What Are the GDPR Requirements for Healthcare AI?

Rasit Dinc

Rasit Dinc Digital Health & AI Research

Published: March 12, 2022 | Healthcare Data Privacy and Security

DOI: 10.5281/zenodo.17998555

Abstract

The integration of Artificial Intelligence (AI) in healthcare presents transformative opportunities, from diagnostics to personalized treatments. However, th...

What Are the GDPR Requirements for Healthcare AI?

By Rasit Dinc

The integration of Artificial Intelligence (AI) in healthcare presents transformative opportunities, from diagnostics to personalized treatments. However, this advancement also brings significant data protection challenges. The European Union's General Data Protection Regulation (GDPR) establishes a high standard for data protection, with stringent requirements for sensitive health information. This article outlines the key GDPR requirements for healthcare organizations and AI developers using AI in the healthcare sector.

Understanding GDPR in the Context of Healthcare AI

GDPR classifies health data as a “special category of personal data,” granting it a higher level of protection due to its sensitivity [1]. Processing this data is prohibited unless specific conditions are met. The core principles of GDPR are fundamental for compliant AI use in healthcare:

Lawfulness, Fairness, and Transparency: *Processing of personal data must be lawful, fair, and transparent. Patients must be clearly informed about how their data is being used by AI systems.* **Data Minimization:** Only the data that is strictly necessary for the specified purpose should be collected and processed. AI models should be designed to function effectively with the minimum amount of personal data possible. ***Purpose Limitation:*** *Data collected for a specific purpose should not be used for other, incompatible purposes without a new legal basis.* **Accountability:** Data controllers are responsible for demonstrating compliance with GDPR. This requires comprehensive documentation of all data processing activities.

Key GDPR Requirements for Healthcare AI

Navigating GDPR's complexities is crucial for the ethical implementation of AI in healthcare. Key requirements include:

Lawful Basis for Processing

Processing special category data, such as health information, requires a lawful basis under GDPR's Article 9. While explicit consent is an option, it may not always be the most practical. Other lawful bases include the necessity for providing health or social care, or for public interest reasons in public health [2].

Data Protection Impact Assessments (DPIAs)

The use of AI in healthcare is often a high-risk activity due to large-scale processing of sensitive data. GDPR mandates a Data Protection Impact Assessment (DPIA) for any processing likely to result in a high risk to individuals' rights and freedoms. A DPIA is a process to identify and mitigate data protection risks.

Rights of Individuals

GDPR grants individuals several rights over their personal data. For healthcare AI, the most relevant rights are:

The Right of Access: *Patients have the right to obtain confirmation that their data is being processed and to access that data.* **The Right to Rectification:** Patients can request the correction of inaccurate personal data. ***The Right to Erasure ('Right to be Forgotten'):*** *In certain circumstances, patients can request the deletion of their personal data.* **The Right not to be Subject to Automated Decision-Making:** Article 22 of the GDPR provides individuals with the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. This is particularly relevant for AI systems that make diagnostic or treatment recommendations. To comply, there must be a "human in the loop" to review and validate the AI's output, especially for critical decisions [2].

Data Security

Both GDPR and the realities of handling sensitive health data demand robust security measures. This includes implementing "appropriate technical and organisational measures" to ensure a level of security appropriate to the risk. For AI systems, this means encrypting data both at rest and in transit, implementing strong access controls, and maintaining detailed audit logs of data access and processing activities [2].

The EU AI Act and its Interplay with GDPR

The EU's Artificial Intelligence Act complements GDPR by categorizing AI systems based on risk. Many healthcare AI applications are "high-risk" and subject to new obligations, including risk management, data quality, transparency, and human oversight, which align with GDPR's data protection principles [1].

Conclusion

The transformative potential of AI in healthcare is matched by its data protection challenges. GDPR compliance is a prerequisite for building patient trust and ensuring the ethical use of health data. A “privacy by design” approach, thorough risk assessments, and upholding individual rights allow healthcare organizations and AI developers to leverage AI while respecting data protection. As the regulatory landscape evolves with the AI Act, a proactive approach to compliance is essential.

References

[1] European Commission. (2025). *Artificial Intelligence in healthcare*. Retrieved from https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en

[2] Inquira Health. (2025). *GDPR and HIPAA Compliance in Healthcare AI: What IT Leaders Must Know*. Retrieved from https://www.inquira.health/blog/gdpr-and-hipaa-compliance-in-healthcare-ai-what-it-leaders-must-know

---