The first challenge facing DM manufacturers is to gain an overview of the intersections between regulatory requirements, for example and a minima those of the RDM, the RGPD and the IA law.

The AI and DM Act: a global approach based on risk management

Erik Luysterborg,
Partner in charge of the Data Privacy & Digital Trust & Digital Trust at Deloitte AG

For this dossier, we sought the opinion of a legal expert in issues relating to artificial intelligence in healthcare. Here, Mr Luysterborg describes the implications of the new European law on AI for medical devices and the main difficulties it raises for manufacturers.

Erik Luysterborg

The European Union's Artificial Intelligence Act (AI Act) came into force on 1 August 2024 in the form of EU Regulation 2024/1689, which is directly applicable in Member States. As such, it shares the same legal status as, for example, the EU Medical Device Regulation (MDR) and the EU General Data Protection Regulation (GDPR). The AI Act creates a uniform, horizontally effective legal framework, with a view in particular to ensuring trust in the development, marketing/distribution and use of artificial intelligence. The transitional periods for organisations will vary depending on the types of AI involved, with an initial deadline (relating to AI systems that will no longer be permitted and AI training) of 2 February 2025, and subsequently the introduction of specific obligations that will apply to general-purpose AI models from 2 August 2025. The majority of the obligations laid down by the AI Act (e.g. high-risk systems) will then come into force on 2 August 2026, with others following on 2 August 2027.

Scope and definition

The AI Act applies to providers (i.e. manufacturers) who place AI systems on the EU market, to users (deployers, importers, distributors, etc.) within the EU, and to non-EU

providers/users if the results of their AI systems are used in the EU. Each category has its own requirements. This extraterritorial scope is similar to that of the GDPR.

The Act gives a broad definition of an AI system as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments". Autonomy and the ability to make inferences are thus the key attributes that distinguish an AI system from any other software.

A high-risk classification for DM incorporating AI

AI systems are then categorised based on the level of risk they pose, from unacceptable (e.g. manipulation of vulnerable groups) and high risk to limited and minimal risk. Limited-risk applications (e.g. chatbots) are subject to transparency requirements, while minimal-risk AI systems (e.g. video games) largely escape regulation. The AI Act specifically defines most AI-based medical devices as 'high risk', which translates into strict compliance obligations, such as quality management systems, robust data management and governance, security, documentation of technical and ethical choices, and transparency and human oversight obligations, as well as ongoing monitoring and the establishment of systems for reporting serious incidents.

For manufacturers of AI-powered medical devices, this means navigating a complex regulatory landscape where requirements specific to the AI Act often overlap, and sometimes conflict, with medical device and data protection regulations (e.g. the MDR and GDPR respectively).

What are the main challenges facing medical device manufacturers (MDMs)?

Expanding on the full list of specific legal requirements set out in the AI Act would take up too much space here. Instead, let us take a look at the risk levels of some of the key compliance challenges facing an MDM endeavouring to comply with these requirements.

- **Evaluate the overlaps between the various reference systems**

First, MDMs will need to have a clear overview of the intersections between the regulatory requirements of the MDR, GDPR and AI Act. While there are overlaps with MDR and GDPR requirements that may be helpful for compliance with the EU's AI Act (e.g. risk assessment, quality management, technical documentation, post-market monitoring, transparency, accountability, etc.), there is still a lack of clarity and consistency in these obligations.

Although in the long term these inconsistencies will be corrected, in the short term these additional compliance burdens, combined with both the current shortage of skilled resources and an increase in the workload and costs within MDMs, will require considerable effort and focus (especially for SMEs). In sum, the main overlapping challenges relate to

accountability, transparency, purpose identification, human oversight, non-discrimination and fairness, accuracy, technical robustness and cybersecurity.

- **Adopt a holistic and uniform approach to data management**

Second, the AI Act is more concerned with the impact of AI systems than the underlying complex code. Thus it seeks to further highlight who uses what data, for what purpose and how it is protected and monitored. This requires a holistic and uniform approach to master data management and governance processes (data deletion, data classification, etc.). Today, MDMs often adopt very different approaches to, for instance, quality management systems and data governance practices across the various business units. In order to unlock the full potential of AI in medical devices, you must first get your data management practices in order, given that they form the bedrock of reliable data analysis.

- **Harmonising governance**

Third, successful implementation of the AI Act will require combined and effective efforts from a wide range of stakeholders within often siloed and decentralised governance structures. This poses potential risks because, even if the MDM is ready to comply with the requirements of the AI Act, there may be significant compliance issues due to lack of capacity as well as different maturity or governance levels and different risk management approaches in different business units. The need for a holistic approach before, during and after the development and market launch phase will be paramount.

- **Implementing flexible governance**

Fourth, the dynamic pace of AI innovation could suffer from a static approach to governance. Such innovation emphasises the need for flexible, agile and adaptive governance frameworks that can accommodate new AI advances, technologies, methodologies and challenges that have yet to emerge. If this is to be achieved, it will be necessary to integrate more technological knowledge (in particular relating to AI) into existing control functions. This will be particularly necessary in situations where regulated medical devices are combined with general-purpose AI models developed by a third party. For example, an AI-powered medical device that uses classical machine learning to analyse medical images with a view to diagnosing a medical condition could be augmented with a separate general AI, such as a large language model (LLM), to enhance medical AI's reasoning upfront and to expand its output capabilities (e.g. providing diagnostic results in natural language). The LLM started as a general AI application (i.e. one with an intended general use), but is now an AI subsystem within an overall medical system or product whose intended use is medical diagnosis. Compliance officers and other control functions will need to be able to spot such 'transformations'.

Final remarks

The EU's AI Act applies a comprehensive risk-based approach to regulating medical devices. Patient trust, a critical factor in the healthcare sector, can be improved by addressing ethical concerns and ensuring regulatory compliance, which promotes transparency in the implementation of AI technologies.

One of the most promising benefits of AI when it comes to medical devices is that it can significantly reduce the time that physicians have to spend on administrative tasks.

Paradoxically, to achieve this goal, medical device manufacturers will first need to spend more time complying with the various legal and compliance requirements relating to AI. Rather than a revolution, this will require a constant and profound evolution in terms of data management and governance from now on.

Article DeviceMed 6 2024

INFO

The subject covered here by Mr Luysterborg was the subject of a presentation at EPHJ 2024, as part of a round table dedicated to the impact of AI on health and medical devices. This round table was organised by the EPHJ teams in partnership with Inartis.

Deloitte is helping companies in the healthcare sector that are integrating AI into their products to put in place appropriate functional and technical architectures. These are the result of the definition and application of an AI service catalogue shared by the IT and business departments. Deloitte's experts have mastered the manipulation of data and the implementation of complex traditional models and algorithms specific to a business or industry.