Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira, Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27755-cd

Emerging Risks and Epistemic Uncertainty in Medtech Industry Innovation

Roberto Filippini

PhD Independent Scientific Consultant. E-mail: filippini.consulting@gmail.com

Bernardo Innocenti

BEAMS Department, Universitè Libre de Bruxelles, Belgium. E-mail: bernardo.innocenti@ulb.be

Abstracts
Innovation is an intrinsic characteristic of the medical technology (MedTech) industry and a major driver of improved healthcare outcomes. Recent advances in digitalization, artificial intelligence (AI), telemedicine, and advanced robotics are drastically transforming diagnostics, treatment, and care delivery. At the same time, these innovations challenge established safety and risk management paradigms, as novel technologies are often introduced into clinical practice before sufficient knowledge is available to fully characterize their risks. This situation creates a structural mismatch between the innovation speed and the maturity of regulatory frameworks. This paper analyses innovation in healthcare and MedTech from an engineering perspective, with a particular focus on emerging risks and epistemic uncertainty. It argues that traditional risk assessment approaches, largely developed for mature technologies, are inadequate to address the complexity, adaptiveness, and interconnection of modern medical systems. To address this limitation, an epistemic risk assessment model is proposed that explicitly distinguishes between known and unknown risks and emphasizes the uncertainty associated with risk estimates at market entry and throughout the product lifecycle.
The applicability of the proposed model is presented through representative examples, including digital healthcare systems, telemedicine and personalized healthcare, AI-based medical devices, and advanced robotics, with explicit reference to Medical Device Regulation risk classes. These examples demonstrate that, while innovation delivers clear benefits, it also amplifies uncertainty in risk estimation, increases exposure to unknown risks, and challenges conventional post-market surveillance strategies.
The paper concludes that the explicit integration of epistemic uncertainty into benefit–risk analysis, and its transparent communication, are essential to support informed decision-making, responsible innovation, and sustained trust in healthcare and MedTech technologies.

Keywords: MedTech, innovation, risk assessment, AI, surgical robots, medical device.

1. Introduction

Innovation is an intrinsic characteristic of the medical technology (MedTech) sector and represents one of its primary drivers of growth, competitiveness, and societal impact (MedTech Europe, 2020). Compared with other industrial domains, MedTech consistently ranks among the most innovative sectors, both in terms of technological advancement and patent activity. This strong innovation capacity is further supported by the structure of the industry itself, which is dominated by small and medium-sized enterprises and start-ups, accounting for approximately 95% of companies, thereby creating a highly dynamic ecosystem that is particularly receptive to technological change (Innocenti and Galbusera, 2022; MedTech Europe, 2020).

A distinctive feature of MedTech innovation is that it rarely emerges in isolation, but often results from the transfer and adaptation of technologies originally developed in other sectors. This cross-sectoral transfer has accelerated both the rate and speed of innovation, expanding the range of medical applications. Areas of innovation are diagnostics through artificial intelligence (AI), telemedicine and remote care via the Internet of Things (IoT) and wearable devices, surgery through advanced robotics, including autonomous, miniaturized, and nanoscale systems. In parallel, big data analytics, often combined with AI, large language models, and blockchain technologies, are reshaping

how medical information is generated, processed, and exploited (Thacharodi et al., 2024).

The MedTech ecosystem include large industrial players, start-ups, academic and research institutions, regulatory bodies, healthcare providers, and the end users (Innocenti and Galbusera, 2022; MedTech Europe, 2020). These stakeholders are familiar with continuous technological evolution and tend to associate innovation with improved performance, increased efficiency, higher profitability, and gains in market share. Healthcare users and organizations similarly tend to focus on the advantages of innovation, particularly in terms of improved clinical outcomes and operational efficiency (DNV, 2025, 2024; Innocenti and Galbusera, 2022). However, this innovation-driven mindset emphasizes benefits more than risks associated with the introduction of novel technologies (MedTech Europe, 2020). For example, digitalization is widely regarded as a key enabler for interoperability between medical devices and healthcare systems, nonetheless increased exposure to cyberthreats and vulnerabilities associated with interconnected digital systems is frequently underestimated (Filippini and Spiller, 2024). The growing reliance on AI, which stands out as one of the most promising innovations (van Kolfschooten and van Oirschot, 2024), raises fundamental questions regarding safety, and emerging risks related to data reliability, bias, and loss of situational awareness when technology is unreliable or fails (DNV, 2025, 2024; Thacharodi et al., 2024).

These emerging risks are cross sectorial and prompted the introduction of new regulatory instruments such as the cyber-resilience Act (European Parliament, 2024a) and the AI Act (European Parliament, 2024b), which will also apply to the healthcare and MedTech sector. For instance, the integration of the AI Act into the Medical Device Regulation (MDR), revises roles and responsibilities of healthcare professionals, thus increasing compliance burdens and ethical concerns (FDA, 2024a, 2024b). For similar reasons, technical standards are undergoing review, but the adaptations are lengthy, if compared to the rapid pace of technological evolution. Good practice is to complement norms with technical guides, but such documents are provisional, subject to interpretation, exceptions, and lack of homogeneous application. Differences between regulatory approaches in the European Union (MDR) and the United States (FDA) further illustrate this challenge, with the former generally adopting a more precautionary stance and the latter emphasizing flexibility and expedited approval pathways.

This paper addresses the role of innovation from in the MedTech industry and explores emerging risks through the development of an epistemic model for risk assessment. Traditional risk assessment is revised by associating the degree of knowledge of the analysed system and the related risks uncertainty, see section 2. This approach aims to support more informed and robust decision-making, by increasing awareness of uncertainty on the benefit–risk ratios. This has direct implications for benefit–risk evaluation at the time innovative technologies are integrated into certified healthcare systems and medical devices. These ideas are exemplified in section 3 for emerging technologies in the Healthcare and Medtech industries.

2. An epistemic model for risk assessment

2.1 *The foundations*

The risk management process for medical products is defined in ISO 14971(International Organization for Standardization (ISO), 2019) and includes system analysis, risk assessment, risk evaluation, benefit–risk analysis, and post-market surveillance. The goal of risk management is to demonstrate that a medical device is and remains safe (i.e. free from unacceptable risks) along its life cycle, under normal conditions of use and reasonably foreseeable failure scenarios. System analysis is essential for risk assessment, as it identifies failure scenarios from multiple system perspectives, including the architecture, the functional descriptions, the data flows, behavioural and state-based representation, the operating environment etc. System analysis outcomes are influenced by both aleatory and epistemic uncertainties, especially within innovation-driven development processes. Unlike conventional approaches that assume relatively mature and well-understood technologies, innovation introduces a significant fraction of epistemic

uncertainty arising from incomplete, unknown a-priori knowledge of the system behaviour, and dynamic interactions with users and operating environments. This uncertainty is intrinsic to risk assessment and, if it cannot be eliminated, eventually it must be understood, managed, and communicated.

2.2 *The epistemic model*

The epistemic model draws inspiration from the work of Aven (Aven and Krohn, 2014), which defines four subsets: Known, Unknown Known, Known Unknown, and Unknown. These subsets reflect increasing degrees of epistemic uncertainty, from the complete knowledge (K-subset) to the absence of knowledge (U-subset). The epistemic model stems from the state-space representation of the system in functioning and failed states, and applies to the failed states only, see Figure 1. Aleatory uncertainty is not incorporated into the model. Specifically, while the Known subset does not include epistemic uncertainty it may still be subject to aleatory uncertainty.

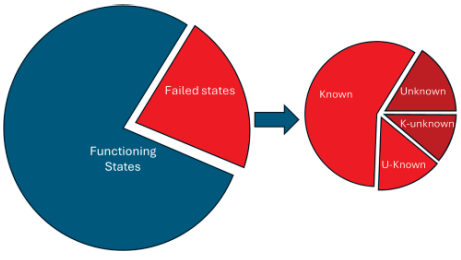

Fig. 1. Subsets of the epistemic model.

The elements of epistemic model subsets are the failure scenarios. A **failure scenario** describes the transition from a functioning state to a failed state. It originates from a single cause or multiple causes (either independent or correlated), and it is defined by the triplet of attributes {*failure process, failure data, failed state*}, where each attribute is associated the values "known" and "unknown". The binary graph of Figure 2 explores all possible combinations of values (2^3 = 8) and it ends up into six subsets. The K-subset contains known failure scenarios. The UK-subset assumes that the failure process is known, while at least one of the other attributes {*failure data, failed state*} is unknown. The resulting subsets are UK1 (unknown failed state), UK2 (unknown failure data), and UK3 (unknown failure data and failed state). The KU-subset assumes that the failure process is unknown, and because of that uncertainty of the failure data is not queried. Conversely the failed state is known, which means that the outcomes of the failure scenario are known, but the failure process is either too complex to describe or unknown. Rare events belong to this subset. Finally, the U-subset contains failure scenarios that were not identified by system analysis and remain completely unknown.

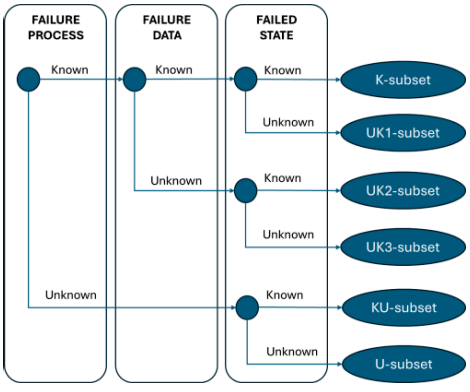

Fig. 2. Uncertainty graph and the epistemic subsets.

Two types of uncertainty characterize the epistemic model: a) absolute uncertainty (*), i.e. the absence of any a priori knowledge of the entire failure scenario; b) partial uncertainty (**), i.e. lack of a priori knowledge of certain attributes of the failure scenarios. The U-subset is affected by absolute uncertainty, whereas UK1, UK2 and UK3 are affected by partial uncertainty. The K-subset is not affected by uncertainty. However, as will be clarified in the following sections of the paper, this may only hold true at time zero. In this paper, it is assumed that the K-subset contains mature technology. The UK subsets (UK1, UK2 and UK3) and KU subset include mature and new technologies and U-subset only includes new technology.

2.3 *Uncertainty and Risk assessment*

The epistemic model is transformed in a probabilistic model by assigning risk metrics (likelihood and severity) to each element of the subsets. This allows the definition of individual risk, overall risk and overall residual risk.

The **individual risk** is the pair P and S associated to the failure scenario, where P is range of likelihood (often expressed as frequency) and S is a range of severity associated to the harm to the patient.

The **overall risk** is the total of all individual risks. It is a random variable in S, result of the sum of the risk random variables associated to the four disjoint subsets:

$$R(t) = R_K(t) + R^*_{UK}(t) + R^{**}_{KU}(t) + R^{**}_{U}(t) \quad (1)$$

$$R^*_{UK}(t) \stackrel{\text{def}}{=} R^*_{UK1}(t) + R^*_{UK2}(t) + R^*_{UK3}(t)$$

The notation reflects both the subsets and the type of uncertainty, defined in the previous section, and includes dependency with time t. Only the first two terms of (1) are carried over for risk evaluation and risk reduction. The third term is not analysed, and the fourth term is completely unknown.

The **overall residual risk**, after the risk reduction by risk control measures, is:

$$\bar{R}(t) = \bar{R}_K(t) + \bar{R}^*_{UK}(t) + \Delta R^{**}(t) \quad (2)$$

$$\Delta R^{**}(t) \stackrel{\text{def}}{=} R^{**}_{KU}(t) + R^{**}_{U}(t)$$

The first two terms are reduced below the acceptable risk threshold. Nonetheless a residual uncertainty remains for the second term, due to the partial uncertainty of the subsets UK1, UK2 and UK3. The third term is the sum of the risks in the unknown subsets. Its contribution can be significant such to exceed the acceptable risk threshold.

Equations (2) and (3) use a non-computational notation. The most appropriate mathematical formulation is the probability distribution in S:

$$\bar{p}(s,t) = \bar{p}_{\mathrm{K}}(s,t) + \bar{p}^*_{UK}(s,t) + \Delta p_{\mathrm{U}}(s,t) \quad (3)$$

Where the cumulative probability at time t is the probability that the system has failed.

$$\sum_{s\in S} \int_0^t \bar{p}(s,t)dt = P(Failed\ state, t)$$

Relative uncertainty from UK-subsets affects the probability distribution along the y axis (UK1), the x axis (UK2) or both (UK3). The term $\Delta p_U(s,t)$ is unknown. This paper does not aim to further develop the model's mathematics, which is reserved for future work.

2.4 *How uncertainty affects the benefits and risks analysis*

Especially for new technology, epistemic uncertainty is highest at market entry and evolves as knowledge accumulates. Yet it is rarely reflected in risk management, and consequently in the determination of the benefit-risk ratio. Current practice mandates to communicate residual risks without explicitly addressing uncertainty and implicitly assuming completeness and invariance of risk estimates. In the context of technical innovation, this assumption is false. Therefore, acknowledging epistemic uncertainty into risk assessment would be essential for at least two purposes. First, it would support informed benefit–risk evaluation and the responsible deployment of innovative medical technologies. Secondly, it would pave the basis for progressive integration of knowledge with data-driven and operational evidence. For example, partial uncertainty is crucial as it highlights where more information is needed.
At present, uncertainty and unknown risks remain outside the scope of conventional risk assessment and benefits risks analysis until they materialize, with negative consequences for patient safety.

3. Examples of Technical Innovation in the Healthcare and MedTech Industry

This section illustrates the application of the proposed epistemic model for risk assessment to selected examples of technical innovation that are increasingly adopted in healthcare and the MedTech industry. Attention is paid to classification under the MDR, as the assigned risk class strongly influences regulatory requirements, risk control strategies, and acceptable levels of uncertainty.

3.1. *Digital Transformation of Healthcare Systems*

Digital transformation is the main layer for several recent innovations. Its scope extends beyond individual medical devices to include healthcare information systems, inter-operability platforms, data infrastructures, and software-based services supporting diagnosis, treatment, and care delivery. From an MDR perspective, many digital solutions fall into class I or IIa, particularly if they provide decision support rather than autonomous decision-making.

The benefits of digitalization are well recognized and include improved efficiency, enhanced continuity of care, better data sharing and data fusion, and support for clinical decision-making. Nevertheless, their integration into complex healthcare ecosystems amplifies the impact of failures. Digital transformation introduces new categories of systemic risks that are not adequately captured by traditional device-centric risk models. These systemic risks arise from complexity and interdependencies between systems, cascading failures across networks, and increased exposure to cybersecurity threats (Filippini and Simensen, 2025).

When mapped onto the epistemic model, digital healthcare systems exhibit known risks typically associated with software faults, data integrity, and cybersecurity vulnerabilities. However, a non-negligible fraction of systemic risks falls in the known unknown subset. Moreover, known risks at time zero may move into unknown known risks, for example because of evolving threat landscape. In conclusion, risk estimates are characterized by epistemic uncertainty and impermanence of initial risk estimates. New approaches for digitalization require, for example, integrated codesign of safety and security (Filippini and Simensen, 2025) adaptive risk management and proactive post-market surveillance.

3.2. *Telemedicine and Personalized Healthcare*

Telemedicine and personalized healthcare build upon digital infrastructures to deliver care to individual patients. Personalized healthcare integrates patient-specific data, including physiological measurements, behavioural information, and, in some cases, genomic data, to support diagnostic and therapeutic decision-making. Depending on their intended purpose and clinical impact, these applications are typically classified as MDR class IIa or IIb.

The benefits of telemedicine and personalized healthcare include improved access to care, earlier interventions, and more effective and targeted treatments. However, emerging risks arise from data quality and completeness, variability in patient behaviour, and reliance on distributed systems operating outside controlled clinical environments. Off-label (unintended) use scenarios are particularly difficult to anticipate, especially when technologies are repurposed or extended beyond their originally intended scope.

Within the epistemic model, telemedicine technologies illustrate the tension between clearly identifiable benefits and uncertain risks. Risk estimates rely heavily on expert judgment, limited clinical evidence, and assumptions derived from analogous technologies. The fraction of unknown known risks (UK-subset) related to long-term use, patient adherence and data drift, is substantial and add up to emerging risks of digital transformation. More than in other applications, here there is the need of acknowledging uncertainty in benefit–risk evaluations and of progressively updating risks as knowledge accumulates through post-market surveillance.

3.3. *Artificial Intelligence in Medical Devices and Healthcare*

Artificial intelligence (AI) is one of the most disruptive innovations in healthcare and MedTech. According to internationally recognized definitions, an AI system operates with varying degrees of autonomy, may exhibit adaptiveness after deployment, and infers outputs—such as predictions, recommendations, or decisions—from input data to achieve defined objectives. Future general-purpose AI models further extend these capabilities across multiple applications, including diagnostics, decision support, and clinical workflow optimization. AI-based medical devices span a broad range of MDR classes, from class I software providing low-risk support functions to class III devices

involved in diagnosis, prognosis, or therapeutic decision-making.

The potential benefits of AI are significant, particularly in terms of diagnostic accuracy, early disease detection, and performance improvements through data fusion. However, these benefits are coupled with emerging risks that are difficult to predict and mitigate, including false or biased outputs, over-reliance by clinicians, and unexpected behaviours. For example, in the case of large language model, hallucinations and non-deterministic outputs constitute a novel class of emerging risks with potentially serious clinical consequences.

From an epistemic model perspective, AI systems pose more fundamental challenges to risk assessment than most other technological innovations. Therefore, a significant fraction of risks is not only unknown but also impermanent. System performance, and consequently safety, may evolve due to data drift, retraining, or changes in the operating environment. Autonomy, complexity, and adaptiveness, in the attempt of mimicking human reasoning are AI features that escape from traditional risk analysis methods and demand for advanced approaches.

AI Act complements the MDR by introducing requirements related to data governance and reliability, transparency, human oversight, and risk-based classification, but it does not eliminate the epistemic uncertainty inherent in AI-based systems. For safety critical applications limiting the use of AI may be a possible temporary solution.

3.4. *Advanced Robotics in Healthcare*

Advanced robotics extends beyond conventional surgical robotics to include autonomous systems, small-scale robots, and emerging nanorobotic applications. These technologies aim to enhance precision, reduce invasiveness, and enable novel diagnostic and therapeutic approaches (Innocenti and Bori, 2021). Depending on their intended use, robotic systems are typically classified as MDR class IIb or III, reflecting their direct interaction with patients and high potential impact on safety.

Benefits include improved surgical outcomes, reduced recovery times, and access to procedures that were previously infeasible. At the same time, emerging risks arise from increased system complexity, autonomy, human–machine interaction, and dependency on software, sensors, and data fusion.

Within the epistemic model, advanced robotics shows how increasing autonomy expands the subsets of unknown risks. While known risks can be associated with mechanical failures, control errors, and sensor malfunctions, unknown risks emerge from adaptive behaviour, interaction with patient-specific anatomy, and integration with other digital systems. For example, for autonomous and semi-autonomous systems, failures may occur in unforeseen states that were not anticipated during design, verification, or validation. Consequently, risk estimates are characterized by a significant fraction of epistemic uncertainty that requires ad-hoc codesign risk-based methods, as well as intensive and proactive post-market surveillance to progressively reduce knowledge gaps.

3.5. *Role of the Epistemic Model Across Examples*

The pattern that emerges across the examples tells that while innovation increases the benefits, it introduces uncertainty by enlarging the fraction of unknown risks. These effects are captured by the epistemic model, which emphasizes that risk estimates based on a priori knowledge should not be treated as fixed values but as evolving quantities with associated uncertainty.

Explicit acknowledgment and communication of epistemic uncertainty is essential to support robust benefit–risk evaluation in healthcare and MedTech technologies. These activities should be integrated in risk management process with the characterization of system uncertainty based on system features like it is done for the safety characteristics. System features are for example the use of new technology, the degree of autonomy, the complexity (e.g. large state space), network integration (interdependencies), and time evolution (e.g. adaptive systems and operating environment). This preliminary uncertainty characterization may end up into more stringent risk management requirements. For example, high initial uncertainty will require enhanced post-market surveillance strategies,

such as increased monitoring frequency or expanded data collection. Given the strict regulatory environment of the MedTech sector, any such approach would ultimately need to be formalized through regulatory guidance or legislation before becoming accepted good practice. Regulatory aspects go beyond of the scope of this paper, which aims primarily to provide inputs and encourage further discussion.

4. Discussion and Conclusion

The statement that "today we certify a medical product that we sell tomorrow with yesterday's knowledge" concisely captures the fundamental asymmetry between the pace of technological innovation and the maturity of knowledge required to completely understand its safety implications and reduce risks. This asymmetry is often underestimated by stakeholders, yet it underlies the increasing likelihood that innovative products may fail to deliver expected benefits, introducing unforeseen risks, or both.

Regulators, manufacturers, and healthcare providers face a structural dilemma: either delay or prohibit the adoption of new technologies until sufficient knowledge is available to characterize their risks or allow market entry with an implicit acceptance of a potentially large fraction of unknown risks. However, neither option is fully satisfactory. Excessive conservatism may hinder beneficial innovation and limit access to improved care, while premature deployment may expose patients and healthcare systems to unacceptable safety hazards. This tension is particularly evident in the context of digital transformation, which acts as a main layer for many recent innovations. As shown in the examples, such transformation amplifies system complexity, increases interdependencies, and introduces new categories of risk—especially cybersecurity and systemic failures—that are difficult to capture using traditional, device-centric risk models. Updating the state of the art is necessary, but insufficient, if it does not address the core problem inherent to innovative technologies.

This paper has argued that the core of the problem lies in the way risk is conceptualized and estimated. Conventional risk management approaches implicitly assume that risks are identifiable, quantifiable, and stable over time. Innovation in part violates these assumptions by introducing epistemic uncertainty related to incomplete a priori knowledge and evolving system behaviour. The epistemic model represents the a priori knowledge and informs about the uncertainty in the risk estimates, for innovation-driven development processes.

The conclusion of this work presents several key findings. The first finding is the recognition that methods for risk assessment, especially for innovative medical technologies require a more rigorous and transparent approach. There is a need for characterizing the degree of uncertainty of a system and how this reflects in the risk estimates. Such an approach would allow to better understand the limitations of a priori knowledge and to make more informed decisions regarding market approval, clinical use, and post-market monitoring. A second finding concerns benefit–risk analysis. While the benefits of innovation—particularly in digital health, AI-based diagnostics, telemedicine, and advanced robotics—are often evident and measurable, the associated risks are characterized by uncertainty and a significant unknown fraction. Incorporating uncertainty into benefit–risk evaluations is therefore essential to avoid a systematic bias toward optimistic assessments of innovation. This is especially critical for higher-risk MDR classes, where failures may have severe consequences for patients. A third outcome relates to risk communication. MedTech industry focuses on communicating residual risks without addressing the uncertainty underlying their estimation. In the context of innovation, this practice is misleading and unsafe. Users, including clinicians and healthcare organizations, may develop unwarranted confidence in technologies whose risk profiles are still evolving. Communicating residual risks together with their associated uncertainty would support more informed use of medical devices and healthcare systems, while also build trust based on transparency rather than implicit assumptions of completeness.

The adoption of an epistemic approach to risk assessment is not without consequences both for regulatory burden and market approval. For example, explicitly acknowledging uncertainty may lead to additional validation requirements, delayed product certification, or restrictions on use. However, these disadvantages must be weighed against the benefits of a scientifically

sound and ethically responsible approach to safety. Informed use of medical technologies may be acceptable even in the presence of high uncertainty, provided that this uncertainty is clearly communicated and appropriately managed. Reconciling this perspective with existing regulatory frameworks represents one of the most significant challenges for regulators in the coming years.

In conclusion, innovation in healthcare and MedTech fundamentally challenges established risk assessment paradigms. This paper has proposed an epistemic model that frames risk as an evolving construct shaped by incomplete knowledge, data limitations, and system complexity. By making uncertainty explicit and central to risk assessment, the proposed approach provides a conceptual foundation for more robust safety assurance, more balanced benefit–risk evaluation, and more transparent communication with users. While it does not eliminate uncertainty, it offers a structured way to acknowledge and manage it, thereby supporting responsible innovation and sustained trust in healthcare technologies.

References

Aven, T., Krohn, B.S., 2014. A new perspective on how to understand, assess and manage risk and the unforeseen. Reliab. Eng. Syst. Saf. 121, 1–10.

DNV, 2025. Building Trust in Digital Transformation of Healthcare.

DNV, 2024. Ensuring Safe and Trustworthy AI: an AI Act Playbook for the Healthcare Sector.

European Parliament, 2024a. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (Cyber Resilience Act). European Union.

European Parliament, 2024b. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (Artificial Intelligence Act). European Union.

FDA, 2024a. Center for Device and Radiological Health, CDRH Innovation Report.

FDA, 2024b. Center for Device and Radiological Health, CDRH Safety Report.

Filippini, R., Simensen, J.E., 2025. Safety and Security Co-Design with Application to Medical Device Industry, in: 35th European Safety and Reliability Conference (ESREL 2025) and the 33rd Society for Risk Analysis Europe Conference (SRA-E 2025). Research Publishing Services, Singapore, pp. 3290–3297.

Filippini, R., Spiller, S., 2024. Cybersecurity and medical devices: a bull in a china shop, in: Proceedings of the 2024 ACM/IEEE 4th International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS) and 2024 IEEE/ACM Second International Workshop on Software Vulnerability. ACM, New York, NY, USA, pp. 61–67.

Innocenti, B., Bori, E., 2021. Robotics in orthopaedic surgery: why, what and how? Arch. Orthop. Trauma Surg.

Innocenti, Bernardo., Galbusera, Fabio., 2022. Human orthopaedic biomechanics: fundamentals, devices and applications. Academic Press.

International Organization for Standardization (ISO), 2019. ISO 14971: Medical devices – Application of risk management to medical devices.

MedTech Europe, 2020. Innovation in Medical Technologies: Reflection Paper.

Thacharodi, A., Singh, P., Meenatchi, R., Tawfeeq Ahmed, Z.H., Kumar, R.R.S., V, N., Kavish, S., Maqbool, M., Hassan, S., 2024. Revolutionizing healthcare and medicine: The impact of modern technologies for a healthier future—A comprehensive review. Health Care Science 3, 329–349.

van Kolfschooten, H., van Oirschot, J., 2024. The EU Artificial Intelligence Act (2024): Implications for healthcare. Health Policy (New York). 149, 105152.