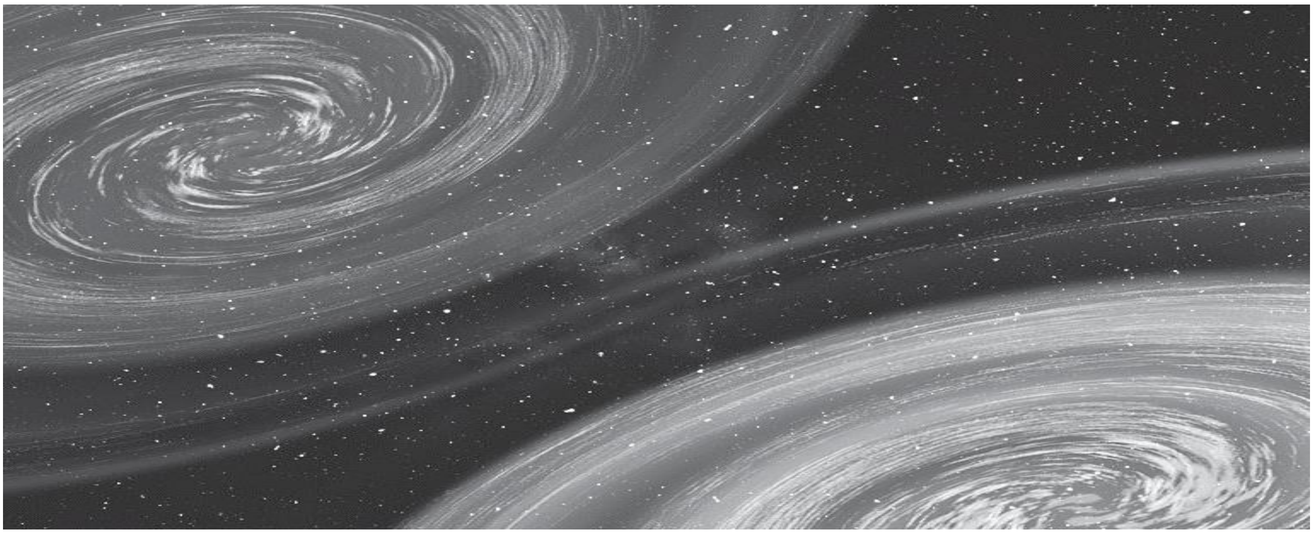

Medical Data and Artificial Intelligence: Challenges and Prospects

Introduction

The convergence of artificial intelligence (AI) with the healthcare sector offers unprecedented possibilities for improving healthcare, but simultaneously raises significant issues regarding personal data protection. This article examines the legal framework governing the use of personal health data in AI systems, the challenges faced by healthcare providers, and best practices for the responsible utilization of these technologies.

Part A: Understanding AI in Healthcare

What is AI

AI refers to a mechanical system designed to operate with different levels of autonomy and may exhibit adaptability after its implementation. This system, for explicit or implicit goals, infers from the input it receives how to produce outputs such as predictions, content, recommendations, or decisions that can affect material or virtual environments.

AI is based on techniques such as:

- Machine Learning (ML): Allows computers to learn from data and improve their performance without explicit programming.

- Deep Learning (DL): Uses multi-layered neural networks to process and analyze complex data, mimicking the function of the human brain.

Applications of AI in Healthcare

The healthcare sector is one of the most promising fields for AI application, with capabilities that can bring revolutionary changes to healthcare delivery.

In the field of disease diagnosis, AI is utilized for recognizing pathological conditions from medical images. Specifically, deep learning algorithms can analyze X-rays, MRIs, and other imaging examinations to detect cancer and other conditions, often with accuracy that compares to or even exceeds that of experienced physicians.

Personalized medicine is another field where AI offers significant possibilities. Through the analysis of genetic data, medical history, and other parameters, AI systems can contribute to the creation of individualized treatment regimens, tailored to the specific needs and characteristics of each patient.

In public health, AI is used for predicting epidemics through the analysis of large datasets and the identification of patterns that can predict the spread of infectious diseases. This allows health authorities to take preventive measures and allocate available resources more effectively.

Additionally, AI contributes to improving hospital management through data analysis for optimizing patient management, staff, and medical supply inventory. This leads to more efficient operation of healthcare facilities, cost reduction, and improvement in the quality of services provided.

Part B: Legal Framework for the Protection of Health Data

Introduction

Health data constitute a particularly sensitive category of personal data that require increased protection. The GDPR introduced a comprehensive framework for the protection of personal data, with special emphasis on health data. The digitization of health services and the increasing use of technologies for collecting and processing medical information have made the need for strict protection rules imperative. This chapter examines the legal framework governing health personal data, the challenges in managing them, and the protective measures that must be taken.

Legislative Framework

The GDPR constitutes the basic legislative framework for the protection of personal data in the European Union. According to Article 4(15) of the GDPR, 'data concerning health' is defined as personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

The GDPR classifies health data in the 'special categories of personal data' (Article 9), for which processing is prohibited in principle. However, specific exceptions are provided, such as when the data subject has given explicit consent, when processing is necessary for reasons of public interest in the area of public health, or when it is necessary for the purposes of preventive or occupational medicine.

Additionally, the implementing Law 4624/2019 of the GDPR includes special provisions for the processing of sensitive personal data, including health data. This law establishes additional guarantees for the protection of health data and determines the conditions under which their processing is permitted.

The Regulation (EU) 2024/1689 on Artificial Intelligence (the “AI Act”) represents a milestone in regulating AI systems in the European space, setting as a primary goal the promotion of human-centered and trustworthy AI that balances technological innovation with the protection of fundamental rights. Particular emphasis is placed on high-risk AI systems, such as those used in healthcare and by public authorities for assessing the eligibility of individuals for essential benefits. In the context of processing personal health data, the Act introduces a multi-level protection system that works complementarily with the GDPR, requiring increased transparency of algorithmic processes so that decisions made by AI systems are explainable and understandable both by healthcare professionals and patients. An innovative element of the Act is the mandatory Fundamental Rights Impact Assessment, a process that must precede the development and use of high-risk AI systems, including detailed analysis of usage procedures, duration of application, categories of individuals who may be affected, and specific risks to fundamental rights. At the same time, it becomes mandatory to conduct a data protection impact assessment before implementing AI systems in healthcare environments, while an important element of the process is the possibility of collaboration with stakeholders, such as citizen groups and civil society organizations, ensuring a participatory approach to risk management and enhancing transparency and accountability through mandatory notification of the competent supervisory authorities.

Categorization and Examples of Personal Health Data

Personal health data include a wide range of information related to an individual's physical or mental health. Specific examples include:

- Medical history, diagnoses, and treatment plans that record the course of an individual's health over time.
- Medication, allergies, and information about surgical procedures the individual has undergone.
- Laboratory test results, X-rays, and other diagnostic information that reveal health status.
- Biometric and genetic data, which reveal unique physiological or behavioral properties of an individual and can be used to predict diseases or personalize treatments.
- Hospitalization data and mental health information, including psychiatric diagnoses and treatments.
- Information about disabilities or chronic conditions that affect the individual's daily life.
- Data from health applications and wearable monitoring devices, such as glucose meters, pedometers, or heart rate monitors.
- Information about lifestyle factors that affect health, such as dietary habits, smoking, or alcohol consumption.

Legal Bases for Processing Health Data

According to Article 9 of the GDPR, the processing of health data is permitted only under specific conditions, which include:

- Explicit consent of the data subject for one or more specific purposes.
- Processing necessary for the fulfillment of obligations and the exercise of rights of the data controller or the data subject in the field of employment law.
- Processing necessary to protect the vital interests of the data subject or another natural person, if the data subject is physically or legally incapable of giving consent.
- Processing necessary for reasons of substantial public interest, based on Union or Member State law.
- Processing necessary for the purposes of preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, provision of health or social care or treatment.
- Processing necessary for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health.

- Processing necessary for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes.

Rights of Data Subjects

Individuals whose health data are being processed have specific rights according to the GDPR, which include:

- Right to information about the processing of their data, including the purposes of processing and the recipients of the data.
- Right of access to their data and to obtain a copy of the data being processed.
- Right to rectification of inaccurate data and completion of incomplete data.
- Right to erasure under certain conditions, such as when the data are no longer necessary for the purposes for which they were collected.
- Right to restriction of processing, for example when the accuracy of the data is contested.
- Right to data portability, allowing individuals to receive and reuse their data for their own purposes.
- Right to object to the processing of their data for specific purposes, such as direct marketing.
- Right not to be subject to a decision based solely on automated processing, including profiling.

Part C: Challenges in Health Data Management & Health Data Protection Measures

Challenges in Health Data Management

The management of health data presents significant challenges, which include:

- Ensuring that health data are used exclusively for medical and scientific purposes, avoiding their misuse for commercial or other purposes.
- Minimizing the risk of third-party access to sensitive data, through the implementation of appropriate technical and organizational security measures.
- Obligation to inform patients about the processing of their data and their rights, ensuring transparency and trust.
- Development of secure infrastructures for data storage and transfer, protecting against cyber attacks and data breaches.
- Balancing between the need for access to health data for research purposes and the protection of individuals' privacy.
- Ensuring cross-border transfer of health data in accordance with GDPR requirements, especially when it comes to transfers outside the EU.
- Addressing challenges arising from new technologies, such as AI and big data in the healthcare sector.

Health Data Protection Measures

For the effective protection of health data, healthcare organizations and other data controllers must implement the following measures:

- Data Protection Impact Assessment (DPIA) before beginning health data processing, to identify and address potential risks.

- Implementation of the data minimization principle, collecting only the absolutely necessary data for the specific purpose.
- Adoption of anonymization or pseudonymization techniques, where possible, to reduce risks for data subjects.
- Implementation of strong security measures, such as encryption, access control, and regular security audits.
- Training of staff regarding their obligations for the protection of health data and the procedures to be followed.
- Appointment of a Data Protection Officer (DPO) in organizations that process health data on a large scale.
- Development and implementation of policies and procedures for addressing data breach incidents.
- Regular evaluation and updating of security measures to address new threats and challenges.

Part D: Challenges - Legal Risks, Obligations and Best Practices

Challenges and Legal Risks

The integration of AI in the healthcare sector raises significant legal and ethical challenges that require careful handling by all stakeholders involved. A primary issue is the lack of adequate consent and information provided to patients regarding how their personal data are processed by AI systems, which may lead to GDPR violations and subsequent legal sanctions. At the same time, sensitive health data are a privileged target for cyber attacks, making it imperative to implement advanced security measures, such as encryption and anonymization, to prevent potential breaches that could result in serious legal consequences. Particularly concerning is the phenomenon of algorithmic discrimination, as algorithms trained with biased or unbalanced data may lead to unfair or erroneous medical decisions, raising issues of medical liability and violation of the principle of equality in access to healthcare. Furthermore, the lack of compliance with the current regulatory framework constitutes a significant source of legal risk for both healthcare providers and AI technology development companies, while the limited transparency and traceability of algorithmic decisions undermines the trust of patients and healthcare professionals, creating fertile ground for legal disputes in cases of adverse outcomes or medical errors attributed to AI systems.

Obligations of Healthcare Service Providers

The modern legislative framework imposes an extensive range of obligations on healthcare service providers regarding the management of personal data and the use of AI systems. A fundamental requirement is full compliance with the GDPR and the AI Act, which establish a strict framework for the lawful processing of sensitive health data. To achieve this goal, healthcare organizations must implement advanced technical and organizational security measures, including data encryption, controlled access systems, secure storage, and protection against cyber attacks. At the same time, they are obligated to maintain a detailed record of processing activities, systematically documenting every procedure involving personal data. Particular emphasis is placed on conducting a Data Protection Impact Assessment (DPIA) before introducing any new AI application into clinical practice, in order to thoroughly analyze potential risks and design appropriate mitigation measures. Equally important is the continuous training of medical and administrative staff in proper data management practices and AI system usage, as well as ensuring that patients are fully and comprehensibly informed about the processing of their data, including the possibility of providing, refusing, or withdrawing their consent. Healthcare service providers also bear the obligation of transparency and accountability, having to demonstrate at all times their compliance with the regulatory framework and the ethical use of AI, while simultaneously ensuring the integrity and quality of data used for medical decision-making. Finally, active cooperation with the competent data protection authorities is of crucial importance, aiming at the timely resolution of issues and the adoption of best practices proposed by European and national regulatory authorities.

Best Practices for AI Use in Healthcare

The effective and ethical integration of AI in the healthcare sector requires the adoption of specific best practices that ensure both patient protection and maximization of technology benefits. A fundamental principle is data anonymization through advanced techniques that remove all personal identifying elements, making it impossible to identify individual patients during the development and use of AI systems. Equally critical is algorithm transparency, with the adoption of explainable AI models that allow doctors and patients to understand the reasoning behind each recommendation or diagnosis, thus enhancing trust and meaningful control of the systems. At the same time, systematic testing of algorithms for potential biases is required, ensuring that training data adequately represent all population groups and do not reproduce existing prejudices that could lead to unequal treatment or erroneous medical decisions. Training medical and nursing staff in the basic principles, capabilities, and limitations of AI is an integral part of every successful application, allowing critical evaluation of system recommendations and their effective integration into clinical practice. Strict compliance with the regulatory framework, including GDPR and the AI Act, is a legal obligation but also a guarantee for protecting patients' rights. The development of comprehensive ethical use protocols and guidelines adapted to the particularities of each healthcare organization contributes to addressing the complex ethical issues raised by the use of AI. Regular testing and evaluation of AI systems for accuracy, reliability, and safety, combined with ensuring human intervention in critical medical decision-making, are fundamental practices for the responsible use of technology. Finally, enhancing cybersecurity through advanced protection techniques and breach incident response protocols is essential for preventing malicious attacks and safeguarding the confidentiality of sensitive health data that feed AI systems.

Conclusions

The integration of AI in the healthcare sector offers significant opportunities for improving healthcare, but requires careful management of health data. The current legal framework, with the GDPR and the AI Act as its main pillars, sets strict requirements for the processing of sensitive data and the development of high-risk AI systems.

The successful utilization of AI in healthcare requires the adoption of best practices that ensure compliance with the legal framework, protection of patients' rights, and ethical use of technologies. Balancing innovation and personal data protection constitutes the greatest challenge, but also the key to leveraging AI capabilities for the benefit of public health.

Continuous training of healthcare professionals, transparency of AI systems, and active participation of patients in the management of their data are fundamental factors for creating an environment of trust and safety in the era of digital health.

Authors:

TMT
Intellectual Property
Employment
Litigation & Dispute Resolution
Chara Daouti
Partner

c.daouti@lambadarioslaw.gr

TMT
Intellectual Property
Virna Angelopoulou
Associate

v.angelopoulou@lambadarioslaw.gr