gaps. The disparate sets of existing standards, each addressing specific components of connected and intelligent medical devices, may result in conflicting requirements for device manufacturers. Moreover, innovative technologies may create new safety hazards that may not be anticipated during the standards-setting process. This could, in turn, limit the effectiveness of standards in ensuring patient safety and product quality. With the globalisation of the supply chain, global consensus standards will be increasingly important in managing risks to patient safety and device security across the lifecycle of medical devices.

It is clear from the literature that although connected, intelligent devices promise important benefits, the deployment of these devices is creating new safety risks and challenges. They emerge, for instance, from the new ways in which these devices are used and their increasingly patient-centric nature. In addition, the literature highlights challenges specific to intelligent devices, for instance, around evidence of effectiveness – an area which highlights the tensions between the GDPR and the requirements imposed by the MDR. Studies also underline the challenges currently facing the healthcare system, including the lack of sufficient infrastructure to ensure the safe deployment of these devices, the skills gap that places a heavy burden on clinical end-users, and the challenges associated with the use of these devices. Overall, it is necessary for manufacturers to account for these risks throughout the device lifecycle.

The embedded connectivity and wireless communications of medical devices also introduce security vulnerabilities. As a result, these devices can act as gateways for hackers to the broader healthcare network with severe risks to patient safety. There appear to be low

barriers for hackers to take advantage of these vulnerabilities. Risk and access management, physical-layer security and software solutions are at the core to mitigate these vulnerabilities. Moreover, while embedded intelligence can amplify security vulnerabilities, AI also appears as an emerging solution to protect against attacks. However, technical solutions are not sufficient to ensure safe and secure devices. Human factors, such as a human-oriented design of security mechanisms and patient communications, need to be considered by stakeholders. Inertia surrounding patients' medical device security updates seems to be particularly challenging. Additionally, strategic stakeholder collaboration is essential to maximise device security and patient safety.

The networked nature of connected, intelligent medical devices also makes them vulnerable to negative interactions between software and the IT. These negative interactions result from interactions between users, between devices and information sources, and between hardware and software. They have potentially negative implications for patient safety. They are further exacerbated by the increasing connectivity of networks and systems and the growing use of the cloud in healthcare. Moreover, the non-technical nature of end-users makes it particularly difficult for manufacturers to account for all possible ways in which users interact with their devices.

Technological change will continue to play an important role in driving innovation in the field, by creating new products and use cases, as well as by adding capabilities into existing devices. Importantly, SMEs and entrepreneurs play a crucial role in the innovation landscape. However, extensive regulatory burdens in the healthcare industry create challenges for smaller companies with limited resources, making it harder to commercialise. The uncertainties related to the innovation cycle, ranging from getting regulatory approval, finding product-market fit, to ensuring safety and security, can cause further difficulties in raising enough capital and thus be able to go through the lifecycle. While there are numerous challenges for innovation in the industry, the field is still characterised by a rich ecosystem of products and devices, and new emerging trends include increased personalised monitoring, new niche devices, and advanced technologies such as artificial intelligence.

REFERENCES

1. Melvin T, Torre M. New medical device regulations: the regulator's view. EFORT Open Reviews. 2019 Jun;4(6):351–6.

2. European Commission. New EU rules on medical devices to enhance patient safety and modernise public health [Internet]. 2017 [cited 2020 Jun 6]. Available from: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_847

3. European Commission. Medical Devices - Sector [Internet]. [cited 2020 Jul 6]. Available from: https://ec.europa.eu/health/md_sector/overview_en#new_regulations

4. European Commission. Communication from the Commission on safe, effective and innovative medical devices and in vitro diagnostic medical devices for the benefit of patients, consumers and healthcare professionals. [Internet]. European Commission; 2012. Available from: https://ec.europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-540-EN-F1-1.Pdf

5. Vasiljeva K, van Duren B, Pandit H. Changing Device Regulations in the European Union: Impact on Research, Innovation and Clinical Practice. Indian Journal of Orthopaedics. 2020;54:123–9.

6. De Maria C, Di Pietro L, Díaz Lantada A, Madete J, Makobore PN, Mridha M, et al. Safe innovation: On medical device legislation in Europe and Africa. Health Policy and Technology. 2018 Jun;7(2):156–65.

7. Schönberger M, Hoffstetter M. Regulations for Medical Devices. In: Emerging Trends in Medical Plastic Engineering and Manufacturing [Internet]. Elsevier; 2016 [cited 2020 Aug 15]. p. 19–64. Available from: https://linkinghub.elsevier.com/retrieve/pii/B9780323370233000026

8. Jeary T, Schulze K, Restuccia D. What medical writers need to know about regulatory approval of mobile health and digital healthcare devices. Medical Writing. 2019 Dec;28(4).

9. Vila Wagner M, Schanze T. Comparison of approval procedures for medical devices in Europe and the USA. Current Directions in Biomedical Engineering. 2019 Sep 1;5(1):605–8.

10. Aronson JK, Heneghan C, Ferner RE. Medical Devices: Definition, Classification, and Regulatory Implications. Drug Saf. 2020 Feb;43(2):83–93.

11. Burrows A. Regulatory challenges for Software as Medical Device (SaMD) and AI. Insights from six industry insiders [Internet]. InformaConnect. 2020 [cited 2020 Jul 7]. Available from: https://informaconnect.com/regulatory-challenges-software-medical-device-ai/

12. Jiang N, Mück JE, Yetisen AK. The Regulation of Wearable Medical Devices. Trends in Biotechnology. 2020 Feb;38(2):129–33.

13. Ordish J, Murfet H, Hall A. Algorithms as medical devices. Cambridge, UK: PHG Foundation; 2019 Sep.

14. Quinn P. The EU commission's risky choice for a non-risk based strategy on assessment of medical devices. Computer Law & Security Review. 2017 Jun;33(3):361–70.

15. IMDRF Software as a Medical Device Working Group. 'Software as a Medical Device': Possible Framework for Risk Categorization and Corresponding Considerations [Internet]. 2014. Available from: http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf

16. European Commission. Medical devices: Guidance document. Qualification and Classification of stand alone software [Internet]. MEDDEV 2.1/6 Jun, 2016. Available from: http://ec.europa.eu/DocsRoom/documents/17921/attachments/1/translations

17. Migliore A. On the new regulation of medical devices in Europe. Expert Review of Medical Devices. 2017 Dec 2;14(12):921–3.

18. Becker K, Lipprandt M, Röhrig R, Neumuth T. Digital health – Software as a medical device in focus of the medical device regulation (MDR). it - Information Technology. 2019 Oct 25;61(5–6):211–8.

19. Medical Device Coordination Group. Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR [Internet]. 2019 [cited 2020 Jun 7]. Available from: https://ec.europa.eu/docsroom/documents/37581

20. Gordon WJ, Stern AD. Challenges and opportunities in software-driven medical devices. Nat Biomed Eng. 2019 Jul;3(7):493–7.

21. Kiseleva A. AI as a Medical Device: Is it Enough to Ensure Performance Transparency and Accountability? European Pharmaceutical Law Review. 2020;4(1):5–16.

22. Le D-N, Le CV, Tromp JG, Nguyen NG, editors. Emerging technologies for health and medicine: virtual reality, augmented reality, artificial intelligence, internet of things, robotics, industry 4.0. Hoboken, New Jersey : Salem, MA: Wiley ; Scrivener Publishing; 2018. 284 p.

23. Patel UK, Anwar A, Saleem S, Malik P, Rasul B, Patel K, et al. Artificial intelligence as an emerging technology in the current care of neurological disorders. J Neurol [Internet]. 2019 Aug 26 [cited 2020 Aug 18]; Available from: http://link.springer.com/10.1007/s00415-019-09518-3

24. European Commission. White Paper on Artificial Intelligence - a European approach to excellence and trust [Internet]. 2020 Feb [cited 2020 Jun 8]. Report No.: COM(2020) 65

final. Available from: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

25. Pesapane F, Suter MB, Codari M, Patella F, Volonté C, Sardanelli F. Regulatory issues for artificial intelligence in radiology. In: Precision Medicine for Investigators, Practitioners and Providers [Internet]. Elsevier; 2020 [cited 2020 Jun 23]. p. 533–43. Available from: https://linkinghub.elsevier.com/retrieve/pii/B9780128191781000526

26. Recht MP, Dewey M, Dreyer K, Langlotz C, Niessen W, Prainsack B, et al. Integrating artificial intelligence into the clinical practice of radiology: challenges and recommendations. Eur Radiol. 2020 Jun;30(6):3576–84.

27. Wicks P, Chiauzzi E. 'Trust but verify' – five approaches to ensure safe medical apps. BMC Med. 2015 Dec;13(1):205.

28. European Commission. Privacy Code of Conduct on mobile health apps [Internet]. 2018 [cited 2020 Jul 7]. Available from: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

29. Trix M. Health Apps, their Privacy Policies and the GDPR. European Journal of Law and Technology. 2019;10(1).

30. Ahmad OF, Stoyanov D, Lovat LB. Barriers and pitfalls for artificial intelligence in gastroenterology: Ethical and regulatory issues. Techniques in Gastrointestinal Endoscopy. 2019 Oct;150636.

31. Jiang F, Jiang Y, Zhi H, Dong Y, Li H, Ma S, et al. Artificial intelligence in healthcare: past, present and future. Stroke Vasc Neurol. 2017 Dec;2(4):230–43.

32. Bukowski M, Farkas R, Beyan O, Moll L, Hahn H, Kiessling F, et al. Implementation of eHealth and AI integrated diagnostics with multidisciplinary digitized data: are we ready from an international perspective? Eur Radiol [Internet]. 2020 May 6 [cited 2020 Aug 18]; Available from: http://link.springer.com/10.1007/s00330-020-06874-x

33. McCarthy AD, Lawford PV. Standalone medical device software: The evolving regulatory framework. Journal of Medical Engineering & Technology. 2015 Oct 3;39(7):441–7.

34. British Standards Institution. What is a standard? [Internet]. 2020 [cited 2020 Aug 16]. Available from: https://www.bsigroup.com/en-SG/Standards/Information-about-standards/what-is-a-standard/

35. Health Sciences Authority Singapore. Medical device guidance. Health Sciences Authority Singapore; 2018.

36. Anand K, Saini KS, Chopra Y, Binod SK. To Recognize the Use of International Standards for Making Harmonized Regulation of Medical Devices in Asia-Pacific. Journal of Young Pharmacists. 2010 Jul;2(3):321–5.

37. Willingmyre GT. Role of Standards: International Commerce for Medical Devices. IEEE Eng Med Biol Mag. 1984 Mar;3(1):26–30.

38. International Organization for Standardization. ISO STANDARDS ARE INTERNATIONALLY AGREED BY EXPERTS [Internet]. ISO. n.d. [cited 2020 Aug 20]. Available from: https://www.iso.org/standards.html

39. International Organization for Standardization. Consumers and Standards: Partnership for a Better World [Internet]. n.d. [cited 2020 Aug 20]. Available from: https://www.iso.org/sites/ConsumersStandards/1_standards.html#section1_2

40. European Committee for Standardization. European Standards [Internet]. n.d. [cited 2020 Aug 20]. Available from: https://www.cen.eu/work/products/ENs/Pages/default.aspx

41. European Telecommunications Standards Institute. Types of Standards [Internet]. n.d. [cited 2020 Aug 20]. Available from: https://www.etsi.org/standards/types-of-standards

42. NHS England. Clinically-led Review of NHS Access Standards [Internet]. n.d. [cited 2020 Aug 20]. Available from: https://www.england.nhs.uk/clinically-led-review-nhs-access-standards/

43. Joyce R, Joshi I, Morley J. NHS Digital Health Technology Standard Draft [Internet]. NHSx; 2020 [cited 2020 Aug 10]. Available from: https://www.nhsx.nhs.uk/media/documents/NHS_Digital_Health_Technology_Standard_draft.pdf

44. NHS Digital. Information Standards [Internet]. 2018 [cited 2020 Aug 20]. Available from: https://digital.nhs.uk/data-and-information/information-standards

45. British Standards Institution. Medical devices — Recognized essential principles of safety and performance of medical devices. 2016;60.

46. British Standards Institution. Healthcare and medical device standards [Internet]. 2020 [cited 2020 Aug 20]. Available from: https://shop.bsigroup.com/en/Browse-by-Sector/Healthcare/?t=r

47. Marucheck A, Greis N, Mena C, Cai L. Product safety and security in the global supply chain: Issues, challenges and research opportunities. Journal of Operations Management. 2011 Nov;29(7–8):707–20.

48. Slotwiner DJ, Deering TF, Fu K, Russo AM, Walsh MN, Hare GFV. Cybersecurity vulnerabilities of cardiac implantable electronic devices: Communication strategies for clinicians—Proceedings of the Heart Rhythm Society's Leadership Summit. Heart Rhythm. 2018 Jul 1;15(7):e61–7.

49. Kasparick M, Andersen B, Franke S, Rockstroh M, Golatowski F, Timmermann D, et al. Enabling artificial intelligence in high acuity medical environments. Minimally Invasive Therapy & Allied Technologies. 2019 Mar 4;28(2):120–6.

50. Halperin D, Heydt-Benjamin TS, Fu K, Kohno T, Maisel WH. Security and Privacy for Implantable Medical Devices. IEEE Pervasive Computing. 2008 Jan;7(1):30–9.

51. Woods B, Coravos A, Corman JD. The Case for a Hippocratic Oath for Connected Medical Devices: Viewpoint. Journal of Medical Internet Research. 2019;21(3):e12568.

52. NHS Digital. Guidance on protecting medical devices [Internet]. 2020 [cited 2020 Aug 17]. Available from: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-on-protecting-medical-devices

53. Weininger S, Jaffe MB, Goldman JM. The Need to Apply Medical Device Informatics in Developing Standards for Safe Interoperable Medical Systems: Anesthesia & Analgesia. 2017 Jan;124(1):127–35.

54. Reynolds CJ, Wyatt JC. Open Source, Open Standards, and Health Care Information Systems. J Med Internet Res. 2011 Feb 17;13(1):e24.

55. Rimmer J. Improving software environments through usability and interaction design. J Audiov Media Med. 2004 Mar;27(1):6–10.

56. Marcilly R, Schiro J, Beuscart-Zéphir MC, Magrabi F. Building Usability Knowledge for Health Information Technology: A Usability-Oriented Analysis of Incident Reports. Appl Clin Inform. 2019;10(3):395–408.

57. Choudhury A. AI in Healthcare: Improving Human Interface for Patient Safety. Better Standards Needed to Make Artificial Intelligence User-Friendly for Clinicians [Internet]. Rochester, NY: Social Science Research Network; 2020 Feb [cited 2020 Jul 30]. Report No.: ID 3529394. Available from: https://papers.ssrn.com/abstract=3529394

58. Sujan MA, Koornneef F, Chozos N, Pozzi S, Kelly T. Safety cases for medical devices and health information technology: Involving health-care organisations in the assurance of safety. Health Informatics J. 2013 Sep 1;19(3):165–82.

59. Blandford A, Furniss D, Vincent C. Patient safety and interactive medical devices: Realigning work as imagined and work as done. Clin Risk. 2014 Sep;20(5):107–10.

60. Singh H, Classen DC, Sittig DF. Creating an Oversight Infrastructure for Electronic Health Record-Related Patient Safety Hazards. J Patient Saf. 2011 Dec;7(4):169–74.

61. Hinton G. Deep Learning—A Technology With the Potential to Transform Health Care. JAMA. 2018 Sep 18;320(11):1101–2.

62. Naylor CD. On the Prospects for a (Deep) Learning Health Care System. JAMA. 2018 Sep 18;320(11):1099–100.

63. Stead WW. Clinical Implications and Challenges of Artificial Intelligence and Deep Learning. JAMA. 2018 Sep 18;320(11):1107–8.

64. Gerke S, Minssen T, Cohen G. Ethical and legal challenges of artificial intelligence-driven healthcare. Artificial Intelligence in Healthcare. 2020;295–336.

65. Hoeren T, Niehoff M. Artificial Intelligence in Medical Diagnoses and the Right to Explanation. Eur Data Prot L Rev. 2018;4:308.

66. McGreevey JD, Hanson CW, Koppel R. Clinical, Legal, and Ethical Aspects of Artificial Intelligence–Assisted Conversational Agents in Health Care. JAMA [Internet]. 2020 Jul 24 [cited 2020 Jul 31]; Available from: https://jamanetwork.com/journals/jama/fullarticle/2768927

67. Ahuja AS. The impact of artificial intelligence in medicine on the future role of the physician. PeerJ [Internet]. 2019 Oct 4 [cited 2020 Aug 3];7. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6779111/

68. LaRosa E, Danks D. Impacts on Trust of Healthcare AI. In: Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society [Internet]. New Orleans, LA, USA: Association for Computing Machinery; 2018 [cited 2020 Aug 3]. p. 210–215. (AIES '18). Available from: https://doi.org/10.1145/3278721.3278771

69. Doyle C, Lennox L, Bell D. A systematic review of evidence on the links between patient experience and clinical safety and effectiveness. BMJ Open. 2013 Jan 1;3(1):e001570.

70. Allen B. The Role of the FDA in Ensuring the Safety and Efficacy of Artificial Intelligence Software and Devices. Journal of the American College of Radiology. 2019 Feb 1;16(2):208–10.

71. Palojoki S, Saranto K, Lehtonen L. Reporting medical device safety incidents to regulatory authorities: An analysis and classification of technology-induced errors. Health Informatics J. 2019 Sep 1;25(3):731–40.

72. Skierka IM. The governance of safety and security risks in connected healthcare. In: Living in the Internet of Things: Cybersecurity of the IoT - 2018. 2018. p. 1–12.

73. Georgantis G, Kostidi E, Dagkinis I, Papachristos DP, Nikitakos N. Quality and safety in medical 3D printing. In 2020.

74. Hwang TJ, Kesselheim AS, Vokinger KN. Lifecycle Regulation of Artificial Intelligence– and Machine Learning–Based Software Devices in Medicine. JAMA. 2019 Dec 17;322(23):2285–6.

75. Christ A, Quint F. Artificial Intelligence : from Research to Application ; the Upper-Rhine Artificial Intelligence Symposium (UR-AI 2019). arXiv:190308495 [cs] [Internet]. 2019 Mar 20 [cited 2020 Aug 5]; Available from: http://arxiv.org/abs/1903.08495

76. Health C for D and R. Postmarket Management of Cybersecurity in Medical Devices [Internet]. U.S. Food and Drug Administration. FDA; 2019 [cited 2020 Jul 3]. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

77. Balka E, Doyle-Waters M, Lecznarowicz D, FitzGerald JM. Technology, governance and patient safety: systems issues in technology and patient safety. Int J Med Inform. 2007 Jun;76 Suppl 1:S35-47.

78. Florin M-V. Governing Cybersecurity Risks and Benefits of the Internet of Things: Connected Medical and Health Devices and Connected Vehicles [Internet]. Infoscience. International Risk Governance Center; 2017 [cited 2020 Mar 6]. Available from: https://infoscience.epfl.ch/record/229380

79. McCradden MD, Joshi S, Anderson JA, Mazwi M, Goldenberg A, Zlotnik Shaul R. Patient safety and quality improvement: Ethical principles for a regulatory approach to bias in healthcare machine learning. J Am Med Inform Assoc [Internet]. 2020 [cited 2020 Aug 2]; Available from: http://academic.oup.com/jamia/article/doi/10.1093/jamia/ocaa085/5862600

80. Armstrong DG, Kleidermacher DN, Klonoff DC, Slepian MJ. Cybersecurity Regulation of Wireless Devices for Performance and Assurance in the Age of "Medjacking". J Diabetes Sci Technol. 2016 Mar 1;10(2):435–8.

81. Kersbergen C. Patient Safety Should Include Patient Privacy: The Shortcomings of the FDA's Recent Draft Guidance regarding Cybersecurity of Medical Devices. Nova L Rev. 2016 2017;41:397.

82. Alsubaei F, Abuhussein A, Shiva S. Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. In: 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops). 2017. p. 112–20.

83. Alasmari S, Anwar M. Security Privacy Challenges in IoT-Based Health Cloud. In: 2016 International Conference on Computational Science and Computational Intelligence (CSCI). 2016. p. 198–201.

84. Wu F, Eagles S. Cybersecurity for Medical Device Manufacturers: Ensuring Safety and Functionality. Biomed Instrum Technol. 2016 Feb;50(1):23–33.

85. Guzman NHC, Wied M, Kozine I, Lundteigen MA. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. Systems Engineering. 2020;23(2):189–210.

86. Atlam HF, Wills GB. IoT Security, Privacy, Safety and Ethics. In: Farsi M, Daneshkhah A, Hosseinian-Far A, Jahankhani H, editors. Digital Twin Technologies and Smart Cities [Internet]. Cham: Springer International Publishing; 2020 [cited 2020 Jul 31]. p. 123–49. (Internet of Things). Available from: https://doi.org/10.1007/978-3-030-18732-3_8

87. Martignani C. Cybersecurity in cardiac implantable electronic devices. Expert Review of Medical Devices. 2019 Jun 3;16(6):437–44.

88. Ellouze N, Rekhis S, Boudriga N, Allouche M. Cardiac Implantable Medical Devices forensics: Postmortem analysis of lethal attacks scenarios. Digital Investigation. 2017;21:11–30.

89. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, et al. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In: 2008 IEEE Symposium on Security and Privacy (sp 2008). 2008. p. 129–42.

90. Marin E, Singelée D, Garcia FD, Chothia T, Willems R, Preneel B. On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. In: Proceedings of the 32nd Annual Conference on Computer Security Applications [Internet]. Los Angeles, California, USA: Association for Computing Machinery; 2016 [cited 2020 May 22]. p. 226–236. (ACSAC '16). Available from: https://doi.org/10.1145/2991079.2991094

91. Kune DF, Backes J, Clark SS, Kramer D, Reynolds M, Fu K, et al. Ghost talk: Mitigating EMI signal injection attacks against analog sensors. In 2013. p. 145–59.

92. Li C, Raghunathan A, Jha NK. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In: 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services. 2011. p. 150–6.

93. Venkatasubramanian KK, Vasserman EY, Sokolsky O, Lee I. Security and Interoperable-Medical-Device Systems, Part 1. IEEE Security Privacy. 2012 Sep;10(5):61–3.

94. Vasserman EY, Venkatasubramanian KK, Sokolsky O, Lee I. Security and Interoperable-Medical-Device Systems, Part 2: Failures, Consequences, and Classification. IEEE Security Privacy. 2012 Nov;10(6):70–3.

95. Tschider CA. Deus Ex Machina: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future. Savannah L Rev. 2018;5(1):177–210.

96. Alexander B, Haseeb S, Baranchuk A. Are implanted electronic devices hackable? Trends in Cardiovascular Medicine. 2019;29(8):476–80.

97. Ellouze N, Rekhis S, Boudriga N, Allouche M. Powerless security for Cardiac Implantable Medical Devices: Use of Wireless Identification and Sensing Platform. Journal of Network and Computer Applications. 2018;107:1–21.

98. Baranchuk A, Refaat MM, Patton KK, Chung MK, Krishnan K, Kutyifa V, et al. Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know? Journal of the American College of Cardiology. 2018 Mar 20;71(11):1284–8.

99. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018 Jul 1;113:48–52.

100. Saxon LA, Varma N, Epstein LM, Ganz LI, Epstein AE. Factors Influencing the Decision to Proceed to Firmware Upgrades to Implanted Pacemakers for Cybersecurity Risk Mitigation. Circulation. 2018 Sep 18;138(12):1274–6.

101. Denning T, Borning A, Friedman B, Gill BT, Kohno T, Maisel WH. Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems [Internet]. Atlanta, Georgia, USA: Association for Computing Machinery; 2010 [cited 2020 Apr 18]. p. 917–926. (CHI '10). Available from: https://doi.org/10.1145/1753326.1753462

102. Awan MF, Fang X, Ramzan M, Neumann N, Wang Q, Plettemeier D, et al. Evaluating secrecy capacity for in-body wireless channels. Entropy. 2019;21(9).

103. Xu F, Qin Z, Tan CC, Wang B, Li Q. IMDGuard: Securing implantable medical devices with the external wearable guardian. In: 2011 Proceedings IEEE INFOCOM [Internet]. Shanghai, China: IEEE; 2011 [cited 2020 Jun 24]. p. 1862–70. Available from: http://ieeexplore.ieee.org/document/5934987/

104. Li C, Raghunathan A, Jha NK. Improving the trustworthiness of medical device software with formal verification methods. IEEE Embedded Systems Letters. 2013;5(3):50–3.

105. Ibrahim M, Alsheikh A, Matar A. Attack graph modeling for implantable pacemaker. Biosensors. 2020;10(2).

106. Jaffar I, Usman M, Jolfaei A. Security hardening of implantable cardioverter defibrillators. In 2019. p. 1173–8.

107. Kintzlinger M, Cohen A, Nissim N, Rav-Acha M, Khalameizer V, Elovici Y, et al. CardiWall: A trusted firewall for the detection of malicious clinical programming of cardiac implantable electronic devices. IEEE Access. 2020;8:48123–40.

108. Lu S, Lysecky R. Analysis of control flow events for timing-based runtime anomaly detection. In: Proceedings of the 10th Workshop on Embedded Systems Security. 2015.

109. Pinisetty S, Roop PS, Sawant V, Schneider G. Security of pacemakers using runtime verification. In 2018.

110. Rao A, Carreon N, Lysecky R, Rozenblit J. Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems. IEEE Software. 2017;35(1):38–43.

111. Stern AD, Gordon WJ, Landman AB, Kramer DB. Cybersecurity features of digital medical devices: an analysis of FDA product summaries. BMJ Open. 2019 Jun 1;9(6):e025374.

112. MDCG. MDCG 2019-16 -Guidance on Cybersecurity for medical devices. Medical Device Coordination Group; 2019.

113. IMDRF. Principles and Practices for Medical Device Cybersecurity. International Medical Device Regulators Forum; 2020 p. 46.

114. Gordon WJ, Stern AD. Challenges and opportunities in software-driven medical devices. Nature Biomedical Engineering. 2019 Jul;3(7):493–7.

115. Software Safety and Security Risk Mitigation in Cyber-physical Systems - IEEE Journals & Magazine [Internet]. [cited 2020 Jun 24]. Available from: https://ieeexplore.ieee.org/abstract/document/8239950

116. Skierka IM. The governance of safety and security risks in connected healthcare. 2018 Jan 1;2 (12 pp.)-2 (12 pp.).

117. Hanna S, Rolles R, Molina-Markham A, Poosankam P, Fu K, Song D. Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices. :5.

118. Alhumud MA, Hossain MA, Masud M. Perspective of health data interoperability on cloud-based Medical Cyber-Physical Systems. In: 2016 IEEE International Conference on Multimedia Expo Workshops (ICMEW). 2016. p. 1–6.

119. Burton J. The Medical Device Industry: Developments in Software Risk Management. Cambridge Scholars Publishing; 2009. 200 p.

120. Alemzadeh H, Iyer RK, Kalbarczyk Z, Raman J. Analysis of Safety-Critical Computer Failures in Medical Devices. IEEE Security Privacy. 2013 Jul;11(4):14–26.

121. Singh K, Selvam P. 5 - Medical device risk management. In: Timiri Shanmugam PS, Chokkalingam L, Bakthavachalam P, editors. Trends in Development of Medical Devices [Internet]. Academic Press; 2020 [cited 2020 Jun 24]. p. 65–76. Available from: http://www.sciencedirect.com/science/article/pii/B9780128209608000058

122. Marucheck A, Greis N, Mena C, Cai L. Product safety and security in the global supply chain: Issues, challenges and research opportunities. Journal of Operations Management. 2011 Nov 1;29(7):707–20.

123. Sharples S, Martin J, Lang A, Craven M, O'Neill S, Barnett J. Medical device design in context: A model of user–device interaction and consequences. Displays. 2012 Oct 1;33(4):221–32.

124. Nindel-Edwards J, Steinke G. Integrating Human Computer Interaction Testing into the Medical Device Approval Process. Communications of the IIMA [Internet]. 2014 Jun 3;9(2). Available from: https://scholarworks.lib.csusb.edu/ciima/vol9/iss2/6

125. Coping with defective software in medical devices - IEEE Journals & Magazine [Internet]. [cited 2020 Jun 24]. Available from: https://ieeexplore.ieee.org/document/1620994

126. McHugh M. Medical Device Software and Technology: the Past, Present and Future. :9.

127. High-Confidence Medical Devices: Cyber-Physical Systems for 21st Century Health Care. :91.

128. Mashkoor A, Biro M. Towards the Trustworthy Development of Active Medical Devices: A Hemodialysis Case Study. IEEE Embedded Syst Lett. 2016 Mar;8(1):14–7.

129. Pesapane F, Volonté C, Codari M, Sardanelli F. Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. Insights Imaging. 2018 Oct 1;9(5):745–53.

130. Software That Can Kill – EEJournal [Internet]. [cited 2020 Jun 24]. Available from: https://www.eejournal.com/article/20120711-swkills/

131. Altayyar SS. The Essential Principles of Safety and Effectiveness for Medical Devices and the Role of Standards. MDER. 2020 Feb;Volume 13:49–55.

132. Borah KJ. Medical device design - an introduction to systems risk. IJISDC. 2017;1(1/2):186.

133. Hourd PC, Williams DJ. Results from an exploratory study to identify the factors that contribute to success for UK medical device small- and medium-sized enterprises. Proc Inst Mech Eng H. 2008 May 1;222(5):717–35.

134. Pammolli F, Riccaboni M, Oglialoro C, Magazzini L, Baio G, Salerno N. Medical Devices Competitiveness and Impact on Public Health Expenditure [Internet]. 2005 [cited 2020 Aug 20]. Available from: https://mpra.ub.uni-muenchen.de/16021/

135. Wizemann T. "Public Health Effectiveness of the FDA 510(k) Clearance Process: Balancing Patient Safety and Innovation". In: The Medical Device Industry Innovation Ecosystem [Internet]. National Academies Press (US); 2010 [cited 2020 Aug 29]. Available from: https://www.ncbi.nlm.nih.gov/books/NBK209786/

136. Singh DFS Adam Wright, Enrico Coiera, Farah Magrabi, Raj Ratwani, David W Bates, Hardeep. Current challenges in health information technology–related patient safety - Dean F Sittig, Adam Wright, Enrico Coiera, Farah Magrabi, Raj Ratwani, David W Bates, Hardeep Singh, 2020. Health Informatics Journal [Internet]. 2018 Dec 11 [cited 2020 Jul 30]; Available from: https://journals.sagepub.com/doi/10.1177/1460458218814893?icid=int.sj-full-text.similar-articles.2

137. Davey SM, Brennan M, Meenan BJ, McAdam R. Innovation in the medical device sector: an open business model approach for high-tech small firms. Technology Analysis & Strategic Management. 2011 Sep 1;23(8):807–24.

138. Pullen A, Weerd-Nederhof PC de, Groen AJ, Fisscher OAM. SME Network Characteristics vs. Product Innovativeness: How to Achieve High Innovation Performance. Creativity and Innovation Management. 2012;21(2):130–46.

139. Pullen AJJ, Weerd-Nederhof PC de, Groen AJ, Fisscher OAM. Open Innovation in Practice: Goal Complementarity and Closed NPD Networks to Explain Differences in Innovation Performance for SMEs in the Medical Devices Sector. Journal of Product Innovation Management. 2012;29(6):917–34.

140. Omachonu VK, Einspruch NG. Innovation in Healthcare Delivery Systems: A Conceptual Framework. 2010;15:20.

141. Goodman CS, Gelijns AC. The changing environment for technological innovation in health care. Baxter Health Policy Rev. 1996;2:267–315.

142. Smith B, Tarricone R, Vella V. The role of product life cycle in medical technology innovation. Journal of Medical Marketing: Device, Diagnostic and Pharmaceutical Marketing. 2013 Mar 6;13:37–43.

143. Hengstler M, Enkel E, Duelli S. Applied artificial intelligence and trust—The case of autonomous vehicles and medical assistance devices. Technological Forecasting and Social Change. 2016 Apr 1;105:105–20.

144. Ciani O, Armeni P, Boscolo PR, Cavazza M, Jommi C, Tarricone R. De innovatione: The concept of innovation for medical technologies and its implications for healthcare policy-making. Health Policy and Technology. 2016 Mar 1;5(1):47–64.

145. Andreu-Perez J, Leff DR, Ip HMD, Yang G-Z. From Wearable Sensors to Smart Implants--Toward Pervasive and Personalized Healthcare. IEEE Transactions on Biomedical Engineering. 2015 Dec;62(12):2750–62.

146. Yang G, Xie L, Mäntysalo M, Zhou X, Pang Z, Xu LD, et al. A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box. IEEE Transactions on Industrial Informatics. 2014 Nov;10(4):2180–91.

147. Pullano SA, Mahbub I, Bianco MG, Shamsir S, Islam SK, Gaylord MS, et al. Medical Devices for Pediatric Apnea Monitoring and Therapy: Past and New Trends. IEEE Reviews in Biomedical Engineering. 2017;10:199–212.

148. Bergsland J, Elle OJ, Fosse E. Barriers to medical device innovation. Med Devices (Auckl). 2014 Jun 13;7:205–9.

149. Ackerly DC, Valverde AM, Diener LW, Dossary KL, Schulman KA. Fueling Innovation In Medical Devices (And Beyond): Venture Capital In Health Care. Health Affairs. 2008 Jan 1;27(Supplement 1):w68–75.

150. Henshall C, Schuller T, HTAi Policy Forum. Health technology assessment, value-based decision making, and innovation. Int J Technol Assess Health Care. 2013 Oct;29(4):353–9.

151. Campbell B, Knox P. Promise and plausibility: Health technology adoption decisions with limited evidence. International Journal of Technology Assessment in Health Care. 2016;32(3):122–5.

Regulatory and Standardization Challenges for Connected and Intelligent Medical Devices

Annex 3: Interview Findings

UCL In Partnership with bsi.

1 INTERVIEW STRUCTURE

19 stakeholders involved with medical devices were interviewed between the 9th of June and the 25th of August 2020. They have contributed valuable insights from various perspectives, including academia, manufacturers, trade associations, consultancy firms, and regulatory bodies.

Interviews were semi-structured to enable free discussion, and questions touched upon various perspectives, including the regulatory and standardization challenges, the product lifecycle, cybersecurity, innovation, and emerging trends. A list of sample questions are available at the end of this Annex.

The findings are summarised below.

2 PROFILE OF INTERVIEWEES

In total, we have interviewed seven representatives from the industry, six representatives of regulators and public authorities, and six academics.

Most interviewees were involved with devices throughout the entire product lifecycle. Several stakeholders were mostly involved with the first stages of ideation and prototyping.

3 STANDARDS AND REGULATIONS

Key takeaways:

- **Challenges involved in regulating connected, intelligent medical devices:** rapid technological development with devices being produced quicker than regulations can catch up; misalignment across markets; complex to understand and interpret regulations and standards.
- **Challenges of the MDR and IVDR:** increased regulatory burdens have negative effects on smaller companies with fewer resources and no other products to rely on; increased risk of acquisition by larger players; re-classification is costly and existing products might be prioritised over newcomers leading to market delays; insufficient Notified Body capacity.
- **Benefits of the MDR and IVDR:** better post-market surveillance; extra rigour and quality; more focus on software; broader approach to risk; improved safety, security and usability medical devices, including for software-based devices.
- **Advantages of standards:** more adaptive than regulations; can be used as a tool to determine what good looks like; help building secure products from day one.

- **Disadvantages of standards:** lack of clarity; hard to interpret; not user-friendly format; smaller companies lack resources; industry-led rather than collaborative.
- **Regulatory gaps:** emerging technologies; loopholes; producers use the MDR implementation delay to delay the transition.
- **Potential improvements for regulations and standards:** more collaboration between industry, organisations and academia; work more horizontally rather than vertically; more user-friendly and digital (e.g. through GitHub); EU can draw upon best practices and guidelines from FDA when it comes to innovation; and academic institutions could verify. and publish evidence that supports the certification of low-risk products by using certain computational assessment methods.

Challenges for regulating connected, intelligent devices

- Regulating emerging technologies is seen as a challenge, due to their complexity and fast pace of development.
- Regulations are hard to understand and interpret. This is reflected primarily by industry stakeholders who are sometimes unaware of the device classification and the applicable frameworks.
- The main themes concern emerging technologies, internationalisation, organisational challenges, and product classification.

Several stakeholders noted that regulatory frameworks have not kept up with the rapid pace of emerging technologies' development. This results in regulatory gaps in areas such as artificial intelligence and risks, for instance, arising from increased connectivity. Moreover, these technologies create challenges related to product classification, as the lines between the different risk and complexity levels get increasingly blurred.

Several interviewees noted that regulations are challenging to understand and interpret, delay market access, and create organisational issues for manufacturers. Notably, more stakeholders from the industry highlighted this challenge, representing its potential impact on manufacturers. As a consultancy dealing with digital health products underlined, many digital health product providers do not realise that they qualify as a medical device and remain relatively unaware of the relevant standards and regulations. Further, as noted by an industry stakeholder, teams will have varying degrees of knowledge, causing potential misalignment within the organisation. Similarly, there seems to be a shortage of expertise to evaluate advanced technologies from a regulatory perspective.

In terms of internationalisation, respondents from regulatory bodies mentioned the challenge of harmonization, and the need to look at contextual and cultural differences across international markets and structures. Because of Brexit, there is a lack of regulatory alignment, and companies may prefer the US market, and, ultimately, there may be products developed in the UK but sold in the US.

Benefits and challenges of the new MDR and IVDR

- Benefits include increased post-market surveillance and improved security, as well as covering technology better.
- Challenges include increased regulatory burdens and up-classifications. They particularly affect SMEs with limited resources.

When asked about the challenges and benefits of the new MDR, respondents highlighted both positive aspects of the latest frameworks and challenges related to enforcement and implementation.

Two respondents representing regulators noted that the MDR is still vague in its descriptions and offers no clear guidance for more advanced technologies such as ML. Despite this, many regulators had a positive attitude towards the MDR, because it strengthens safety and post-market surveillance. Besides, one noted it ensures safety improvements across the entire supply chain and provides for better traceability.

However, the interviews also highlighted numerous challenges and adverse effects of the MDR. Respondents from industry, academia, and regulators alike indicated that new regulations could harm small companies, as the rules are becoming more complicated and require more resources. Similarly, some noted the potential costs involved with the re-classification, which might delay bringing devices to market. This could also lead to a blockage of new companies, or companies in new markets, as Notified Bodies might prioritise recertifying existing products. Besides, the re-certification process might affect patients' access to care. The recent COVID-19 outbreak and Brexit contribute to unpreparedness and uncertainty. Moreover, one interviewee suggested that the MDR will make it more challenging for newcomers to enter the market, which has led to an increase in acquisitions of start-ups by larger companies.

On the other hand, nine respondents mentioned that the new MDR had a positive impact on the landscape, leading to better post-market surveillance and quality, as well as extra rigour. This, in turn, improves the safety, security, and usability of medical devices. One interviewee noted that software up-classifications resulting from Rule 11 of the MDR are beneficial and provide more protection, as the MDR focuses on risk rather than physical harm as previous directives. Moreover, the MDR focuses increasingly on software, which is more in line with modern technologies and trends in the field of medical devices. However, it has also been indicated that the progress in this area is limited as the MDR fails to focus on new technologies, such as AI.

Advantages of standards

- Standards help ensure safety, quality, performance and help meet regulatory requirements.

- There was a consensus among the interviewees on the importance of using standards to decide what good looks like and to enable good by design, by ensuring high quality product and meeting safety requirements. From the perspective of the industry, standards help organisations stay on track with regulatory requirements and provide quality during product development.

Standards can be integrated into the product design processes to ensure high-quality and safe devices. They provide a foundation of quality concerning safety, security, usability, and information governance, and are crucial to ensure patient safety and trust.

Regarding emerging challenges, standards are also increasingly important for digital technologies. For instance, the existing regulatory frameworks fail to capture AI and other emerging technical risks such as cybersecurity. Moreover, standards are also crucial for interoperability.

From an innovation perspective, several industry stakeholders pointed out how standards could enable innovation by functioning as a competitive advantage for quicker market access by building trust and compliant products.

Disadvantages of standards

- Standards, as well as regulations, still fail to comprehensively capture the complexities of emerging technologies.
- Standards may be seen as unclear and complicated to interpret.

Some respondents highlighted the lack of clarity of some standards, and compared using standards to "learning a new language." Indeed, the difficulty of understanding standards and regulations was a re-occurring theme in the interviews. This is particularly challenging for small companies and developers, who find it difficult to navigate standards.

Five interviewees representing industry highlighted the outdated and inaccessible format of standards. It was noted that standards should be more modern, flexible, and interactive and collaborative to better align with how small technology teams work today. A few academics also noted that standards were seen as complex to implement in practice.

Among a few regulators and academics, standard fragmentation and the lack of clarity what standards should be used in what circumstances were recurring themes. It has been also noted that there are still gaps for emerging technologies and interoperability in the existing standards framework.

Regulatory gaps

- Regulatory gaps are primarily centred around emerging technologies.

When asked about regulatory gaps, around half of the interviewees agreed that there are gaps for emerging technologies, especially as technological development occurs faster than regulatory changes.

Moreover, an interviewee from industry highlighted an issue around the evidence of efficacy, and that regulatory frameworks are not suited for the iterative process that software development follows. As noted, "it assumes medical devices are static and fixed once on the market". On the other hand, one industry respondent presented a different view, saying that the appropriate regulatory frameworks exist, but need to be modified and adapted to new data and technologies. Moreover, when answering this question, several respondents stressed the lack of clarity when it comes to regulations.

Further, there are no taxonomies or standards on risk classification when it comes to digital health, and awareness of safety and security (both cyber and physical) in the industry is still needed. An academic also mentioned there is an issue around combining citizen-generated health data with official health data.

There are also potential loopholes, and one respondent from industry mentioned that companies are actively trying to circumvent regulations, particularly given the delay of the MDR transition period. This gives manufacturers more time to apply for conformity certificates under the MDD, and be subject to less onerous requirements, as they are more likely to qualify as Class I device.

Potential improvements for standards and regulations

- Standards should be more collaborative and accessible.
- Standards should provide more examples and guidance to make them less complicated to understand.

Interviewees from public authorities and industry alike stress the importance of working collaboratively on standards development for emerging technologies, rather than working in silos. Public agencies and industry need to collaborate and implement knowledge and information sharing mechanisms. An entrepreneur suggested that standards-development should be done horizontally and collaboratively (e.g. through GitHub as developers work nowadays) and in conjunction with other international organisations. Standards should be accessible and integrated across design, safety and product, rather than addressing individual, siloed components of devices. Numerous stakeholders underlined that national and international collaboration between regulators and healthcare providers is required. This is because, in the case of global technologies, no jurisdiction can hope to develop effective and efficient standards alone. It has also been indicated that there must be a degree of market consolidation before stable and mature standard and regulations can be introduced. More coordination and capacity are required overall.

When it comes to industry, consultancy firms help developers assess what an update means in terms of regulation and compliance, but this can be clarified further as standards and regulations can be hard to interpret. Apart from being more accessible, standards need to be clearer by, for instance, including more examples and guidance.

4 SAFETY AND SECURITY

Key takeaways:

- **Security challenges:** increased connectivity; interconnectivity and interoperability; hackers; the need for trust and security for the patient; some products are not as robust as they should be, cyber-physical elements (e.g. temperature); vulnerabilities from the wider system
- **Safety challenges:** non-compliant devices are placed on the market; safety issues all comes down to error in the lifecycle/design; software errors and unexpected behaviour; usability and possible misunderstandings between stakeholders
- **Other:** Difficult to differentiate between the two concepts safety and security, but should be looked at separately

Security challenges

- Connectivity gives rise to new vulnerabilities, including cyber security risks such as hackers.
- Some standardisation gaps for security.
- Better cyber hygiene is needed.
- Privacy, security and safety are crucial to address to ensure patient safety and trust

Numerous respondents recognised that the increased connectedness between devices is one of the largest security risks, because it makes devices more vulnerable to cyberattacks. As a result, connected medical devices can act as gateways to other platforms and the broader healthcare network. In this context, it was highlighted that good cyber hygiene is required from both end-users and manufacturers to ensure the security of devices.

Moreover, the interconnectedness between networks and devices, as well as interoperability, create vulnerabilities in the system they operate in. For instance, tensions and vulnerabilities can arise from the interactions between hardware and software and may potentially create risks for patient's safety. Further, tensions can arise from the way the end-user interacts with the device. Therefore, it is crucial that end-users, such as health workers or patients, know what the device is intended for and how to use it.

According to several stakeholders, regulatory frameworks are not suitable to protect users from misuse and the unintended consequences.

To ensure the safety and security of devices across the supply chain, several stakeholders noted the value of standards in achieving this goal.

Safety challenges

- Non-compliant devices are placed on the market
- Safety issues all comes down to error in the lifecycle/design; software errors and unexpected behaviour

While safety was very interlinked with security in the interviews overall, there were some challenges mentioned in regard to safety specifically.

Some respondents highlighted app-store when it comes to security and safety, and how there are several non-compliant devices and apps that are currently available on the market when they perhaps should not be. As noted by one stakeholder from a regulatory body, there is currently no clear system in place for how to manage and deal with these kinds of issues. However, it has not been seen as a key safety threat just yet.

In order to ensure safety and usability in the lifecycle is the usability and the inclusion of clinicians in the process to conduct proper risk assessments. While engineers are experts in their fields, they lack the clinical insights needed to ensure safety and thus should incorporate feedback from clinicians. Similarly, manufacturers must take into consideration end-users in the design process and identify how users will interact with the device to avoid misuse. Several respondents also mentioned the importance of cyber-physical elements, for instance the safety of device components, tolerance and resilience to external factors, as well as the probability of device performance.

Overall, patient safety was the key theme in the interviews when asking about security. When it comes to medical devices, several respondents mentioned the word 'trust'. To introduce a product to market, manufacturers need to ensure the patient is at the core of the product to gain trust – this includes capturing both safety and cybersecurity. Privacy and security might not be priorities *per se*, but they are crucial to improve patient safety. Existing standards use security, safety and usability/effectiveness as three key domains to assess whether health software (software as medical device, medical device or unregulated health IT) is fit for purpose.

Safety and security all boil down to errors – in the design process, software development or other errors in the lifecycle. As devices vary, so do their risks for causing harm and threatening patient safety. As two respondents pointed out, during trials, it is crucial that devices are also tested in real-life environments as well to understand the behaviour of the device.

Errors in devices such as implantable medical devices can lead to critical consequences. For instance, hacking a pacemaker such as changing the code can technically lead to a

breakdown of the device. Likewise, if a glucose monitoring equipment would have been manipulated.

5 INNOVATION AND ORGANISATION

Key takeaways:

- **Organisational challenges:** high barriers to entry; complicated, strict regulatory frameworks; long innovation cycle; high costs and dependence on the 'buyers' (such as NHS) adoption criteria; risk of acquisitions

Organisational challenges for market entry

- Regulatory burden and long processes are seen as the most challenging aspects for innovation and SMEs.

Interviewees see the regulatory burdens, market access and resource requirements as the key challenges to innovation.

Several respondents from industry and academia underlined that the field of medical devices is very complex, and that understanding regulations and the environment is difficult for newcomers and less-resources companies. Medical devices are a high-innovation arena, but there are many barriers such as trials and processes, which can severely threaten scalability. The innovation cycle is long, and it often takes years to commercialise. While larger companies have other products to fall back on, this is not true for smaller companies.

It was also pointed out that companies need to think about the adoption framework for their 'buyers' (such as the NHS) and the criteria they consider from early on. However, it is hard for companies with little resources to think about the piece price early on in their journey. Healthcare providers are also considered as too bureaucratic to adopt to these new technologies.

6 FUTURE AND TRENDS

Key takeaways:

- **Technologies:** AI, ML, Big data
- **Industries and uses:** predictive analytics; mental health; AI for back-office functions; data portability; more transparency; accessibility; proactive management of health

- **Risks and challenges:** black box decisions made by AI; higher costs for complex products; doctors need more education; regulators need to assess combination products

Main trends

- Main trends include AI and other advanced technologies
- Emerging areas include mental health, predictive analytics, and portability of data

The main emerging trend is that advanced technologies are giving rise to new products and adding capabilities to the existing ones. All respondents mentioned AI and ML as the key emerging technologies, where AI would often be incorporated in a product to aid decision-making.

A few emerging industries and use-cases that were mentioned include mental health, predictive analytics, and exploitation of AI for functionality and back-office functions. Further, portability of data and using non-clinical data to influence non-physical conditions of patients through data analysis were mentioned. Another emerging trend is that digital health literate generations tend to be less concerned about privacy, e.g. using social media mood testing to prevent self-harm.

Moreover, several interviewees highlighted the trend towards proactive management of health and more democratisation and personalisation in the healthcare industry. Through technologies and knowledge, patients can become more engaged and only see the doctor when unwell, not for common checks.

A common theme seemed to be that devices will work with healthcare rather than replace functions (through the blurring of the lines between various disciplines) and that the landscape is developing rapidly. Further, transparency and openness will be valued by future generations, and the importance of testing of usability and security will only increase.

Key challenges resulting from these trends

- Unsupervised and complicated algorithms are hard to interpret, which creates challenges for classification of combination products, such as hardware and software

As an increasing number of medical devices embed intelligence, there is an increasing risk of black box algorithms contributing to decision-making processes in medicine. For unsupervised algorithms, it is complex (if not impossible) to fully understand the mechanisms and justifications behind the output. This does not only create potential risks for the security and safety of devices and trust issues among users, but also generates regulatory challenges as regulators struggle to construct frameworks around such complex algorithms.

As boundaries between disciplines become increasingly blurry, regulators have yet to figure out how to assess and classify combination products. Further, the overlap between wellness/well-being and medical uses can lead to manufacturers to market their devices as wellness devices to bypass regulations. This is because wellness products are not subject to the same compliance burdens and do not have to ensure the same level of safety and security as medical devices would be expected to have. Again, this demonstrates challenges around the existing classification and regulatory mechanisms.

Several respondents highlighted that standards could support technological progress, as they are more adaptive and can fill in the regulatory gaps. Further, standards can help build incentives for ethical design and explainability for complex algorithms.

SAMPLE QUESTIONS (FOR INTERVIEWS WITH INDUSTRY STAKEHOLDERS)

Introduction & Organisation

- What kind of devices does your organisation work with?
- What is your specific involvement with intelligent, connected medical devices?
- At what stage of the medical devices' development do you tend to be involved?
- What is your organisation's structure like, and what teams are involved with medical devices?
- What would you say are the main stages of the medical device development lifecycle?

Innovation & Organisation

- What are the main organisational challenges for a new company or for a new product to enter the market?
- What challenges did your organisation face when entering the market?

Standards

- At what stage of the medical device development lifecycle do you consider regulations and standards? Are you aware of the main regulations and standards relevant to the products you work with?
- Has the new Medical Devices Regulation or the In Vitro Device Regulation had any impact on your work? Has the classification of your products changed?
- Does your organisation engage with standards? Are there any obstacles to engaging with standards?
- Have you incorporated standards in your organisational processes? (To e.g. ensure safety, to ensure compliance, or for adaptation to market needs)
- Could you identify any potential negative consequences from using standards?
- Have you observed any major regulatory gaps in the field?
- Given an opportunity, what would you improve in terms of regulation and standards in this area?

Security

- How do you ensure security across the supply chain and in the production of your devices?
- What are the main security challenges for your product?

Futures & Trends

- What are the main trends and innovations you see emerging in the field of intelligent and connected medical devices? Do you intend to work or are you currently working on any of these innovations?
- What are the key challenges or risks that these trends and innovations may create?

- How do you think regulations and standards could help to address these challenges? Why is this so?

Conclusion

- Do you have any suggestions who else we could interview?
- Do you have any further comments or questions?

Regulatory and Standardization Challenges for Connected and Intelligent Medical Devices

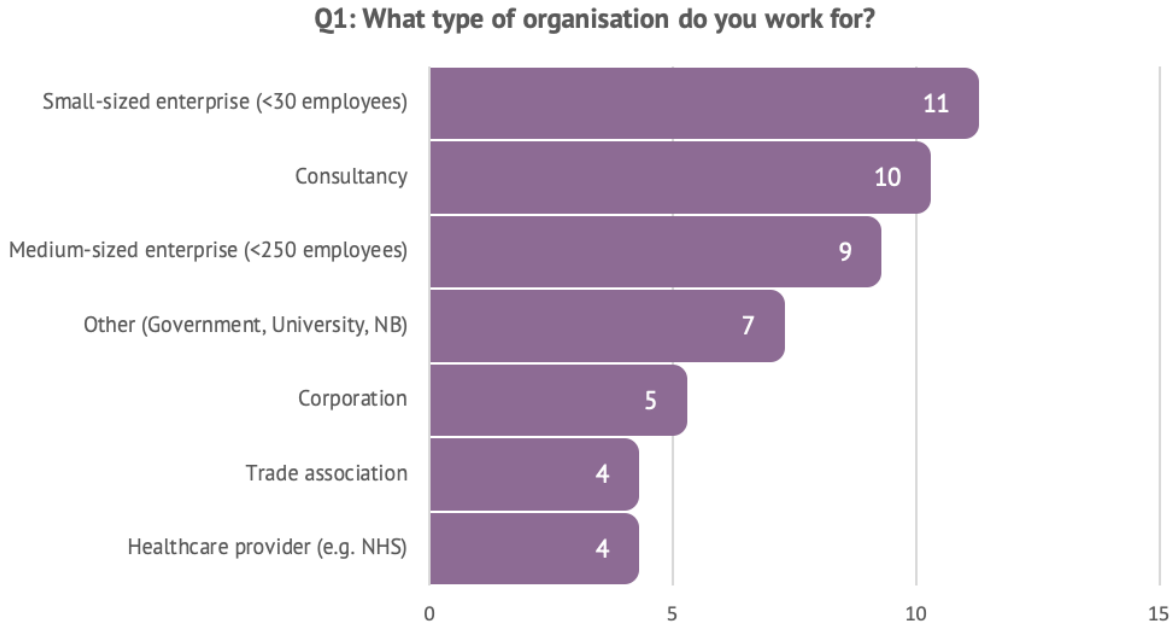
Annex 4: Survey Findings

UCL In Partnership with bsi.

SUMMARY OF FINDINGS

An online survey, covering areas related to regulations, standards, and innovation, formed an important part of the primary research. In total, 50 respondents from the medical devices' sector contributed to the survey. The survey consisted of 19 questions. The results are summarised below.

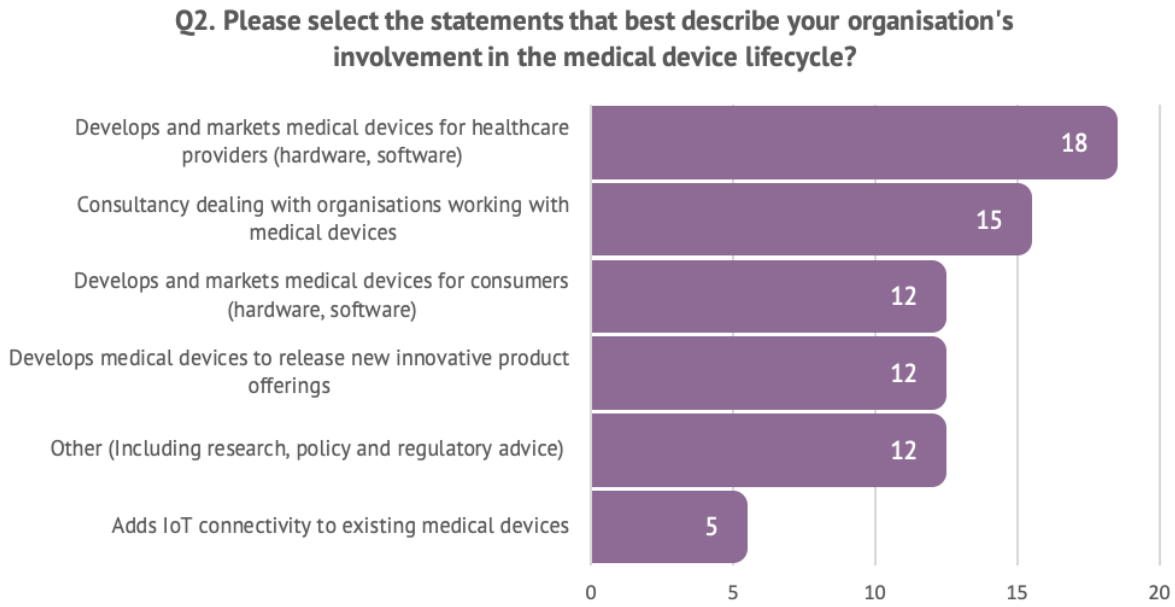
Q1. What type of organisation do you work for?



A wide range of stakeholders participated in the survey. SMEs (20 combined, with 11 for small and 9 for medium-sized enterprises) and consultancies (10) are the most widely represented stakeholder groups. Other respondents included corporations (5), trade associations (4) and healthcare providers (4).

Respondents that chose 'Other' comprise universities (2), the UK civil service (1), a student (1), a Notified Body (1), a regulator (1), and health technology network (1).

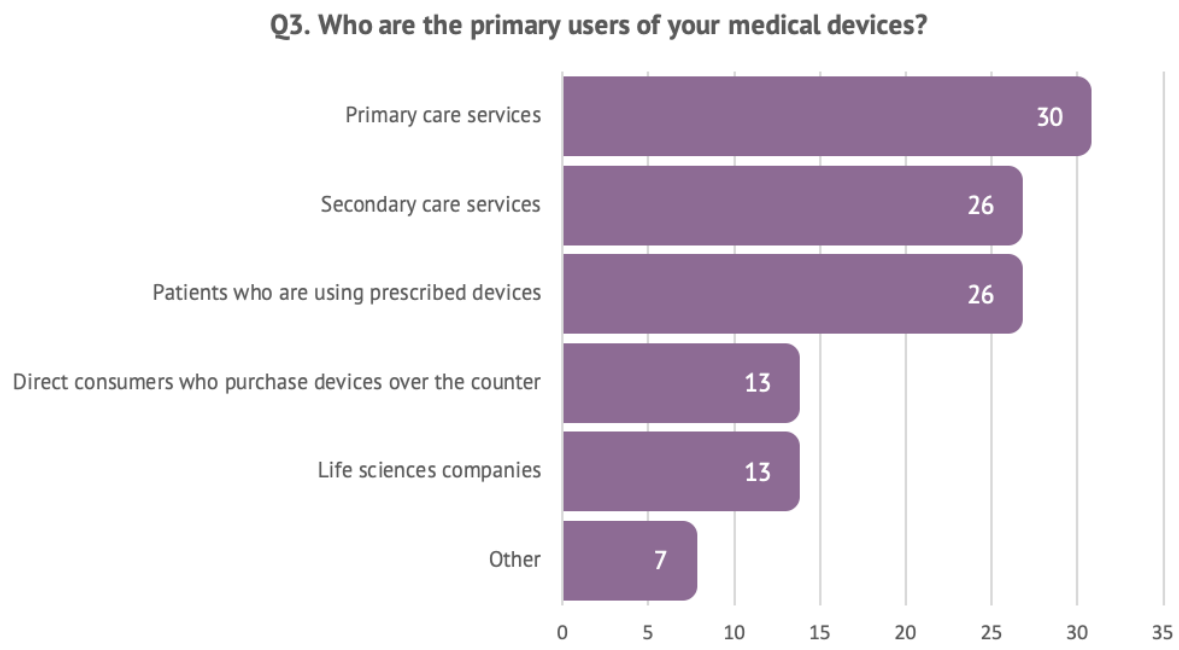
Q2. Please select the statements that best describe your organisation's involvement in the medical device lifecycle?



It was most popular among the respondents to develop devices for healthcare providers (18), followed by engaging in consultancy work for organisations involved with medical devices (15). Respondents also develop medical devices for consumers (12), innovative product offerings (12) and add IoT functionalities to existing devices (5).

'Other' involvement included: support investments in the sector, advising health providers in the use of medical devices, regulatory services, and researchers.

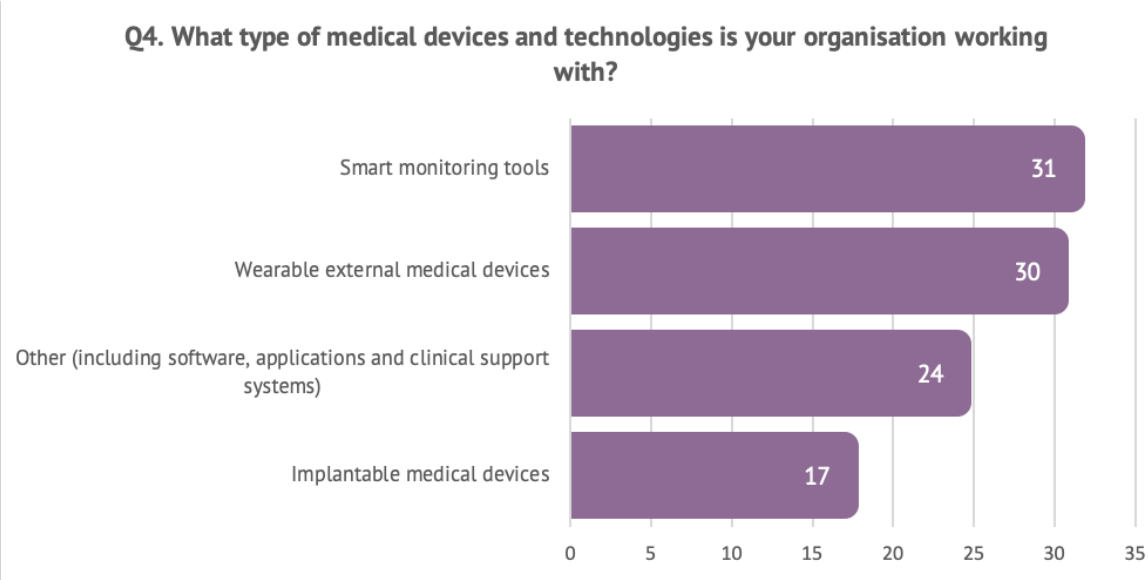
Q3: Who are the primary users of your medical devices?



Most respondents (30) engage with primary care services, followed by secondary care services (26) and patients (26). For other respondents, the primary users of devices include consumers buying devices over the counter (13) and life science companies (13).

'Other' was selected by respondents who serve multiple groups of users, or other users such as manufacturers.

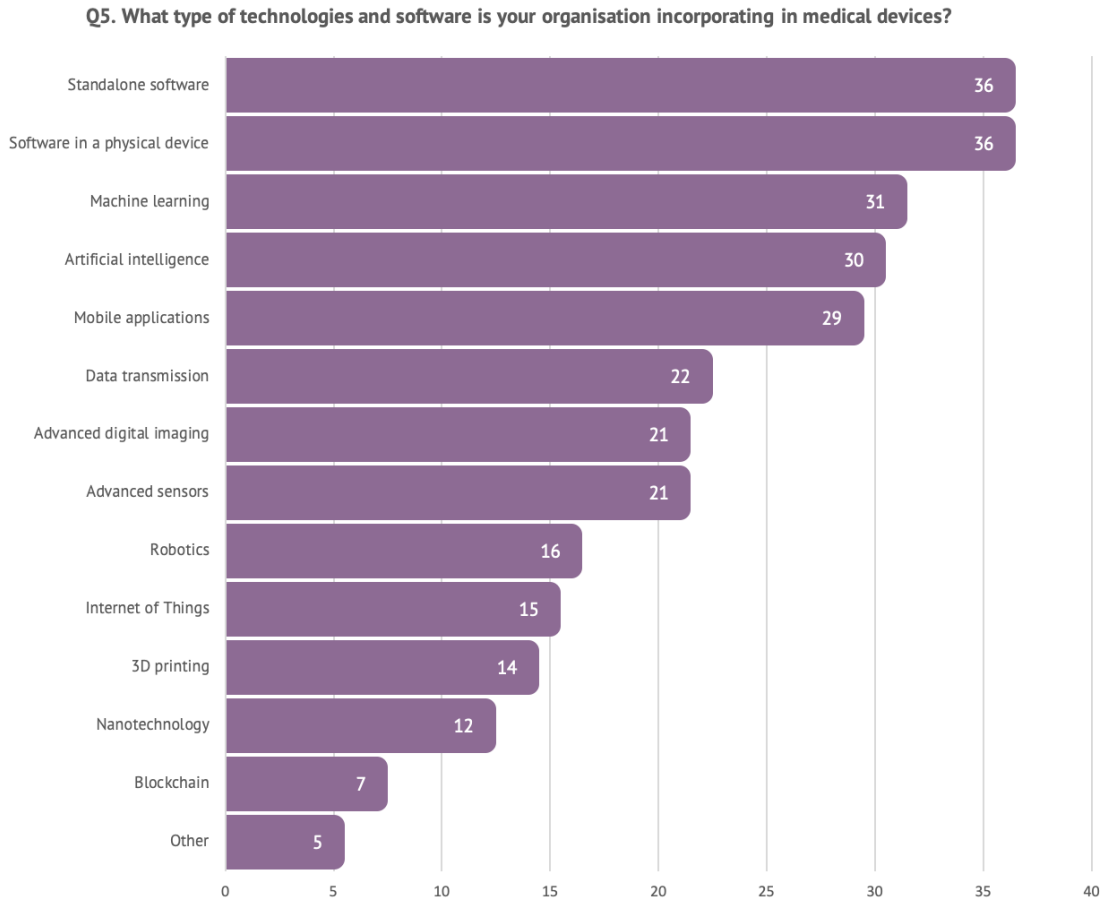
Q4: What type of medical devices and technologies is your organisation working with?



This question revealed a wide range of product types and uses, including smart monitoring tools (31), wearable devices (30) and implantable medical devices (17).

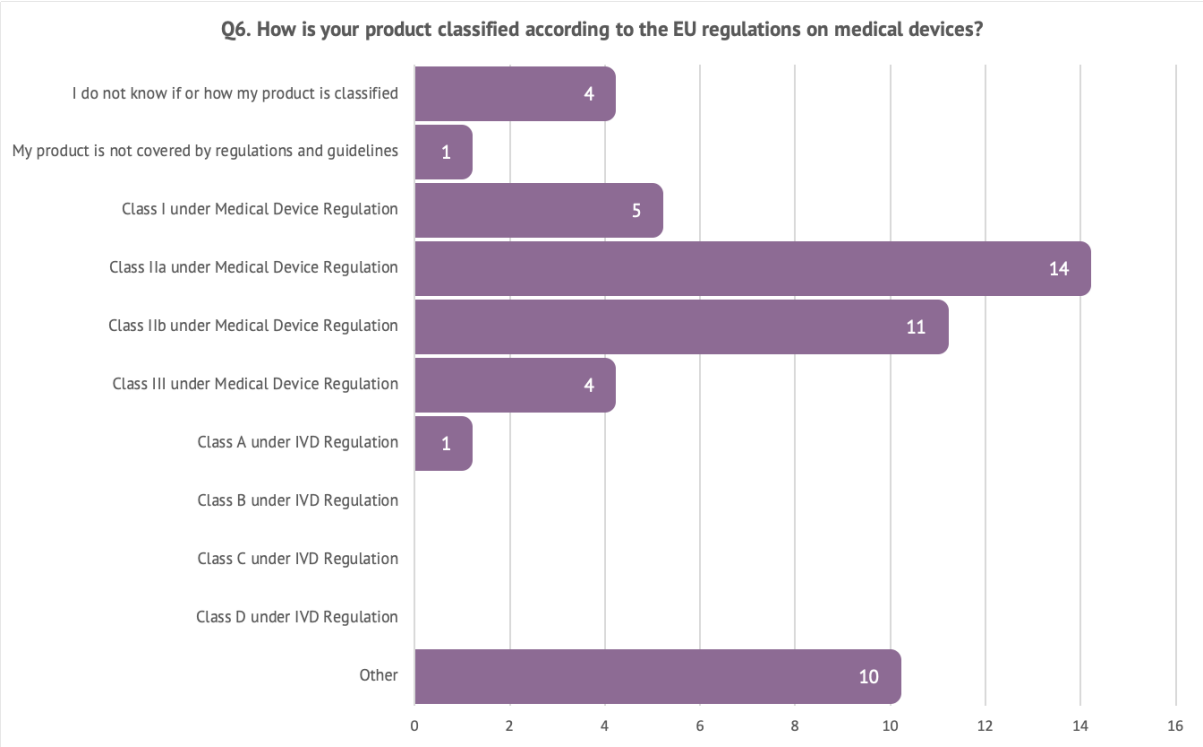
'Other' included clinical support systems, ultrasound, electromechanical diagnostic and therapy devices (e.g. imaging system and PAP machines), drug delivery, non-wearable external medical devices (pacemaker), Integrated Care Clinical Information Systems, software, mental health, digital consultations, cardio-respiratory diagnostic/monitoring devices, and digital therapeutics.

Q5. What type of technologies and software is your organisation incorporating in medical devices?



The survey revealed a wide range of technologies used in medical devices, reflecting the diversity of this industry.

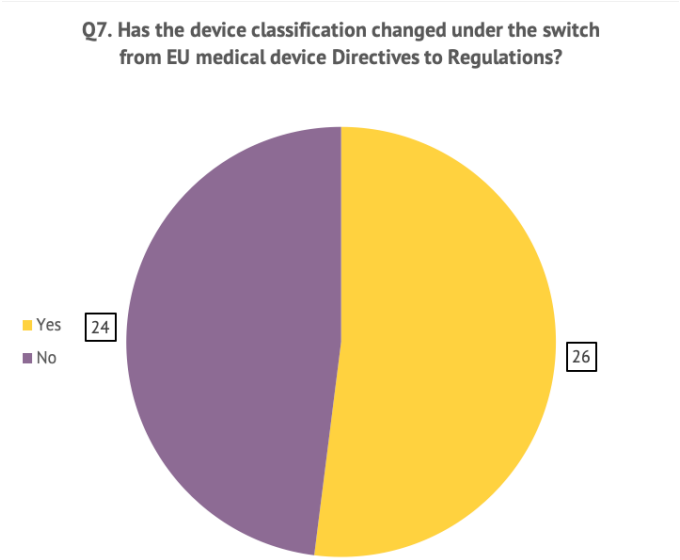
Q6: How is your product classified according to the EU regulations on medical devices?



The majority of respondents worked with devices classified under the MDR, most commonly Class IIa devices (14) as well as Class IIb (11), Class III (4) and Class I (5). Only one respondent worked with devices under the IVDR, classified as a Class A device. A minority of respondents did not know how their device was classified (4) or indicated that their product is not regulated (1).

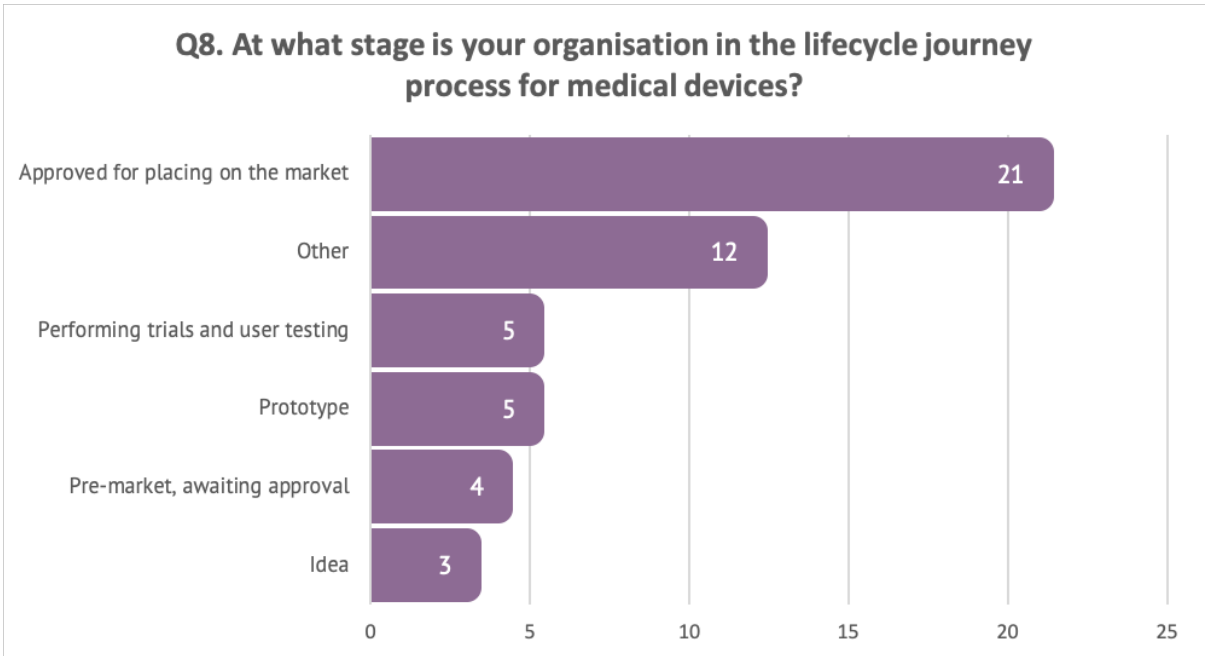
Respondents selected 'Other' (10) because, for instance, this question was not relevant to them as they were consultancies.

Q7. Has the device classification changed under the switch from EU medical device directives to regulations?



For most respondents (26) the device classification will change as a result of the MDR/IVDR.

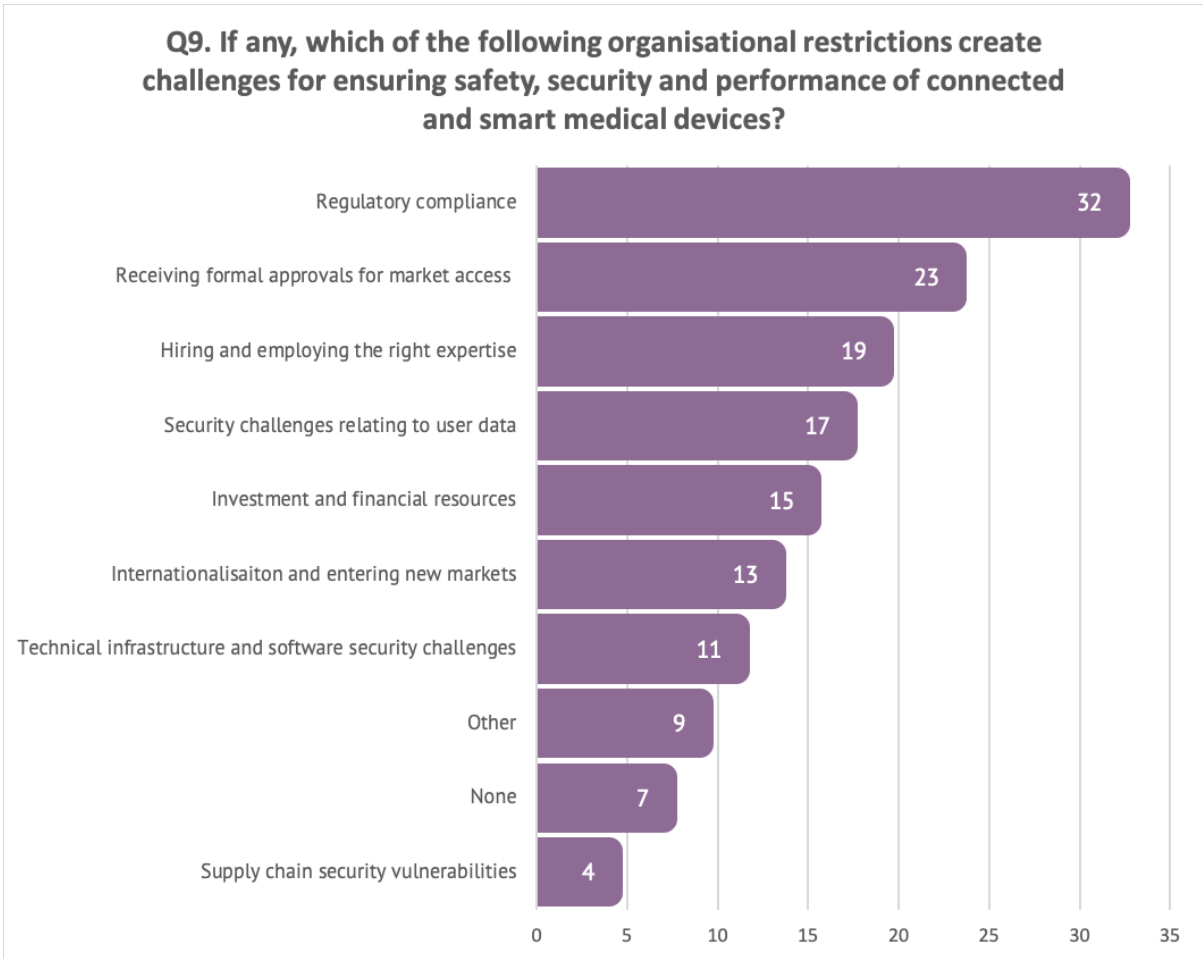
Q8. At what stage is your organisation in the lifecycle journey process?



The largest group of stakeholders was working with devices already placed on the market (21), with others focusing on the earlier stages of the lifecycle including performing trials and tests (5), prototype (5), awaiting approval (4) and idea (3).

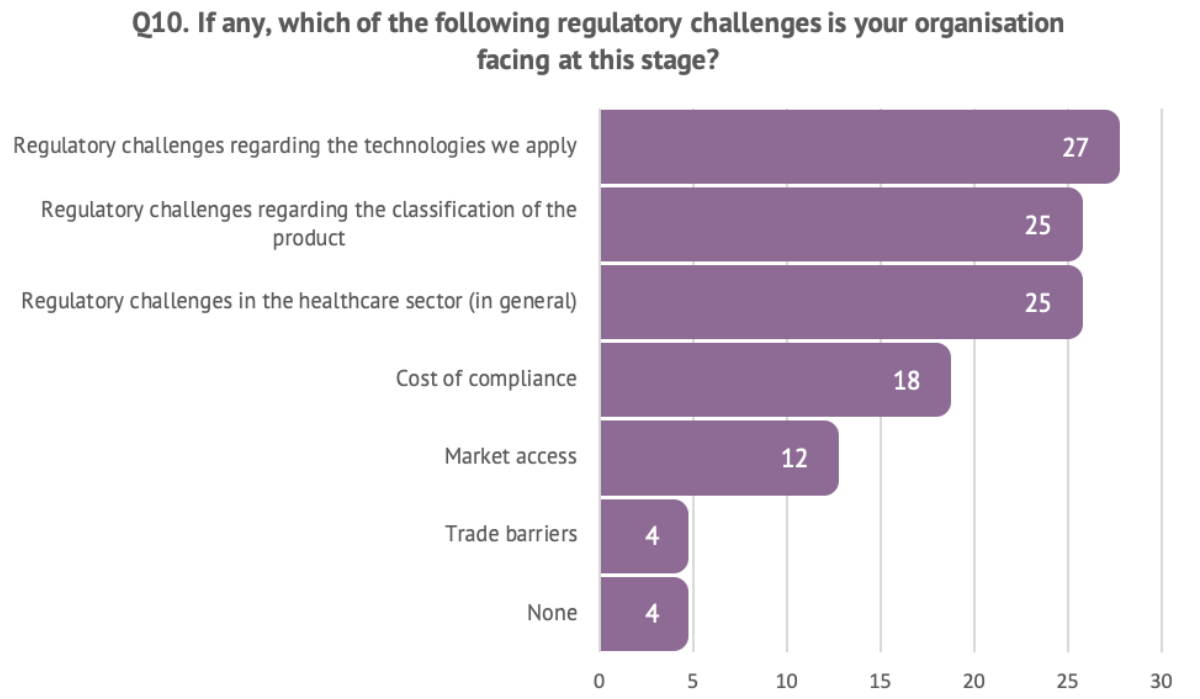
Some respondents chose 'Other' because, for instance, they were involved across the entire lifecycle.

Q9. If any, which of the following organisational restrictions create challenges for ensuring safety, security and performance of connected and smart medical devices?



Most respondents argued that regulatory compliance (32) and market access (23) were the most prominent challenges, followed by hiring the right expertise (19), security challenges related to user data (17), investment (15), internationalisation (13) and security challenges related to the technical infrastructure (11).

Q10. If any, which of the following regulatory challenges is your organisation facing at this stage?



Over a half of respondents face regulatory challenges regarding the technologies they apply (27). Other regulatory challenges concern product classification (25) the healthcare sector (25), the cost of compliance (18), market access (12) and trade barriers (4). A small minority noted that they face no challenges (4).

Key take-aways from 'further comments' on Q10:

Regulations

- Changing regulatory and classification requirements a recurring theme, reflected by several respondents
- MDR results in more regulatory burdens as some devices have been up-classified
- Regulatory uncertainty might delay market access
- There is a lack of expertise and Notified Body capacity

Emerging technologies

- There is little regulatory guidance on AI/ML, especially in the EU compared to the US

Organisational challenges related to innovation

- Smaller companies face resource constraints

Q11. Please describe how your organisation gains knowledge about regulatory requirements in the market (e.g. for medical devices, electrical safety, GDPR)? Please include, what, if any, standards are used to support this and how are they applied?

Source of knowledge	(n=)
Independent research on regulations	19
Standards	14
Internal Function	10
Participation in Standard Development Committees	10
Trade association or industry network	9
Industry Events	8
Training	5
Contact with Regulatory Bodies	3
Engaging with experts or other companies	2

Standards mentioned	(n=)
13485	8
14971	6
62304	4
60601	3
62366	3
14155	2
27001	2
9001	1

Q12. Please describe how your organisation gains understanding of how the healthcare sector evaluates and adopts new services and products (e.g. interoperability, efficacy, economic benefit)? Please include, what, if any, standards are used to support this and how are they applied?

Source of understanding	(n=)
Independent research and networking	7
Industry Events	6
Contact with the healthcare sector	6
Standards	5
Trade association or industry network	3
Information from purchase	2
Training	2
Engaging with experts	1

Q13. What is your organisation's overall approach to design and manufacture a good technical product (non-regulatory)? Please include, what, if any, standards are used to support this and how are they applied?

Source	(n=)
Standards (e.g., ISO 13485, ISO 62366-1, IEC 62304, ISO 14971)	20
Ensuring usability	8
Reliability & Validation	3
Focus on clinical requirements and needs	2
Best practices and clear documentation	2
Focus on safety, general	2
Using modern technologies and tools	1

Q14. How does your organisation ensure safety and security across the supply chain? Please include, what, if any, standards are used to support this and how are they applied?

Source	(n=)
Standards	16
N/A	15
Audit	4
Contractual arrangement	3
Avoiding single source suppliers	2
Best practice	2
Specific technologies	1
Internal system	1
Consultancy	1
Supply chain risk management	1
Internal expertise	1
Approved vendors	1
Detailed specifications	1
QMS	1
Guidelines from public authorities	1

Standards mentioned	(n=)
14971	3
82304	2
13485	2
27001	2
62304	2
14155	1
60601	1
80001	1
24971	1
13480	1
10993	1

Q15. What do you think will be the biggest changes to your organisation, or the healthcare sector in general, in the next 3 years?

Key take-aways:

MDR/IVDR, Regulatory and Standardization challenges

- Onerous compliance requirements under the MDR
- Compliance burdens for SMEs
- Balancing innovation and safety
- Lack of EU harmonized standards for the MDR
- Delayed market access due to the MDR
- Constant change; change from the MDD/ AIMDD/ IVDD to MDR/ IVDR
- Costs

Innovation

- Lack of innovation adoption across integrated care systems and challenges of a digital future
- Balancing safety with innovation while encouraging responsible innovation
- Overcoming barriers to AI deployment more widely - regulatory, around data sharing, validation and responsibility

Organisational challenges

- Obtaining monetary backing to produce regulated devices
- Transforming from a start-up to a more mature company

Safety

- Data security challenges for healthcare infrastructure
- Security and AI develop to keep up to speed by competitors from non-medical areas

Expertise

- Hiring and affording the right competence and expertise

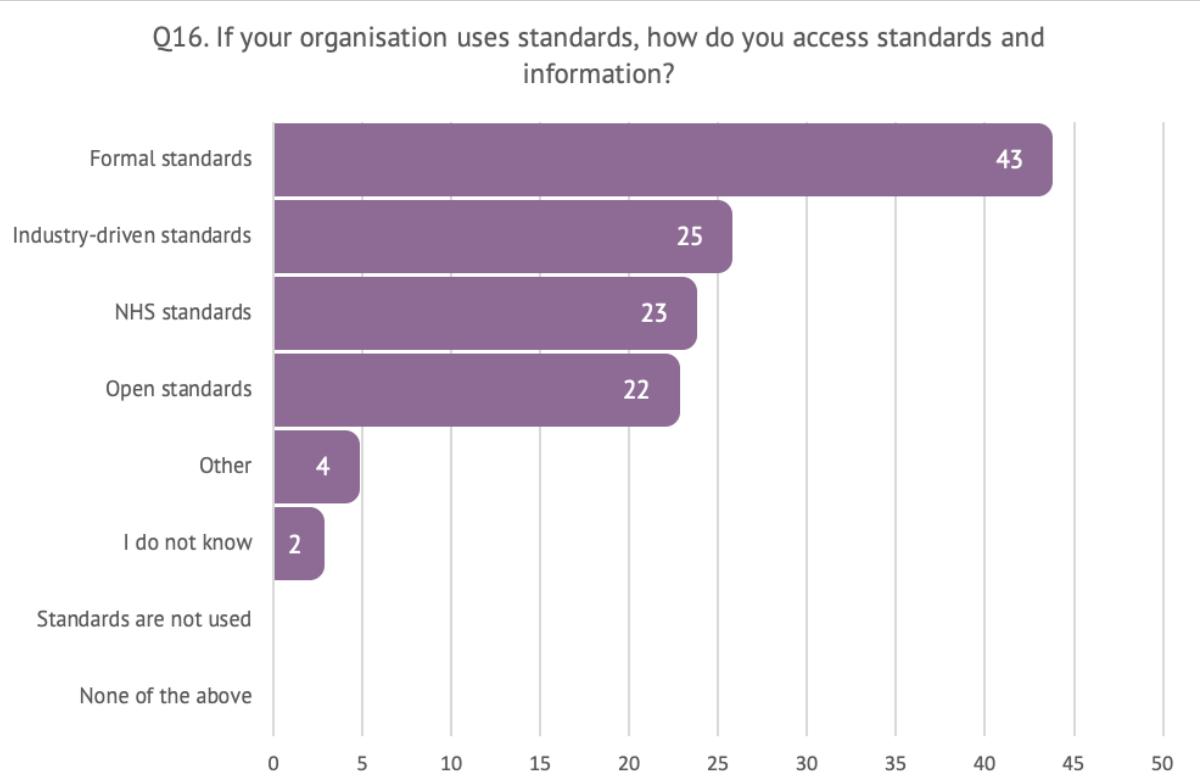
Emerging technologies

- More connectedness and interoperability, as well as a reduction in the size of devices
- AI and ML will ramp up
- Launching ML and conducting micro clinical trials with live data

COVID-19

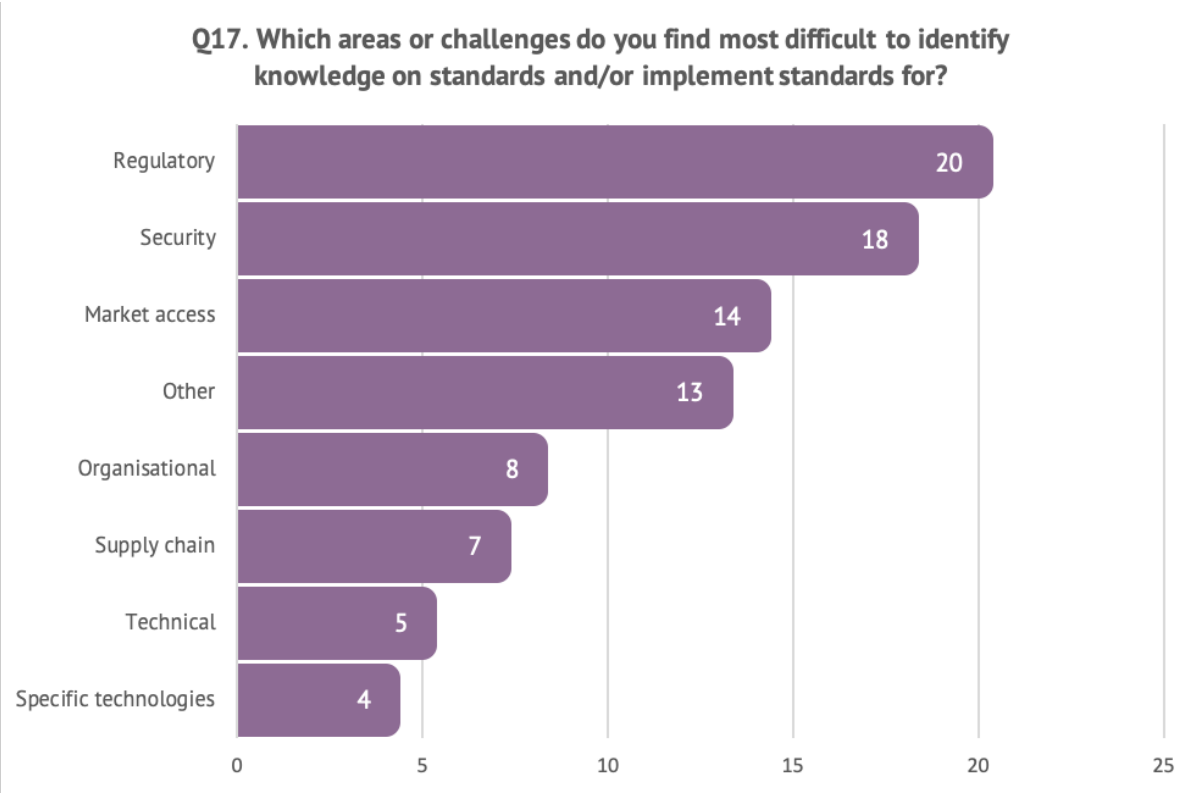
- COVID-19 will change the digital health world
- COVID-19 will change very little; the European healthcare system moves very slowly
- COVID-19 has shown that the 200-year-old model of patients queuing to see doctors is ready for a change
- The post-pandemic world requires reorientation, and currently, there is a limited capacity of Notified Bodies and obtaining approval requires significant time

Q16. If your organisation uses standards, how do you access standards and information?



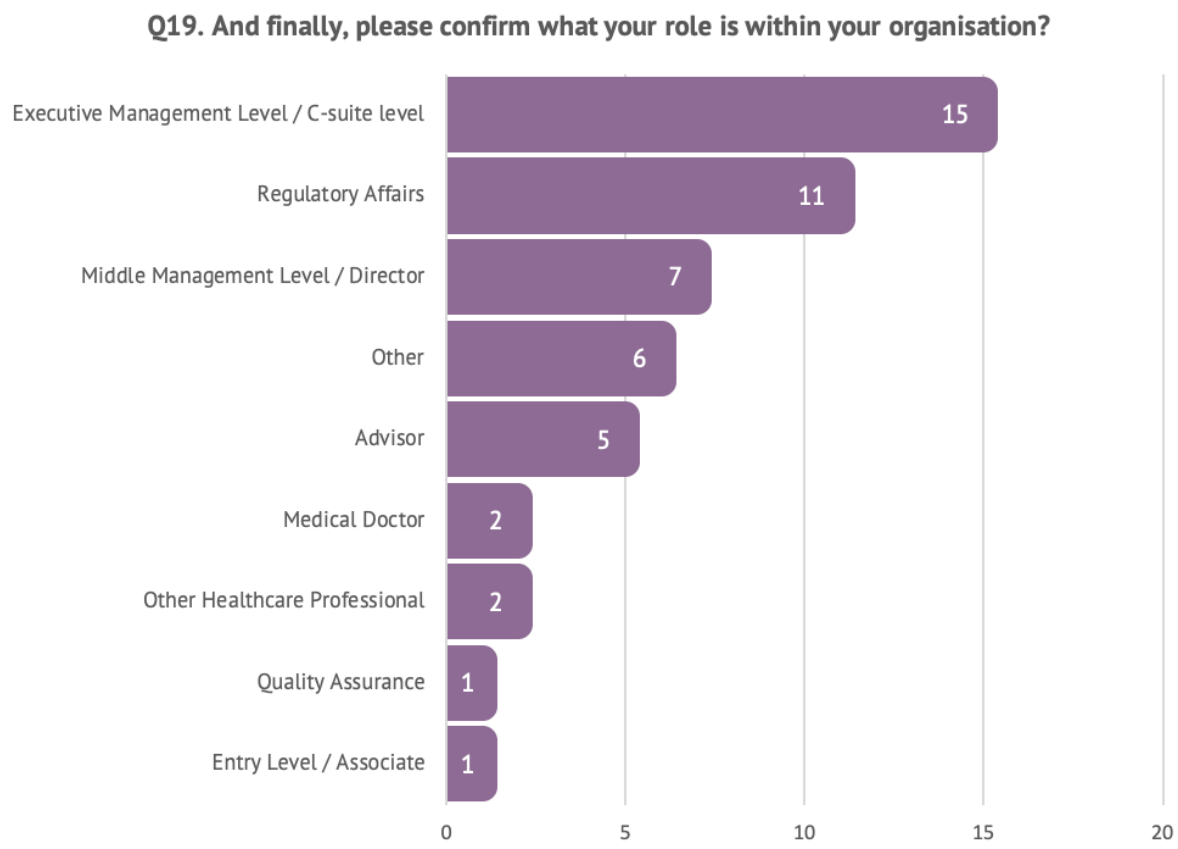
Most common answer was formal standards (43), followed by industry-driven standards (25), and NHS standards (23).

Q17. Which areas or challenges do you find most difficult to identify and / or implement standards and knowledge for?



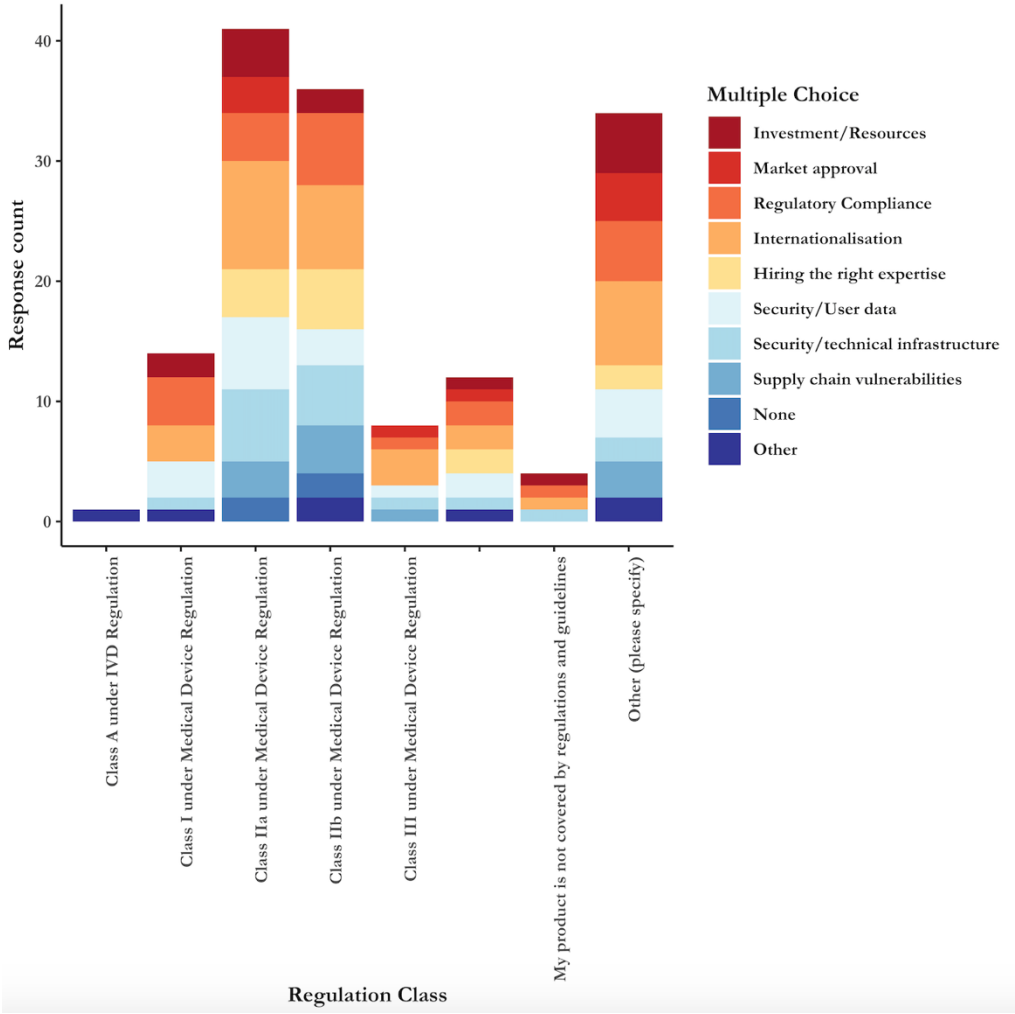
Respondents considered the regulatory standards to be most challenging to apply (20), closely followed by security standards (18). Other challenging areas concern market access (14), organisational challenges (7), the supply chain (7), technical (5) and standards for specific technologies (4).

Q19. And finally, please confirm what your role is within your organisation?

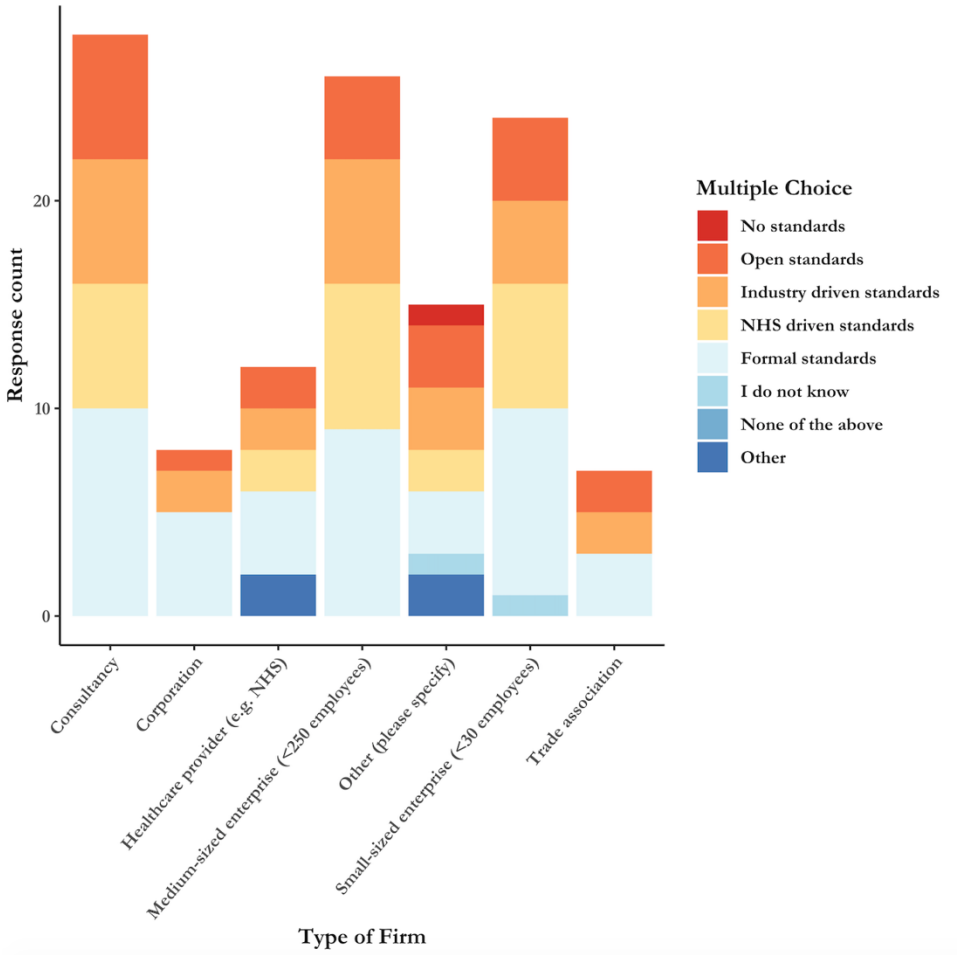


Respondents represented diverse seniority levels within their organisations, including C-suite (15), regulatory affairs (11), middle management (7), advisor (5), medical doctor (2) or other healthcare professional (2), quality assurance (1) and entry level (1).

Additional analysis:



This graph looks at the respondents' perception of the challenges faced, depending on the classification of their device. Hiring seemed to be a challenge for respondent working with Class IIa and IIb, but not for Class I devices. Security challenges related to user data was somewhat more important to respondents engaging with class IIa devices in comparison to class IIb devices. Regulatory compliance was slightly more complex for Class IIb in comparison to Class IIa devices.



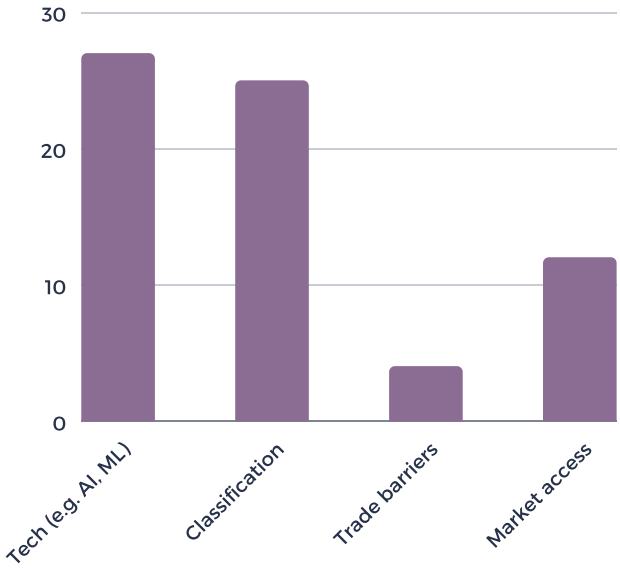
This graph looks at the type of standards that the respective organisations use. It is clear that, across the board, formal standards are most commonly used. This is potentially indicative of the importance that harmonized standards play.

Regulatory and standardization challenges for intelligent and connected medical devices

UCL IN PARTNERSHIP WITH BSI

WHAT IS THIS ALL ABOUT?

As medical devices become increasingly connected and intelligent, several challenges emerge around safety, security and regulatory frameworks. For this research interviews with 19 stakeholders involved with medical devices were conducted, as well as a survey with 50 respondents, to identify regulatory gaps, emerging trends, new safety and security risks, and the role of standards in the new digital era.



REGULATORY CHALLENGES

Survey respondents found regulations around advanced technologies (27) and product classification (25) most challenging. The survey reflects uncertainties and regulatory gaps for combination products and advanced technologies. Most respondents (46) reported that the MDR has increased the burden of regulatory compliance, due to up-classification and more onerous requirements.

INNOVATION CHALLENGES

Regulatory burdens are seen as the main challenge for organisations in the industry, followed by hiring expertise, and having enough resources to go through rigorous testing and regulatory compliance.

THE ATTITUDE TOWARDS STANDARDS

Standards ensure patient safety, through quality assurance of device designs, organisational processes and information governance.

Standards can be used as a competitive advantage and to enable quicker market access.

Standards are hard to interpret and implement.

There are standardization gaps around cybersecurity and advanced technologies.

52%

of survey respondents noted that their device classification changed under the MDR

100%

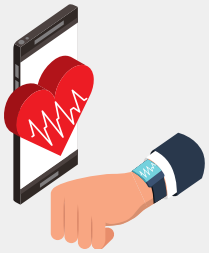
of survey respondents engage with standards

74%

of interviewees said AI will be the main trend

BLURRED LINES

The lines between digital health and clinical use of devices are increasingly blurred. The differences between wellness devices and medical devices are often not clear. This creates regulatory, safety and classification challenges.

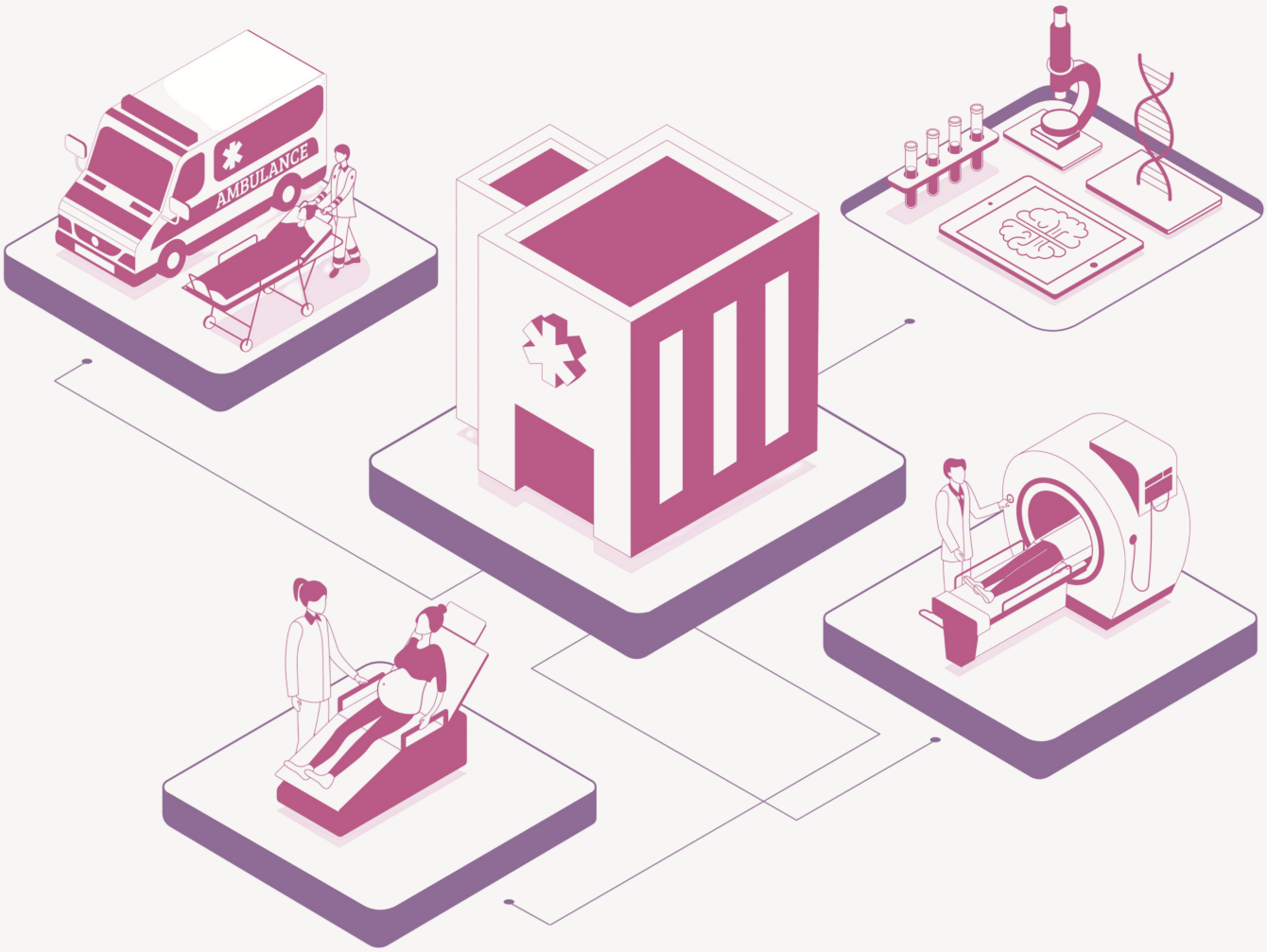


NEW RISKS

Negative interactions between software and the IT environment can threaten patient safety, and increased connectivity makes devices more vulnerable to cyber attacks.

ENTREPRENEURS' GUIDE

To Navigating the Regulatory & Standardization Landscape for Connected and Intelligent Medical Devices



UCL In Partnership with bsi.

CONTENTS

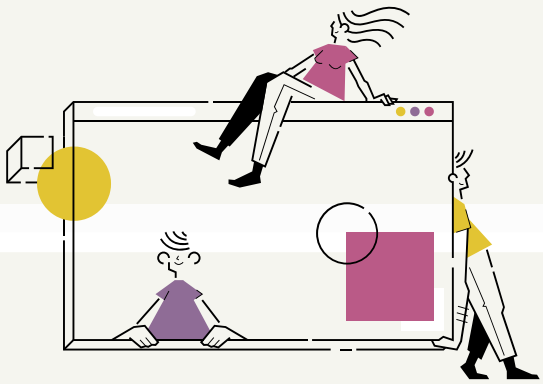
Introduction

What is the guide about?

Regulatory and standardization frameworks for medical devices can be difficult to navigate, especially for smaller market players and newcomers. Regulatory provisions may be particularly challenging to apply to innovative medical devices, for instance, incorporating software or advanced algorithms.

To respond to this problem, this document provides clear, practical guidance for manufacturers of connected and intelligent medical devices. The objective is to help any entrepreneur in the sector navigate the regulatory and standardization landscape. This guide also signposts relevant resources, accounts for common safety and security risks and provides resources explaining the fundraising process.

This document will guide you through the key considerations you should bear in mind at each step of developing your device. A summary of key points is presented in the last page of this guide.



About Project

This guide is one of the outputs of an eight-month collaboration between University College London's Department of Science, Technology, Engineering and Public Policy (UCL STEaPP) and the British Standards Institution. The research identified the need to provide start-ups, entrepreneurs and SMEs with simple guidance on how to navigate the regulatory and standardization landscape for intelligent, connected medical devices. For further details, refer to the main project report.

The UCL STEaPP team comprised five Master's of Public Administration in Digital Technologies and Policy candidates, mentored by Dr Irina Brass.

Medical Device Lifecyle

01	CONCEPT	*An initial evaluation of a possible commercial product*
02	PLANNING	*The design input definition, based on user needs and technical requirements*
03	DESIGN	*The development of product design and of manufacturing process, verification and validation*
04	VALIDATION	*Final validation of the manufacturing process and preparation for market entry*
05	LAUNCH	*Following regulatory approval, the medical device can be launched into the market*
06	POST-MARKET	*Focus on traceability and efficient reporting of errors*
07	RETIREMENT	*The end-of-life of the product, including safe disposal and retirement*

Software Lifecycle

01 SOFTWARE DEVELOPMENT

02 SOFTWARE INSTALLATION AND OPERATION

03 SOFTWARE MAINTENANCE

04 TROUBLESHOOTING

05 DEINSTALLATION

REGULATORY OBLIGATIONS

The software lifecycle covers all aspects from ideation to the de-installation or decommissioning of the product.

Importantly, both the MDR and the MDD require software manufacturers to develop it “in accordance with state of the art”. This has important implications for the device lifecycle. According to the MDR, manufacturers must take “into account the principles of development lifecycle, risk management, including information security, verification and validation”.

Regulations

- Medical devices are highly regulated which means that you need to comply with numerous requirements if you work with them.

- This guide provides guidance for manufacturers, but you may also have responsibilities if you work with medical devices in a different capacity, for instance as an importer or a distributor.

Resources

- **Click here for useful guidance and updates from the European Commission**

- **Click here for latest documents from the MHRA on the post-transition framework**

Note

- **If you want to sell devices in the EU and Great Britain, you will have to comply with two different regimes**

- **You should monitor the legislative process in the UK to stay up-to-date with the changes**

RECENT TRENDS AND LIKELY CHANGES

Both in the EU and the UK, there has been significant regulatory activity.

European Union

- The MDR will apply from 2021, but certificates for low-risk devices will be valid until May 2024.

- The IVDR will apply from 2022, but certificates for low-risk devices will be valid until May 2027.

If you have not yet done so, you should prepare for the new EU Regulations

United Kingdom

Brexit will have significant implications for manufacturers

- **The MHRA's guidance** - after 1 January 2021 there will be a new regulatory regime in Great Britain. Medical devices will have to register with the MHRA and affix a new UK Conformity Mark, but CE marks will be valid until June 2023. Importantly, different regime will apply in Northern Ireland where the EU framework will continue to apply.

- **Medicines and Medical Devices Bill** – envisages strengthening the MHRA.

- **Independent Medicines and Medical Devices Safety Review** (known as the Cumberlege Report) – contains recommendations on improving patient safety, for instance by establishing safety-focused institutions and overhauling the MHRA.

Obligations in the EU

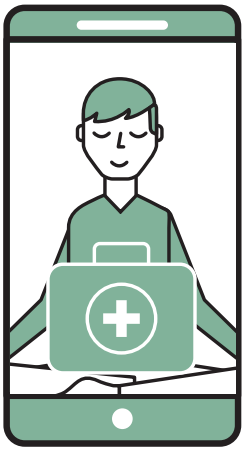
Is my device a medical device?

- This depends on its intended purpose. If it is used for diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, it is likely to be a medical device.

- Check Article 2 of the MDR/ IVDR. These regulations broadened the definition of a medical device, so you may be caught by the regime even if your device was previously unregulated.

MYTH

I have developed a phone app, so it is not a medical device.



BUST

WRONG. Your app may still be a medical device if it has a medical purpose. If your app is in the healthcare space, check the MDR and the IVDR for specific definitions.

What are the key obligations for manufacturers?

The MDR imposes important obligations across the entire lifecycle. Article 10 of the MDR outlines your key obligations.

You need to have in place the following:

- Risk management and quality management system, you must conduct clinical evaluations, compile technical documentation and have in place mechanisms to cover the financial responsibility

Internal organisation

- You need a person responsible for regulatory compliance
- If you are based outside of the EU, you will need an authorised representative (Article 11) - this applies to companies based in Great Britain after Brexit

Design requirements

- Devices must be designed and manufactured in accordance with Annex I MDR, listing General Safety and Performance Requirements

Click here to learn more about the General Safety and Compliance requirements

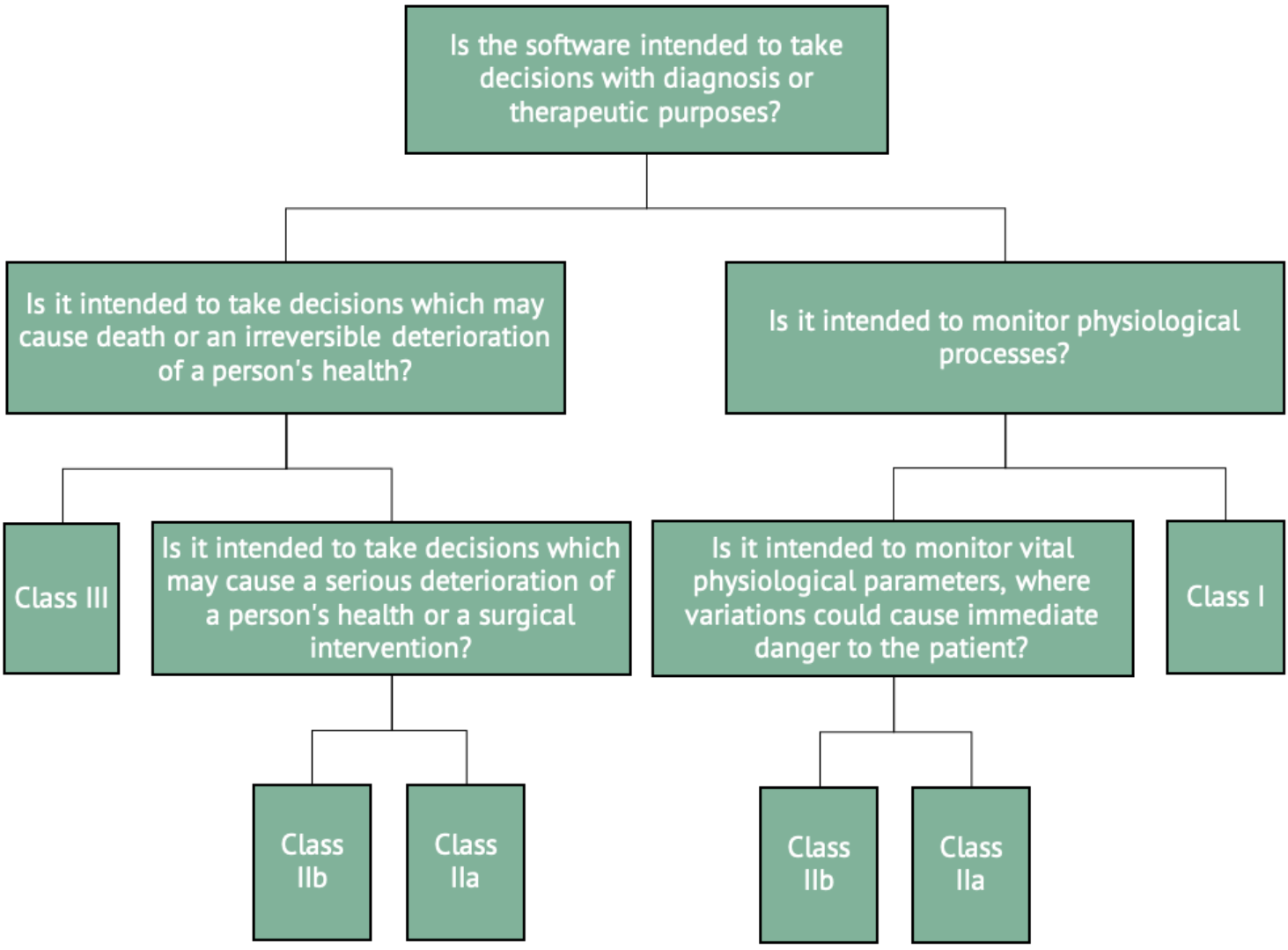
Market Entry Preparation: Classification

The classification process depends on the nature of your device.

If your software drives or influences the use of a device, it will fall within the same class as the device. Follow Classification Rules in Annex VIII. Click here to learn more about medical device classification.

If your software is independent of any other device, it will be classified in its own right under Rule 11 of Annex VIII MDR.

The process is:



CHECKLIST: PREPARATION FOR MARKET ENTRY

- ◯ Establish the risk class of your device (Annex VIII) – this is a crucial step as it will determine the regulatory compliance obligations
- ◯ Compile technical documentation (Annex II and III)
- ◯ Conduct clinical trials to ensure safety and verify performance (Articles 62-80)

Click here to learn more about medical device classification

CHECKLIST: PLACING DEVICE ON MARKET

- ◯ Pass a conformity assessment – the process depends on your device characteristics and is not required for Class I devices
- ◯ Provide a declaration of conformity
- ◯ Place a CE mark on your device
- ◯ Assign UDI to your device
- ◯ Provide information to Eudamed

Click here to learn more about conformity assessment

NOTIFIED BODIES

To undertake a conformity assessment, you need a Notified Body.

Currently 15 Notified Bodies are designated, but the European Commission is planning to appoint further ones.

Click here for an up to date list of Notified Bodies

Remember: due to Notified Body capacity, the assessment process may take several months

INFORMATION ABOUT POST-MARKET SURVEILLANCE

POST-MARKET OBLIGATIONS

Once your device is on the market, you have proactive and reactive obligations. You need to submit a Post Market Surveillance Report (Class I devices) or a Periodic Safety Update Report (Class IIa, IIb, III) (Article 85 and 86 MDR).

You are also responsible for Post Market Clinical Performance Follow Up (Annex XIV)

- You must record any notable changes that impact the initial data

You also have vigilance obligations to report serious incidents (Article 87)

- Vigilance reports must be submitted to the pan-European database

You must inform your Notified Body about significant changes to your device.

- **Remember: your responsibilities continue when devices are placed on the market and you must have in place systems to cover financial responsibility**

- **Click here to learn more about your post-market obligations**

MDR Classification	Submission	How often?
Class I	PMSR	Upon request
Class IIa	PSUR	Minimum every 2 years
Class IIb	PSUR	Minimum every year
Class III	PSUR	Minimum every year

Common Risks: Safety and Security

The rise of connected, intelligent medical devices offers significant benefits for the healthcare system, especially by improving patient care and automation of certain processes, thus increasing the efficiency of the healthcare system.

However, the increased connectivity in medical devices exposes them to cybersecurity and safety vulnerabilities which can threaten patient safety and privacy. Hence, this section provides useful guidance on how to incorporate **security and safety** principles throughout the device lifecycle.

FOUR KEY PRINCIPLES TO FOLLOW FOR SECURE MEDICAL DEVICES

- **Security throughout the lifecycle** – The security of medical devices should be considered at all stages from the pre-market, post-market and retirement/decommissioning stages.
- **Security by design** – The security of the medical devices has been considered, designed and applied, ensuring best practices and the following key security characteristics are practiced across the whole lifecycle: Availability, integrity, accountability and confidentiality.
- **Security by default** – The medical device includes sufficient capability to function according to the characteristics at the initial deployment.
- **Verifiable security** – All three principles should be verifiable.

Click here for IMDRF Cybersecurity Principles and Practices

Click here for EU MDCG Cybersecurity Guidance

Common Risks: Safety and Security

A medical device is said to be clinically effective when it has the effect intended by the manufacturer for the medical condition.

ESSENTIAL PRINCIPLES OF SAFETY AND EFFECTIVENESS FOR MEDICAL DEVICES

- **"A medical device has to be designed and developed ensuring that:**
- **All risks associated with the use of the device are compatible with a high level of health and safety and acceptable risks must be eliminated when weighed against the intended benefit to the patient.**
- **The clinical condition or safety of the patient, or the health and safety of the user would not be compromised under the circumstances and for all the intended purposes for which the device was designed.**
- **A well reasoned and documented investigation of any foreseeable risks is carried out by the manufacturer in order to use the device and compare these risks with a well reasoned and documented analysis of the benefits."**

Click here for IMDRF Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices

Click here for BSI General Safety and Performance Requirements (Annex I) in the New Medical Device Regulation

BEST PRACTICES FOR SOFTWARE DEVELOPMENT FOR MEDICAL DEVICES

- Software will also need to be validated and verified on its own as part of the regulatory process. One big challenge for software developers is to adhere to the same set of rigorous regulations as the more traditional manufacturers.
- Software will be held to the same standard as hardware and will go through validation and verification processes.
- Apart from ensuring you fulfil the criteria when gathering the technical requirements and deciding on infrastructure, there are some best practices or tips you can apply in your organisation.
- While this is a very broad topic, here are a few actions any software team should be aware of and understand.

- Implement a Compliant Quality Management System (QMS).
- Implement Digital Document Control for Fully Electronics QMS.
- Ensure documentation. For medical device companies, this would include assembling a Design Technical File and providing evidence that the organisation operates in an ISO13485-compliant QMS. Your software team should be integrated into your overall QMS.
- Plan for device interoperability from the first day. The device will likely need to be able to use different protocols from various vendors.
- Clearly separate any code built for the device, and any non-device code, i.e. independent source code repositories.
- Continuous integration means merging everybody's work together frequently and running automated tests on it. Remember that this is a common approach among software teams, a highly collaborative environment, but it is crucial that other teams, scientists and researchers, are also incorporated in this process.
- Think about security, safety, and regulations from day one, and ensure the developers are aware of the process and technical requirements prior to starting.

Other Frameworks: United States

The US Food and Drug Administration (FDA) is the oldest and most comprehensive consumer protection government agency.

Their aim is to promote and protect health. Within the FDA, the Center for Devices and Radiological Health (CDRH) is responsible for protecting and promoting public health.

Key Website: https://www.fda.gov/medical-devices

Useful Resources

- Click here for Standards (Medical Devices)
- Click here for General Guidance Documents
- Click here for Digital Health Resources
- Click here for Cybersecurity Guidance
- Click here for Artificial Intelligence and Machine Learning (AI/ML) in Software as a Medical Device
- Click here for Device Software Functions, including Mobile Medical Applications
- Click here for Health IT
- Click here for Medical Device Data Systems
- Click here for Medical Device Interoperability
- Click here for Software as a Medical Device
- Click here for Telemedicine
- Click here for Wireless Medical Devices
- Click here for CDRH Learn (Learning modules describing many aspects of medical device regulations, covering both premarket and post market topics)

Other Frameworks: Data Protection

General Data Protection Regulation (GDPR)

- The GDPR provides guidance on data protection and privacy in the EU and the European Economic Area.

UK Data Protection Act 2018

- The Data Protection Act 2018 is the UK's implementation of the GDPR.

KEY DATA PROTECTION AREAS

- Informed Consent Criteria
- Data Concerning Health Scope
- Pre-GDPR data collection
- Right to be forgotten (applies to commercial collection of health data)
- Data Protection Impact assessment (DPIA): Data concerning health /profiling
- Profiling requirements: Including right to object if processing significantly affects data subject
- Data portability right of user
- Security requirements
- Export of data to outside EU Jurisdictions

Standards

- ***Standards are an agreed best practice and cover a range of activities.***
- Throughout the lifecycle of medical devices, standards serve to ensure the safety, quality and performance of these devices.
- Standards may be developed at different levels - international, regional, national and sector. They may be further categorised into basic, process, group / horizontal and vertical standards.
- This section aims to provide you with an overview of key standards across various categories, as well as resources for navigating the UK standards landscape.

ENGAGING WITH STANDARDS FROM DAY ONE

- **Find out what standards may be applicable to the device you are developing, by referring to the list of standards below or on the websites of the relevant healthcare providers, regulators and standards bodies.**
- **To commence the certification process, get in touch with a Notified Body who is authorised to perform the conformity assessment in the relevant market. This will involve an audit process, which may require the submission of technical documents pertaining to your device.**
- **A certificate of registration will be issued after the Notified Body has assessed that:**
  - **Information provided by the applicant is sufficient with respect to the certification requirements and scope from certification**
  - **All major non-conformities have been closed out**
  - **The plan for correction and corrective action for all outstanding minor non-conformities have been reviewed and accepted.**
- **To maintain this certification, take care to ensure that terms of the certification continue to be met. This certification may be suspended, withdrawn or reduced in scope under certain conditions.**

HARMONIZED STANDARDS

- You may have also heard of the term “harmonized standards”. In the European context, this refers to a European standard developed by a recognised European Standards Organisation (CEN, CENELEC, ETSI). In other words, these standards are uniform throughout Europe.

- The use of these standards is voluntary. Compliance with harmonized standards provides presumption of conformity with relevant EU regulations and mandatory legal requirements. This essentially means that compliance with these standards could facilitate access to many European markets.

- For the transition to the new Medical Device Regulation and In Vitro Diagnostic Medical Device Regulation, the European Commission has requested for harmonization of standards. This is still in progress.

MYTH

Only multinational corporations can participate in the standards making process.

BUST

No, nominations of committee members are typically made through profession bodies. There are currently 1,350 BSI committees and over 12,200 standards-makers, comprising volunteers from a variety of professions and industries.

Apply here if you have experience in the standard you want to help develop

OR

Contact BSI at standardsmakers@bsigroup.com should you have further queries on the next steps.

MYTH

The standards landscape is really complicated.

BUST

There are many resources to guide you through this landscape. Here are some UK organisations which may be able to provide you with guidance and support:

Medicines and Healthcare products Regulatory Agency (MHRA)
Innovation Office

Phone number: + 44 203 0806000
Email: info@mhra.gov.uk
Click here for online enquiry form

British Standards Institution
Phone number: +44 345 080 9000
Click here for online enquiry form

BSI also offers a Compliance Navigator, which could aid in keeping track of applicable standards and regulations

N*ote: Regardless of the outcome of the Brexit trade deal, BSI will continue to be a Notified Body designated under the MDR.*

Association of
British HealthTech Industries Ltd

Phone number: +44 (0)20 7960 4360
Email: enquiries@abhi.org.uk

The British In Vitro Diagnostic Association
Phone number: +44 (0)3333 208 823
Email: membership@bivda.org.uk

Key Standards

Basic standards

Applicable to multiple sectors

- BS EN ISO 9001 Quality management systems
- BS EN ISO/IEC 27000 Information Security Management
- BS EN ISO 31000 Risk management

Process standards

- BS EN ISO 27799 Information security management in health using ISO/IEC 27002
- BS EN ISO 13485 Quality Management System
- BS EN ISO 14971 Application of risk management to medical devices
- BS EN 62366 Application of usability engineering to medical devices
- BS EN 62304 Medical device software. Software life-cycle processes
- BS EN 80001 Application of risk management for IT-networks incorporating medical devices
- BS EN ISO 10993 Biological evaluation of medical devices
- DCB0160 Clinical risk management. Deployment and use of Health IT Systems
- DCB0129 Clinical risk management. Manufacture of health IT systems
- DCB0086 Data Security and Protection Toolkit
- DCB3051 Identity Verification and Authentication Standard for Digital Health and Care Services
- CEN/ISO TR 20416 Medical devices - Post-market surveillance for manufacturers

Group / horizontal standards

Applicable to a wide range of medical devices

- BS ISO 16142 Recognized essential principles of safety and performance of medical devices
- BS EN 60601-1 Medical electrical equipment
- BS EN 60601-1-9 Requirements for environmentally conscious design

Vertical Standards

*Applicable to **Health IT networks***

- BS EN ISO 13606 Electronic health record communication
- BS EN ISO/IEEE 11073 Point-of-care medical device communication
- DCB1596 Secure email

Vertical Standards

*Applicable to **blood glucose monitoring devices (as a specific example of IVDs)***

- BS EN ISO 15197 Requirements for blood-glucose monitoring systems for self-testing in managing diabetes mellitus
- BS EN ISO 11073-10417 Personal health device communication: Glucose Meter

Legend

- International Standards / Technical Reports adopted in the EU
- International Standards
- European Harmonised Standards
- UK Healthcare System Standards

Fundraising Opportunities

The healthcare sector is one of the most impactful sectors, and medical devices play a crucial role in developing and disrupting the health system and patient care. Ensuring you have enough capital for your device to be allowed on the market can be complicated.

So, how can I access funding? There is a myriad of different routes, ranging from traditional bank loans, to corporate financing, venture capital, government-backing and grants.

VENTURE CAPITAL

Venture capital (VC), a form of private equity typically invested in high-growth opportunities fuelled by technology, provides early-stage and late-stage financing. Medical device VC-firms specialise in providing companies with the resources, capital, and expertise to grow the company, ensure compliance, and bring the product to market.

What do they look for?

While all investors have different criteria, a few factors are common to assess:

- Sizeable market opportunities.
- Technology and scalability
- Safety and security of the device
- Business and technical risks
- Does the device have a proven clinical need?
- Who is the end-user for the device?

How do we find VC-investors?

All VC-firms have a different focus area in terms of when in a company's cycle they invest, in what geographical regions, and sectors. Do your research to identify any firms and investors with criteria that match your start-up.

A few helpful resources to identify companies and their investors in your industry and area include:

Click here for Crunchbase resources

Click here for Index resources

CORPORATIONS

- Corporate investment is another way to bring liquidity to the company while partnering with a more significant player to increase credibility and access more resources.

- At times, corporations can request to obtain distribution rights or look at acquiring the company. These can be more traditional medical device companies or technology companies.

GOVERNMENT-BACKED FUNDING AND INNOVATION GRANTS

There are opportunities to apply for grants to support the company. The type of grants and funding available, and the sectors and ideas they cover, vary. The first idea is to look for any innovation agency in your specific country. A few helpful resources to search for grants:

- Click here for Innovate UK resources
- Click here for NHS Innovation resources
- Click here for European Commission resources
- Click here for Vinnova, Sweden's Innovation agency
- Click here to learn more about Innovation Competitions, UK

SUMMARY

Remember, as a manufacturer of a medical device you have various obligations at each lifecycle stage

CONCEPT

- Determine whether your device is classified as a medical device and review the relevant regulations and standards
- Identify resource requirements and potential routes to market
- **Applicable standards: ISO 13485, ISO 14971, ISO 16142, EN 62304**

PLANNING

- Prototype development, risk analysis and setting regulatory strategy
- Find a Notified Body and establish the likely class of your device
- **Applicable standards: ISO 13485, ISO 14971, DCB0129, DCB0160**

DESIGN

- Comply with the General Safety and Security Requirements in Annex I
- Apply Safety and Security by design principles
- Develop product roadmap and gather user and technical requirements
- **Applicable standards: ISO 13485, ISO 14971, ISO 16142, EN 62366**

VALIDATION

- Conduct trials and compile technical documentation
- Set market plan
- **Applicable standards: ISO 13485, ISO 14971, ISO 16142, ISO 22799, DCB0160**

LAUNCH

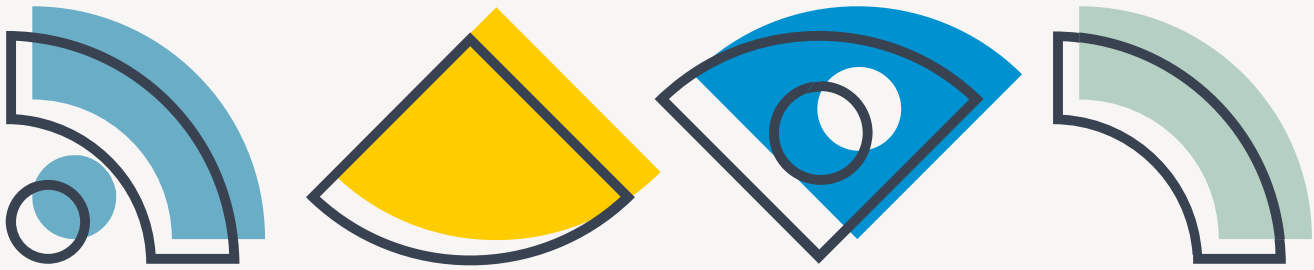
- Undertake conformity assessment and provide a declaration of conformity
- Attach CE mark and assign UDI
- Execute commercial activities such as marketing and establish sales channels
- **Applicable standards: ISO 13485, ISO 14791, ISO/IEEE 11073, ISO 13606, DCB3051**

POST-MARKET

- Comply with your post market surveillance and vigilance requirements
- Ensure software updates comply with regulations; if needed recertify your device and assign a new UDI
- **Applicable standards: ISO 13845, ISO 14971, ISO/TR 20416**

RETIREMENT

- Ensure safe and secure disposal of a device
- **Applicable standards: ISO 13485, ISO 14971, IEC60601-1-9**



COVER PAGE ILLUSTRATION CREDIT: ITG.DIGITAL & CANVA