Diagn Interv Radiol 2026; DOI: 10.4274/dir.2025.252851

ARTIFICIAL INTELLIGENCE AND INFORMATICS

COMMENTARY

The AI Act: responsibilities and obligations for healthcare professionals and organizations

Kicky Gerhilde van Leeuwen[1,2]
Leon Doorn[3,4]
Erik Gelderblom[5]

[1]Romion Health, Utrecht, The Netherlands
[2]Health AI Register, Utrecht, The Netherlands
[3]MedQAIR, Amsterdam, The Netherlands
[4]QAIR, Amsterdam, The Netherlands
[5]Radboud University Medical Center, Department of Medical Technology and Clinical Physics, Nijmegen, The Netherlands

Corresponding author: Kicky van Leeuwen

E-mail: Kicky.vanleeuwen@romionhealth.com

Received 23 March 2025; revision requested 08 April 2025; accepted 12 May 2025.

Epub: 29.05.2025

Publication date: 04.05.2026

DOI:10.4274/dir.2025.252851

On August 1, 2024, the artificial intelligence (AI) Act 2024/1689 officially came into force within the European Union (EU). Since the United States Executive Order 14110 on AI from 2023 was recently revoked, it sets the global standard as a regulatory framework to govern AI systems.[1] The Act applies across all sectors and, as such, also introduces requirements and controls for the use of AI in healthcare. Although medical devices (MDs) (with and without AI) have long been subject to the rules and requirements of the MD Regulation (MDR) (preceded by the MD directive) and the *in vitro* diagnostics regulation (IVDR) (preceded by the *in vitro* diagnostic MDs directive), these requirements primarily focus on the manufacturers.[2,3] The AI Act extends this dynamic by introducing AI-specific requirements for manufacturers (providers), as well as additional responsibilities for the users (deployers) of AI-enabled MDs.

Central to the AI Act is the classification of AI systems based on their level of risk: prohibited, high-risk, limited-risk, minimal-risk, and general-purpose AI models (with and without systemic risk) or systems. MDs incorporating AI are generally classified as "high-risk" because AI often serves as a key functionality or safety component, and most software-based MDs require a conformity assessment, per their assigned risk classification, by a notified body under the MDR or IVDR before they can be placed on the EU market. High-risk AI systems must meet stringent requirements for design, risk management, performance, transparency, human oversight, logging, and monitoring under the AI Act to ensure their safe and effective use.[4]

The additional requirements for the providers do not exempt healthcare organizations and individual users, designated deployers, from keeping pace with the new regulations.[5] Some requirements are already covered by the MDR and IVDR, such as ensuring the MD is used according to its intended purpose and reporting incidents. Other regulatory frameworks, such as the General Data Protection Regulation 2016/679, may require healthcare organizations to conduct data protection impact assessments to ensure privacy is adequately protected.[6]

This commentary highlights the most important additional requirements for deployers of high-risk AI solutions in healthcare, as summarized in Figure 1 and Table 1. It explores the boundaries of responsibility between the MD industry, healthcare organizations, and individual users. We reflect on how the AI Act reshapes accountability and places new demands on healthcare professionals as users of AI systems.

Obligations for healthcare organizations and users (deployers)

Ensuring artificial intelligence literacy among healthcare staff

Healthcare organizations are expected to ensure the AI literacy of their staff to support the safe and responsible use of AI systems (AI Act, article 4). The level of AI literacy required depends on context and role. For clinical users, this may involve general AI knowledge (understanding the capabilities and risks of AI) and system-specific knowledge (understanding how to interpret the AI system's output and detect malfunctioning). This responsibility applies not only at the time of deployment but also over the entire product lifecycle, as updates with new functionalities may occur over time. Other responsibilities include input data control,

You may cite this article as: van Leeuwen KG, Doorn L, Gelderblom E. The AI Act: responsibilities and obligations for healthcare professionals and organizations. *Diagn Interv Radiol*. 2026;32(3):273-275.

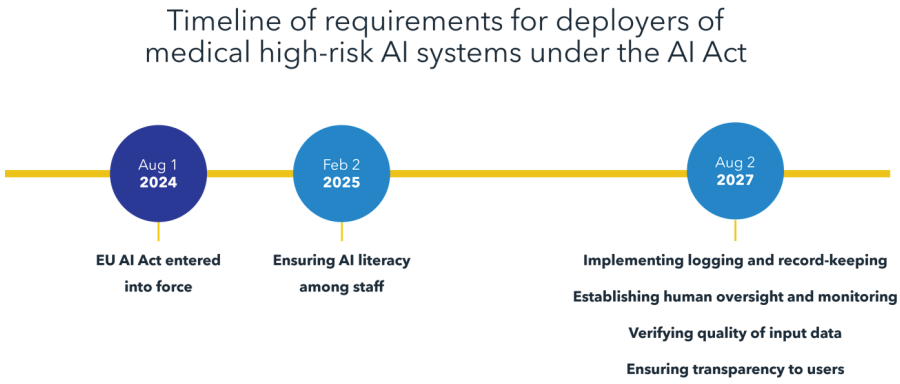

Figure 1. Timeline of requirements for deployers of medical high-risk AI systems under the AI Act. AI, artificial intelligence.

Table 1. Responsibilities for deployers (healthcare organizations) of AI systems under the AI Act

Responsibilities for deployers of AI systems under the AI Act	Related articles
Ensuring AI literacy among staff	Article 4
Implementing logging and record-keeping	Article 26(6)
Establishing human oversight and monitoring	Articles 26(2), 26(5)
Verifying the quality of input data	Article 26(4)
Ensuring transparency to users	Article 50

AI, artificial intelligence.

record keeping, and monitoring for automation bias, which will require IT personnel and medical physicists to become AI literate. Management and leadership roles may also need to enhance their AI literacy, as they are often involved in implementation decisions and governance (AI Act, Preamble 20 and 91).

The topic of AI is still often lacking in formal educational programs.[7] It is therefore up to healthcare organizations to judge what level of AI literacy is sufficient and for whom. Suitable materials and supplementary training may be obtained through professional societies, conferences, external parties, or AI system providers. It is important to note that this requirement applies as of February 2, 2025, as shown in Figure 1.

The AI Act also promotes the AI literacy of "affected persons," who, in the healthcare context, are likely to be patients or their relatives. It states that the European AI Board should support the commission in promoting AI literacy tools and public awareness (AI Act, Preamble 20). Some hospitals contribute by informing and educating patients on how AI is applied, for example, through posters or information on their websites.

Providers' role: Providers also have a responsibility to ensure sufficient AI literacy. They must ensure their own staff are AI literate and facilitate adequate knowledge among their users (AI Act, article 4). Appropriate instructions for use are often obligatory under the MDR and IVDR and are always obligatory under the AI Act (AI Act, article 13). Providers also frequently organize user training to support the responsible use of their systems.

Implementing logging and record-keeping

Logging and record-keeping responsibilities under the AI Act are shared between the AI system provider and the deployer.

Deployers are responsible for managing and storing logs once the system is in use within their organization. They must ensure that logs are retained for a period appropriate to the AI system's intended purpose, with a minimum duration of 6 months, unless determined otherwise by another EU or national law. These logs should be accessible for internal reviews, audits, and the reporting of incidents to relevant authorities when necessary (AI Act, article 26(6)).

Providers' role: Providers are responsible for embedding technical capabilities within the AI system to allow for automatic event recording over its entire lifecycle. These logs must capture key events related to system functionality, including identifying potential risks and data necessary to facilitate human oversight and monitoring. Some AI vendors and platforms already provide dashboards with longitudinal insights on system functioning to facilitate monitoring and human oversight (AI Act, article 12).

Establishing human oversight and monitoring

Human oversight is required to minimize risks to health, safety, and fundamental rights (AI Act, Article 26(2), 26(5)). This involves defining clear workflows to ensure that anomalies or unexpected performance are detected. For example, healthcare professionals must have the authority to override AI predictions when clinical judgment contradicts the AI output. Human oversight must also safeguard against automation bias by ensuring that healthcare professionals critically assess the recommendations provided by the AI system. If deployers suspect that using a high-risk AI system according to its instructions could pose a risk, they must immediately suspend its use and notify the provider and relevant authorities without delay. In the case of a serious incident, they must first inform the provider, followed by the importer or distributor and the market surveillance authority. Depending on the nature of the incident, the surveillance authority may be either the traditional MD competent authority for safety incidents or the appointed national surveillance authority under the AI Act for infringements of fundamental rights (AI Act, article 3[49(c)]).

Human oversight may range from reviewing individual results generated by an AI system to more holistic oversight, in which trends are monitored over time to allow early detection of performance drift, bias, or malfunctioning of the AI system. Logging and record-keeping capabilities play a key role in supporting such oversight measures. Although the AI Act does not exclude the possibility of autonomous AI use, it requires that appropriate oversight measures be in place to ensure safe deployment. As the concept of autonomy remains open to interpretation, future guidelines will be essential to clarify what level of human oversight is suitable for different degrees of autonomy.

Providers' role: Providers of high-risk AI systems must ensure that their systems are designed to enable effective human oversight through appropriate human–machine interface tooling. These measures should be

built into the system or be possible for the deployer to implement. Oversight measures must be proportionate to the system's risks, autonomy, and context (AI Act, article 14).

Verifying the quality of input data

Deployers are responsible for verifying that the data input into AI systems complies with the requirements specified by the provider (AI Act, article 26(4)). Poor quality or incomplete input data could lead to erroneous AI predictions, posing risks to patient safety. Where AI systems may continue to learn from data in clinical practice, proper quality control by the healthcare provider becomes even more important, as it may affect the overall accuracy of the AI system. Healthcare organizations may consider implementing automated procedures to pre-screen data for quality assurance and to ensure it adheres to the requirements outlined by the AI system's provider. For example, in radiological AI, data orchestration is often used to ensure that images meet specified criteria, such as resolution and metadata, to allow the system to process them correctly.

Providers' role: In the instructions to users, providers must clearly specify the input data requirements (AI Act, article 13(3)).

Ensuring transparency to users

The responsibility for providing transparency on the AI system predominantly lies with the provider; however, it is up to deployers to ensure that this information reaches the users. Users are most often healthcare providers, for example, when an AI system supports a physician in the diagnostic process. However, users can also be patients, such as when they use an AI system for (chronic) disease management. Healthcare organizations must ensure that users of AI systems are adequately informed that they are using an AI-based product and are aware of its capabilities, limitations, and potential risks to health, safety, and fundamental rights (AI Act, Preamble 27, 72; article 50).

Providers' role: Providers are responsible for supplying information about the AI system through an instruction for use (AI Act, article 13), which is already mandatory under the MDR for most MDs. Additionally, the AI Act explicitly states that users must be informed when they are interacting with an AI system (AI Act, Preamble 72; article 50(1)).

Impact on in-house developed AI

In-house developed MDs, used exclusively for a healthcare organization's own patients and not placed on the market, may be exempt from third-party (notified body) conformity assessments under the MDR. Without this obligation, such devices are not classified as high-risk under the AI Act, Article 6 (b). However, article 43(3) suggests that certain AI systems, contrary to Article 6(b), may still qualify as high-risk even though they are exempt from third-party conformity assessments under Union Harmonisation Legislation listed in Annex I. To facilitate uniform implementation of the AI Act for in-house developed AI-enabled MDs, further clarification or guidance from the European Commission is desired.

In the meantime, healthcare organizations could apply the MDR concept for in-house developed products. This means they should aim to ensure safety, security, and the protection of fundamental rights. This can be achieved by following the requirements for high-risk AI systems, including risk management, quality management system requirements, and post-market monitoring, potentially through the use of harmonized standards.

General-purpose models and administrative AI tools

Software solutions using general-purpose AI models, such as large language models, are gaining popularity. These systems can support administrative work, automate note-taking, summarization, or report generation. The intended purpose of the AI system utilizing a general-purpose AI model determines its risk classification under the AI Act. When there is no medical intended purpose (and therefore no qualification as a MD under the MDR), these systems are generally considered minimal-risk under the AI Act. There are no specific obligations for deployers of AI systems classified as minimal-risk. However, providers of general-purpose AI systems face additional requirements, mostly related to effectiveness, interoperability, robustness, reliability, transparency, and model evaluation (AI Act, article 50).

In conclusion, the AI Act represents a substantial shift in regulating AI systems used in healthcare, extending responsibilities to healthcare organizations as deployers. By emphasizing AI literacy, data quality, human oversight, transparency, and monitoring, the Act promotes the safe and effective use of AI in clinical practice. Healthcare organizations must rise to the challenge of implementing these systems responsibly, balancing innovation with patient safety, even as many standards and guidance documents are still under development.[8] Ultimately, the success of AI in healthcare depends on collaboration between providers and deployers, along with a shared commitment to compliance, education, and ethical use.

Footnotes

Conflict of interest disclosure

The authors declared no conflicts of interest.

References

1. European Artificial Intelligence Act, 2024/1689 (2024). Accessed: December 30, 2024. [Crossref]
2. European Medical Device Regulation, 2017/745 (2017). European Commission. Accessed: December 30, 2024. [Crossref]
3. European *in-vitro* diagnostics regulation, 2017/746 (2017). European Commission. Accessed December 30, 2024. [Crossref]
4. Aboy M, Minssen T, Vayena E. Navigating the EU AI Act: implications for regulated digital medical products. *NPJ Digit Med.* 2024;7(1):237. [Crossref]
5. Kotter E, D'Antonoli TA, Cuocolo R, et al. Guiding AI in radiology: ESR's recommendations for effective implementation of the European AI Act. *Insights Imaging*. 2025;16(1):33. [Crossref]
6. European General Data Protection Regulation, 2016/679 (2016). Accessed December 30, 2024. [Crossref]
7. Gilbert A, Pizzolla E, Palmieri S, Briganti G. Artificial intelligence in healthcare and regulation challenges: a mini guide for (mental) health professionals. *Psychiatr Danub*. 2024;36(Suppl 2):348-353. [Crossref]
8. van Kolfschooten H, van Oirschot J. The EU artificial intelligence Act (2024): implications for healthcare. *Health Policy*. 2024;149:105152. [Crossref]