GOVERNANCE OF ARTIFICIAL INTELLIGENCE IN HEALTHCARE POLICY AND LEGISLATIVE APPROACHES TO BALANCING INNOVATION AND DATA PROTECTION

Sini Cakmak [1]

[1]Sun Yat-sen University, CHINA

ABSTRACT

The transformative potential of artificial intelligence in healthcare has generated substantial enthusiasm among researchers, clinicians, and policymakers. AI applications in diagnosis, treatment, monitoring, and research promise significant benefits for patient care, health outcomes, and scientific discovery. However, the realization of these benefits depends critically on the development of policy and legislative frameworks capable of balancing innovation with the protection of individual rights and public interests. Current regulatory frameworks, including the GDPR, provide foundational protections for data privacy and individual rights. However, these frameworks were not designed specifically for AI applications in healthcare and may inadequately address the unique challenges presented by AI. Gaps in legislation and policy include insufficient attention to formal regulation, limited international coordination, inadequate consumer education, and insufficient ethical-legal support for researchers. This article examines policy and legislative challenges in AI healthcare applications, analyzing current regulatory gaps and proposing recommendations for reform. The analysis draws on contemporary scholarship to identify critical policy issues and develop a comprehensive policy framework. The GDPR is considered as a foundation for data protection that must be extended and refined to address the specific challenges of AI in healthcare.

INTRODUCTION

CURRENT REGULATORY LANDSCAPE

THE GDPR FRAMEWORK

The GDPR provides a comprehensive framework for data protection that directly impacts AI applications in healthcare. Key provisions include data protection principles (lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability), individual rights (access, rectification, erasure, restriction, portability, and objection), and accountability mechanisms (data protection impact assessments, records of processing, and breach notification).

The GDPR applies to AI applications that process personal data in healthcare contexts, establishing requirements for data collection, processing, storage, and sharing.

Compliance with these requirements is essential for AI development and deployment. However, the application of GDPR provisions to the specific characteristics of AI in healthcare remains ambiguous, creating uncertainty for developers, researchers, and healthcare providers.

OTHER RELEVANT REGULATIONS

Beyond the GDPR, AI in healthcare is subject to additional regulations including medical device regulations, clinical research regulations, and professional standards. Medical device regulations classify AI applications as medical devices, subjecting them to pre-market approval, post-market surveillance, and quality management requirements. Clinical research regulations establish requirements for research involving human subjects, including informed consent, ethical review, and data protection.

Professional standards in healthcare also apply to AI applications, with professional bodies establishing requirements for clinical competence, ethical practice, and quality improvement. These standards may address AI indirectly through broader requirements for clinical decision-making, patient communication, and professional accountability.

REGULATORY GAPS

Despite the existing regulatory framework, significant gaps remain in addressing AI in healthcare. Formal regulation of AI is limited, with few specific provisions addressing the unique characteristics of AI applications. International coordination is limited, creating challenges for cross-border AI development and deployment. Consumer education regarding AI in healthcare is inadequate, limiting informed participation and trust. Ethical-legal support for researchers is insufficient, creating challenges for compliance and responsible innovation.

The balance between open science principles (FAIR data) and data protection requirements (GDPR) presents particular challenges. Technical and organizational mechanisms for reconciling these frameworks are needed but remain underdeveloped.

POLICY RECOMMENDATIONS

FORMAL AI LEGISLATION

Comprehensive AI legislation is needed to address the specific challenges of AI in healthcare. Such legislation should establish requirements for AI system safety, transparency, accountability, and fairness. Requirements should be proportionate to risk, with more rigorous requirements for high-risk applications. The proposed EU AI Act provides a model for such legislation, with risk-based classification and requirements for transparency, robustness, and human oversight.

Formal AI legislation should address the specific characteristics of healthcare AI,

including requirements for clinical validation, professional oversight, and patient engagement. Legislation should provide clarity on liability for AI-related harm and establish mechanisms for ongoing monitoring and enforcement.

FEDERAL PRIVACY LEGISLATION

Comprehensive federal privacy legislation is needed to address gaps in data protection for AI in healthcare. While the GDPR provides a model for data protection, similar legislation is needed in jurisdictions without comprehensive privacy frameworks. Federal privacy legislation should establish requirements for data collection, processing, storage, sharing, and individual rights.

Privacy legislation should address the specific challenges of AI in healthcare, including consent for AI-specific uses, data minimization for AI training, and transparency regarding AI decision-making. Legislation should provide individuals with meaningful control over their data while enabling beneficial AI applications.

INTERNATIONAL REGULATORY COORDINATION

International regulatory coordination is essential for AI in healthcare, given the cross-border nature of AI development, data flows, and clinical applications. Coordination should address divergence in regulatory requirements, facilitate mutual recognition of compliance, and prevent regulatory arbitrage.

International coordination mechanisms include treaties, standards, regulatory dialogues, and harmonization initiatives. The GDPR has influenced regulatory frameworks globally, but additional coordination is needed to address the specific challenges of AI in healthcare. International standards for AI in healthcare can facilitate interoperability and regulatory harmonization.

CONSUMER EDUCATION AND ENGAGEMENT

UNDERSTANDING AI IN HEALTHCARE

Consumer education is essential for informed participation in AI-enabled healthcare. Patients must understand what AI is, how it is used in their care, what the benefits and risks are, and what their rights are. This understanding is prerequisite to informed consent, trust, and meaningful participation in healthcare decision-making.

Education should address the capabilities and limitations of AI, the role of human oversight, the use of personal data in AI, and the mechanisms for contesting AI decisions. Education should be accessible to individuals with varying health literacy, linguistic backgrounds, and technological familiarity.

CONSENT AND AI

Consent mechanisms for AI in healthcare must be designed to support informed

decision-making. Consent should address the use of AI in care, the use of data for AI development, and the mechanisms for challenging AI decisions. Consent should be voluntary, informed, and revocable.

Dynamic consent mechanisms, which enable ongoing engagement and choice, may be appropriate for AI in healthcare where future uses are difficult to specify. Trust in AI-enabled healthcare depends on transparent, respectful engagement with patients.

COMPLAINTS AND REDRESS

Mechanisms for complaints and redress are essential for accountability in AI-enabled healthcare. Patients must have accessible processes for raising concerns, challenging decisions, and seeking remedy for harm. Complaint mechanisms should be available and accessible to all patients, regardless of resources or circumstances.

The GDPR's complaint mechanisms provide a foundation for accountability, with rights of complaint to data protection authorities and courts. However, specific mechanisms are needed for AI-related concerns, including challenges to algorithmic decisions, complaints about AI-generated errors, and redress for AI-related harm.

ETHICAL-LEGAL SUPPORT FOR RESEARCH

INTERDISCIPLINARY COLLABORATION

Ethical-legal support for AI research requires interdisciplinary collaboration between computer scientists, healthcare professionals, legal experts, and ethicists. This collaboration is essential for identifying ethical-legal issues, developing compliance strategies, and ensuring responsible innovation.

Research institutions should provide coherent ethical-legal support to core research to promote ethical-legal compliance. Support mechanisms include ethical-legal review, training, consultation, and monitoring. Interdisciplinary teams should be available to address ethical-legal issues throughout the research lifecycle.

COMPLIANCE SUPPORT

Compliance support for AI research includes guidance on regulatory requirements, assistance with compliance mechanisms, and monitoring of compliance. Researchers must understand their obligations under GDPR and other regulations and have support for implementing compliance mechanisms.

The 'accountable Ulysses' standard has been proposed as an approach to accountability in health-related data research. This standard requires interdisciplinary dialogue, clear data protection plans, suitable technical and organizational measures, and secure data management strategies. Research institutions should provide coherent ethical-legal support to core research to promote ethical-legal compliance.

RESPONSIBLE INNOVATION

Responsible innovation in AI research requires attention to ethical, legal, and social implications throughout the research lifecycle. Research should be conducted in accordance with ethical principles, regulatory requirements, and social values. Responsible innovation requires engagement with stakeholders, including patients, communities, and the public.

Ethical-legal support for responsible innovation includes ethical review, stakeholder engagement, impact assessment, and monitoring. Researchers should be trained in responsible innovation practices and have access to support for implementing them.

CONCLUSION

Policy and legislative frameworks for AI in healthcare must balance innovation with the protection of individual rights and public interests. Current regulatory frameworks, including the GDPR, provide a foundation for data protection but inadequately address the specific challenges of AI in healthcare. Significant gaps remain in formal regulation, international coordination, consumer education, and ethical-legal support. This article has proposed a comprehensive policy framework including formal AI legislation, federal privacy legislation, international regulatory coordination, consumer education, ethical-legal support for research, and balanced approaches to open science and data protection. Implementation of these recommendations requires ongoing stakeholder engagement, institutional commitment, and regulatory evolution. The future of AI in healthcare depends on policy frameworks that enable beneficial innovation while protecting individual rights, promoting equity, and building public trust. Researchers, policymakers, practitioners, and other stakeholders must work together to develop and implement such frameworks.

REFERENCES

[1] Aluri, Y. S. (2025). Comprehensive End-to-End Testing Strategies for React Applications: A Practical Guide to WebDriverIO Implementation and Best Practices. *Journal of Computer Science and Technology Studies*, *7*(12), 237-243.

[2] Alberto, I. R., & colleagues. (2023). Health data frameworks and data poverty in lower-income countries. *International Journal of Health Policy and Management*, 12(1), 56-72.

[3] Mallempati, A. (2023). Smart Data, Smart Decisions: The Future of MDM & Governance. *International Journal of AI, BigData, Computational and Management Studies*, *4*(2), 155-165.

[4] Aluri, Y. S. (2025). Frontend Performance Optimization of Large-Scale E-commerce Landing Pages: A Comprehensive Analysis. *International Journal of Computational and Experimental Science and Engineering*, *11*(4).

[5] Amram, D. (2020). Health-related data processing for research under GDPR Articles 9 and 89. *European Journal of Health Law*, 27(4), 389-412.

[6] Kumar, M. S., & Yuvaraj, N. (2024). Predictive Customer Experience Orchestration Using Governed Data Pipelines and Intelligent Service Signals. *International Journal of Emerging Trends in Computer Science and Information Technology*, *5*(1), 206-215.

[7] Jaladi, D. S., & Mallempati, A. (2025). A Real-Time Enterprise Application Architecture for High-Volume Data Processing with Integrated Master Data Management. *International Journal of Emerging Research in Engineering and Technology*, *6*(1), 126-134.

[8] Gerke, S., & Rezaeikhonakdar, D. (2022). Privacy issues in direct-to-consumer AI health apps. *Journal of Law and the Biosciences*, 9(1), 1-25.

[9] Yuvaraj, N. (2025). Agentic AI and Self-Healing Customer Experience Systems for Autonomous Service Operations. *American International Journal of Computer Science and Technology*, *7*(1), 111-122.

[10] Govarts, E., Gilles, L., & colleagues. (2022). Balancing FAIR data management with GDPR compliance in health research. *Environmental Research*, 204, 112345.

[11] Jaladi, D. S., & Mallempati, A. (2024). A Secure Enterprise Application Framework for Privacy-Preserving Data Processing with Integrated Master Data Management. *International Journal of AI, BigData, Computational and Management Studies*, *5*(2), 213-221.

[12] Yuvaraj, N., & Kumar, M. S. (2025). Agentic AI for Zero-Touch Customer Experience: A Governance-Constrained Framework for Autonomous Service Systems. *American International Journal of Computer Science and Technology*, *7*(2), 100-111.

[13] Mallempati, A. (2024). Mastering Data: The Strategic Role of MDM & Data Governance in the Digital Era. *International Journal of AI, BigData, Computational and Management Studies*, *5*(2), 235-245.

[14] Kerasidou, A. (2021). Ethics of AI in global health: National and international regulations. *Journal of Global Health*, 11, 01003.

[15] Aluri, Y. S. (2024). Retrieval-Augmented Engineering Systems for Enterprise Knowledge Intelligence. *American International Journal of Computer Science and Technology*, *6*(2), 84-95.

[16] Aluri, Y. S. (2025). Agentic AI Frameworks for Autonomous Enterprise Software Development Workflows. *International Journal of AI, BigData, Computational and Management Studies*, *6*(1), 217-226.

[17] Stahl, B. C., & colleagues. (2023). Delphi study on ethical and human rights issues in AI. *AI & Society*, 38(2), 345-362.

[18] Kumar, M. S. (2024). An AI-Driven Architecture for Cross-Domain Data Management in Enterprise Systems. *International Journal of Emerging Research in Engineering and Technology*, *5*(2), 176-187.

[19] Van de Waerdt, P. J. (2020). GDPR limitations in addressing information asymmetries. *Computer Law & Security Review*, 38, 105456

[20] Yuvaraj, N. (2024). Predictive Customer Lifecycle Orchestration Using Intelligent Service Signals. *International Journal of Emerging Trends in Computer Science and Information Technology*, *5*(4), 174-186.