Navigating the Regulatory Maze: GDPR Rules for Medical AI in Europe

Rasit Dinc

Rasit Dinc Digital Health & AI Research

Published: February 12, 2023 | AI Diagnostics

DOI: 10.5281/zenodo.17997619

Abstract

The integration of Artificial Intelligence AI into medical practice promises a revolution in diagnostics, treatment, and patient care. From sophisticated ima...

The Foundation of Trust in Digital Health

The integration of Artificial Intelligence (AI) into medical practice promises a revolution in diagnostics, treatment, and patient care. From sophisticated image analysis to predictive health modeling, AI systems are rapidly becoming indispensable tools in the European healthcare landscape. However, this progress is fundamentally intertwined with the stringent data protection framework established by the **General Data Protection Regulation (GDPR)** (Regulation (EU) 2016/679) [4]. For developers, clinicians, and policymakers, understanding the precise application of GDPR to medical AI is not merely a compliance exercise, but a prerequisite for building trustworthy and ethical digital health solutions.

The GDPR's rules for medical AI are complex, primarily because they intersect with other critical EU regulations, including the new **AI Act** and the **Medical Device Regulation (MDR)** [1]. While the AI Act focuses on the safety and ethical use of AI systems themselves, the GDPR governs the processing of the highly sensitive personal data that fuels these systems.

Processing Health Data: The Article 9 Hurdle

The most significant challenge for medical AI under GDPR lies in **Article 9**, which prohibits the processing of "special categories of personal data," including health data, genetic data, and biometric data, unless a specific exception applies [2]. Since medical AI systems are inherently designed to process health data, developers must identify a clear legal basis under Article 9(2) to legitimize their operations.

The most common exceptions relied upon in the context of medical AI are:

1. **Explicit Consent (Art. 9(2)(a)):** While often the default, obtaining explicit, informed, and freely given consent from patients for the broad and

evolving uses of AI can be logistically challenging and may be withdrawn at any time. 2. **Public Health Interest (Art. 9(2)(i)):** Processing necessary for reasons of public interest in the area of public health, such as ensuring high standards of quality and safety of healthcare, provided it is based on Union or Member State law. 3. **Scientific Research (Art. 9(2)(j)):** Processing necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to appropriate safeguards [3].

The choice of legal basis is crucial, as it dictates the level of transparency, accountability, and patient rights that must be upheld.

The Purpose Limitation and Data Re-use

A core principle of the GDPR is **purpose limitation**, which mandates that data collected for one purpose cannot be re-used for an incompatible secondary purpose [3]. This is particularly relevant when patient data, initially collected for clinical care, is later repurposed to train a new AI model.

To re-use data for AI training, a **compatibility assessment** must be performed. Scientific research is generally considered a compatible secondary use, provided that robust safeguards—such as **pseudonymisation**, **anonymisation**, and **data minimisation**—are implemented [3]. These measures are essential to mitigate risks to data subjects and demonstrate compliance with the accountability principle.

Automated Decision-Making and Patient Rights

Article 22 of the GDPR grants data subjects the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" [2].

In medical AI, this applies to systems that make fully automated decisions, such as an AI-driven triage system that assigns a patient a priority level without human intervention. While Article 22 is often interpreted narrowly, its implications for patient autonomy are profound. Exceptions exist, such as when the decision is necessary for entering into or performing a contract, or is authorized by law. Crucially, even when an exception applies, the data controller must implement suitable measures to safeguard the data subject's rights, including the right to obtain human intervention, to express their point of view, and to contest the decision [2].

The Future: GDPR and the EU AI Act Synergy

The regulatory landscape for medical AI in Europe is rapidly evolving. The **EU AI Act**, which classifies AI systems used as medical devices as **high-risk**, introduces additional requirements for data governance, technical robustness, transparency, and human oversight [1]. These new rules complement the GDPR, creating a dual-layer compliance structure:

| Regulatory Instrument | Primary Focus | Relevance to Medical AI | | :--- | :--- | :--- | | **GDPR** | Protection of personal data and privacy rights. | Governs the

data used to train, test, and operate AI systems (Art. 9, Art. 22). | | **EU AI Act** | Safety and ethical use of AI systems. | Governs the *system* itself, classifying medical AI as high-risk and imposing strict requirements. | | **MDR/IVDR** | Safety and performance of medical devices. | Governs the *product* lifecycle, with AI software often classified as a medical device. |

The combined effect of these regulations is to establish Europe as the global leader in the ethical and responsible deployment of AI in healthcare. Navigating this framework requires a deep, interdisciplinary understanding of law, ethics, and technology.

For more in-depth analysis on this topic, the resources at www.rasitdinc.com provide expert commentary and cutting-edge insights into the intersection of digital health, AI, and regulatory compliance.

References

[1] European Commission. Artificial Intelligence in healthcare. [Online]. Available: https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en (Accessed: Nov 11, 2025). [2] GDPR-info.eu. Art. 9 GDPR – Processing of special categories of personal data. [Online]. Available: https://gdpr-info.eu/art-9-gdpr/ and Art. 22 GDPR – Automated individual decision-making, including profiling. [Online]. Available: https://gdpr-info.eu/art-22-gdpr/ (Accessed: Nov 11, 2025). [3] Taylor Wessing. Re-use of patient data in scientific research to train AI systems - important GDPR considerations. [Online]. Available: https://www.taylorwessing.com/en/synapse/2025/ai-in-life-sciences/re-use-of-patient-data-in-scientific-research-to-train-ai-systems (Accessed: Nov 11, 2025). [4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: Nov 11, 2025).