

Legal Regulation of Artificial Intelligence in Healthcare: International Standards and The Emerging Regulatory Framework of Uzbekistan

Munisa Rayimova

Department of International Law and Human Rights
Tashkent, Uzbekistan, Tashkent State University of Law



Abstract

Artificial intelligence (AI) is increasingly integrated into healthcare systems for medical imaging, disease prediction, clinical decision support, patient monitoring, administrative management and, more recently, generative clinical applications. The rapid adoption of AI creates significant opportunities for improving accessibility, diagnostic accuracy and health-system efficiency, but it simultaneously challenges legal frameworks traditionally designed around identifiable human decision-makers and relatively static medical technologies. Questions concerning patient autonomy, health-data protection, algorithmic discrimination, transparency, clinical validation, professional liability and post-market monitoring have consequently become central to contemporary health law.

This article examines the emerging international and comparative legal framework governing artificial intelligence in healthcare and assesses its implications for Uzbekistan. The research applies doctrinal, comparative and normative legal methods to analyse the World Health Organization's regulatory and ethical standards, the UNESCO Recommendation on the Ethics of Artificial Intelligence, the Council of Europe Framework Convention on Artificial Intelligence, the European Union Artificial Intelligence Act, recent scholarship on medical AI liability, and Uzbekistan's evolving legislation and national AI strategy.

The article argues that general AI regulation alone is insufficient for clinical applications because healthcare AI creates distinctive risks to life, health, privacy and equality. Although Uzbekistan has adopted a national strategy for artificial intelligence development until 2030 and has identified healthcare as a priority field for AI deployment, a sector-specific regulatory architecture for medical AI remains necessary. The article proposes a risk-based model comprising six interconnected elements: classification of healthcare AI according to clinical risk; mandatory pre-market clinical and algorithmic validation; strengthened governance of health data; meaningful human oversight; a distributed liability framework; and continuous post-deployment monitoring. It concludes that alignment with emerging international standards,

	combined with regulatory adaptation to Uzbekistan's healthcare and digital infrastructure, could allow the country to promote innovation without weakening patient protection.
Keywords: Artificial intelligence; healthcare; health law; medical AI; patient safety; liability; personal data; AI Act; Uzbekistan; right to health.	

Introduction

Artificial intelligence is transforming the relationship between technology and medicine. Machine-learning systems are increasingly capable of analysing radiological images, detecting patterns in electronic health records, predicting clinical deterioration, supporting diagnosis, facilitating drug discovery and performing administrative tasks that previously depended entirely upon healthcare professionals. Generative AI and large multi-modal models further expand these possibilities by processing text, images and other forms of medical information simultaneously. The World Health Organization (WHO) recognises that AI may improve diagnosis, treatment, health research, drug development and public-health functions. At the same time, WHO stresses that the design and deployment of health-related AI must place ethics, human rights and accountability at its centre.[1]

This dual character of medical AI—simultaneously promising and potentially harmful—creates an important regulatory dilemma. Excessively restrictive regulation may slow beneficial innovation and limit access to new diagnostic and therapeutic technologies. Conversely, insufficient regulation may expose patients to inaccurate algorithms, discriminatory outputs, privacy violations, cybersecurity vulnerabilities and uncertainty concerning responsibility when AI-assisted decisions cause harm.

These challenges differ qualitatively from many conventional medical technologies. AI systems may change through updates, interact with changing clinical environments and generate outputs through computational processes that are difficult for users to interpret. Moreover, an AI-supported medical decision can involve multiple participants: the software developer, data provider, medical-device manufacturer, healthcare institution and clinician. This fragmentation complicates traditional models of professional negligence and product liability. Recent legal scholarship therefore increasingly questions whether conventional liability doctrines alone are capable of allocating responsibility fairly when medical AI causes patient injury.[2]

The regulatory question is particularly significant for emerging digital-health systems. Uzbekistan has adopted a national Strategy for the Development of Artificial Intelligence Technologies until 2030 through Presidential Resolution No. PQ-358 of 14 October 2024. The Strategy expressly identifies healthcare applications including disease diagnosis, determination of treatment methods, analysis of medical images and patient-data management.[3]

The national policy has therefore moved beyond the theoretical discussion of AI toward practical implementation. According to official information released in 2025–2026, several AI projects are already being implemented in Uzbekistan's healthcare sector, including applications concerning stroke and breast-cancer diagnostics.[4]

The central research question of this article is therefore: What legal framework should govern the development and use of artificial intelligence in healthcare in Uzbekistan in light of emerging international and comparative standards?

The article argues that an effective model should not regulate medical AI exclusively through general technology legislation. Instead, Uzbekistan requires a healthcare-specific, risk-based regulatory framework combining medical-device regulation, data protection, professional responsibility, human-rights safeguards and AI lifecycle governance.

2. Research Methodology

This study employs three interconnected research methods.

First, the doctrinal legal method is used to analyse international instruments and national legislation relevant to AI, healthcare, human rights and personal-data protection.

Second, the study applies a comparative legal method, with particular attention to the European Union's risk-based approach under Regulation (EU) 2024/1689—the Artificial Intelligence Act. The EU framework is not treated as a model that should simply be transplanted into Uzbek law. Instead, it is examined as an advanced regulatory example demonstrating how legal obligations may vary according to the level of risk generated by an AI system.

Third, a normative method is employed to formulate regulatory recommendations for Uzbekistan. The recommendations are based on the specific characteristics of medical AI and the constitutional, legislative and strategic development of digital technologies within Uzbekistan. The analysis is based primarily on legal and policy documents produced by WHO, UNESCO, the Council of Europe, the European Union and competent authorities of Uzbekistan, supplemented by peer-reviewed legal and medical scholarship published between 2023 and 2026.

3. Artificial Intelligence in Healthcare as a Distinct Regulatory Category

The term “artificial intelligence in healthcare” encompasses heterogeneous technologies. An algorithm that schedules hospital appointments creates fundamentally different legal risks from an autonomous system assisting with cancer diagnosis.

Consequently, healthcare AI should not be regulated as a single homogeneous category.

For regulatory purposes, medical AI may be divided broadly into four groups: administrative AI, including scheduling, documentation and resource management; clinical decision-support systems, which assist healthcare professionals in diagnosis or treatment selection; AI-enabled medical devices, including diagnostic software and image-analysis systems; and patient-facing or generative AI systems, including symptom-assessment tools, conversational systems and large multi-modal models.

The legal intensity required for each category should correspond to the potential harm associated with its use.

WHO's 2023 publication *Regulatory Considerations on Artificial Intelligence for Health* similarly emphasises the importance of intended use, risk-benefit assessment, transparency, documentation, data quality, external validation, privacy, cybersecurity and lifecycle monitoring.[5]

This risk-based logic is particularly persuasive in medicine because an algorithm's consequences may extend directly to the right to life and the right to health. Incorrect administrative automation

may generate inconvenience. Incorrect clinical automation may delay cancer diagnosis, recommend an unsuitable intervention or fail to detect a life-threatening condition.

Medical AI regulation must therefore distinguish between technological risk and clinical risk. Technological sophistication should not itself determine regulatory intensity. A relatively simple algorithm influencing a critical medical decision may require stronger oversight than a technically sophisticated AI application performing a non-clinical administrative task.

4. International Normative Framework

4.1. World Health Organization

WHO has developed one of the most comprehensive normative frameworks specifically addressing artificial intelligence in health.

Its 2021 guidance Ethics and Governance of Artificial Intelligence for Health identifies six central principles: protecting human autonomy; promoting human well-being, human safety and the public interest; ensuring transparency, explainability and intelligibility; fostering responsibility and accountability; ensuring inclusiveness and equity; and promoting AI that is responsive and sustainable.[6]

These principles demonstrate that medical AI governance cannot be reduced to questions of technical safety. It is equally concerned with the distribution of benefits, human agency and mechanisms for challenging algorithmically influenced decisions.

WHO's subsequent regulatory work places particular emphasis on transparency throughout the product lifecycle, clearly defined intended use, external validation, data quality and protection against algorithmic bias. WHO also recommends that privacy and cybersecurity safeguards be incorporated from an early stage of system development rather than added only after deployment.[7]

The rapid expansion of generative AI required further adaptation. WHO's guidance concerning large multi-modal models identifies applications including clinical care, patient-guided health use, administrative tasks, medical education and scientific research. WHO simultaneously warns of false, inaccurate, biased or incomplete outputs and recommends regulatory review, post-release auditing and impact assessment where such systems are used in healthcare.[8]

The significance of the WHO approach lies in its lifecycle perspective: regulatory responsibility does not end when an AI system enters the market.

4.2. UNESCO Recommendation on the Ethics of Artificial Intelligence

The UNESCO Recommendation on the Ethics of Artificial Intelligence, adopted in 2021, establishes a broader human-rights framework applicable to healthcare AI.

The Recommendation is based on human dignity, transparency, fairness, accountability, non-discrimination and human oversight.[9]

Healthcare receives specific attention in Policy Area 11. UNESCO calls upon states to ensure that health-related AI systems are safe, effective, scientifically and medically validated, while protecting privacy and ensuring informed involvement of patients.

Particularly significant is UNESCO's position that human care and ultimate diagnostic and treatment decisions should remain under meaningful human responsibility rather than being fully displaced by automated systems.[10]

This approach is important from a legal perspective. “Human oversight” should not become a symbolic requirement where a clinician merely approves an algorithmic recommendation without having sufficient information, competence or practical opportunity to challenge it. Meaningful oversight requires awareness that AI is being used; sufficient understanding of the system's intended function and limitations; access to clinically relevant explanations; authority to reject the recommendation; and sufficient time to exercise independent professional judgment.

4.3. Council of Europe Framework Convention on Artificial Intelligence

The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law was opened for signature on 5 September 2024.

It is the first legally binding international treaty specifically addressing artificial intelligence. Its central purpose is to ensure that activities throughout the lifecycle of AI systems remain consistent with human rights, democracy and the rule of law.[11]

Although it is not a healthcare-specific instrument, its human-rights-centred logic is highly relevant to medical AI. The Convention reflects an important development in AI governance: a shift from purely ethical guidelines toward legally structured accountability.

For healthcare systems, this reinforces the proposition that algorithmic safety should be assessed not only through accuracy metrics but also through rights-based considerations, including privacy, equality, access to remedies and protection against unjustified automated interference with individual autonomy.

5. The European Union AI Act and Medical Artificial Intelligence

Regulation (EU) 2024/1689 represents the world's most developed comprehensive statutory framework for artificial intelligence.

Its principal regulatory technique is a risk-based classification system. AI systems that constitute safety components of regulated products, or are themselves products governed by specified EU harmonisation legislation, may qualify as high-risk systems. This framework expressly includes certain medical devices and in-vitro diagnostic devices where the applicable conformity-assessment requirements are satisfied.[12]

This classification triggers substantive obligations. Providers of high-risk AI systems are required to establish continuous risk-management systems. Article 9 requires identification and evaluation of known and reasonably foreseeable risks to health, safety and fundamental rights throughout the AI system's lifecycle.[13]

Article 10 addresses data governance. Training, validation and testing datasets must be governed in a manner appropriate to the intended purpose of the AI system. Particular attention must be given to data origin, preparation and potential biases capable of affecting health, safety or fundamental rights.[14]

Article 13 requires sufficient transparency to enable deployers to interpret outputs and use them appropriately. Information concerning intended purpose, accuracy, known limitations, foreseeable risks and human-oversight mechanisms must accompany high-risk systems.[15]

Article 14 establishes human-oversight requirements, while Article 15 requires appropriate levels of accuracy, robustness and cybersecurity throughout the lifecycle of the system.[16]

The relevance of the EU model for Uzbekistan lies not in institutional replication but in the legal structure of its obligations. It demonstrates that medical AI governance can move beyond abstract ethical principles and impose specific requirements concerning risk, data, validation, documentation, transparency, human supervision, cybersecurity and monitoring. This regulatory chain could provide an appropriate conceptual foundation for future Uzbek legislation.

6. Patient Autonomy and Informed Consent

One of the most difficult health-law questions concerns whether patients should be specifically informed when AI materially contributes to their diagnosis or treatment.

Traditional informed-consent doctrine generally requires disclosure concerning the proposed medical intervention, material risks and reasonable alternatives. AI introduces a new question: is the use of an algorithm itself information that could be material to patient decision-making?

A distinction should be drawn between invisible administrative use and clinically consequential AI. There may be little justification for requiring separate patient consent whenever AI is used to perform routine administrative tasks. The position is different when an AI system materially influences diagnosis, treatment selection, prognosis, eligibility for healthcare, interpretation of medical images, or another clinically significant decision.

Where AI has a meaningful role, the patient should normally receive information concerning its function and the fact that it contributes to the decision-making process. This does not require clinicians to explain source code or complex machine-learning architecture. The legal objective should instead be clinically meaningful transparency.

The patient should be able to understand that AI is being used; what role the system performs; whether the final decision remains subject to professional human judgment; significant limitations relevant to the patient's circumstances; and, where appropriate, whether a reasonable non-AI alternative is available.

This model protects patient autonomy without transforming medical consent into a technical lecture.

7. Health Data, Privacy and Algorithmic Bias

Artificial intelligence depends upon data, and medical AI frequently depends upon particularly sensitive data. Healthcare datasets may include medical history, genetic information, laboratory results, diagnostic images, medication records, disability information and behavioural data.

The resulting legal problem is not merely confidentiality. AI requires large datasets for training, validation and continuous improvement, potentially creating tension between innovation and privacy.

Uzbekistan's Constitution provides a significant foundation for addressing this issue. Article 31 guarantees protection of personal data and provides individuals with rights relating to inaccurate or unlawfully collected data. Article 48 recognises the right to health and qualified medical care.[17]

The Law of the Republic of Uzbekistan "On Personal Data", No. O'RQ-547 of 2 July 2019, provides the principal legislative framework regulating personal information.[18]

However, medical AI creates challenges that cannot always be addressed through conventional consent-based data protection. AI models may be trained using data originally collected for

clinical care rather than algorithm development; apparently anonymised medical datasets may retain re-identification risks when combined with other information; and algorithmic bias may arise even when data processing is formally lawful.

A dataset may under-represent particular demographic, geographical or clinical groups. Consequently, a system may achieve strong overall accuracy while performing poorly for specific patient populations. This creates a legal equality issue as well as a technical accuracy problem.

Healthcare AI regulation should therefore require developers and healthcare organisations to evaluate performance across relevant patient groups rather than relying exclusively on aggregate accuracy. WHO likewise emphasises data representativeness and the risks of bias arising when training populations fail to reflect the diversity of actual users.[19]

For Uzbekistan, local validation is especially important. An AI system trained predominantly using datasets from another healthcare system cannot automatically be assumed to perform equally well within Uzbek clinical populations, infrastructure and medical practice.

8. Liability for Harm Caused by Medical AI

The integration of AI into clinical decision-making complicates traditional legal responsibility.

Consider a hypothetical situation: an AI system analyses a radiological image and fails to detect a malignant lesion. A physician relies on the system and reports the image as non-suspicious. Treatment is subsequently delayed.

Who should bear responsibility? Possible defendants include the treating physician, the hospital, the AI developer, the manufacturer or distributor, the entity responsible for training data, or several actors simultaneously.

Recent literature demonstrates that existing legal doctrines frequently struggle with this fragmented decision-making structure. Mello and Guha note that healthcare organisations and physicians face complex liability questions when AI tools are incorporated into medical practice.[20] Fotheringham and Smith similarly argue that conventional negligence frameworks may allocate responsibility unfairly where clinicians operate alongside software whose internal defects they cannot reasonably identify.[21] Price, Gerke and Cohen emphasise that AI-related injury potentially implicates multiple forms of liability extending across clinicians, healthcare institutions and technology developers.[22]

A particularly problematic solution would be to treat the AI system itself as legally responsible. Current AI systems do not possess legal or financial capacity comparable to natural or juridical persons. Assigning liability to AI could instead create an accountability gap by shielding human and corporate actors.

A preferable solution is distributed responsibility. Liability should correspond to the actor's control over the relevant source of risk. Developer responsibility may arise from defective design, inadequate training or validation, failure to disclose known limitations, cybersecurity failures, or unsafe updates. Healthcare institution responsibility may arise from inadequate procurement assessment, use of a system outside its authorised purpose, insufficient staff training, failure to monitor performance, or absence of institutional governance. Clinician responsibility may arise where the professional unreasonably ignores contradictory clinical information, uses an AI system beyond its intended purpose, relies blindly on an output despite obvious warning signs, or fails to exercise the degree of human judgment required by professional standards.

This approach avoids placing the entire burden on clinicians while preserving professional responsibility where meaningful clinical judgment remains possible.

9. The Emerging Framework of Uzbekistan

Uzbekistan has taken significant steps toward establishing national AI policy. Presidential Resolution No. PQ-358 of 14 October 2024 approved the Strategy for the Development of Artificial Intelligence Technologies until 2030.[23]

The Strategy establishes objectives including development of the regulatory framework for AI; implementation of AI across social and economic sectors; improvement of relevant standards; strengthening international cooperation; development of computing infrastructure; and expansion of AI knowledge and professional capacity.

Healthcare is expressly included among the priority sectors. Potential applications identified by the Government include disease diagnosis, determination of treatment approaches, analysis of medical images and management of patient data.[24]

Uzbekistan's broader digital strategy was further updated in 2026, reflecting continued development of national AI infrastructure and strategic planning.[25]

The implementation process has already entered the healthcare sector. Government information states that five healthcare AI projects have been under implementation and reports substantial reductions in diagnostic time in selected applications concerning stroke and breast cancer.[26]

These figures should be understood as official implementation reports rather than independent clinical-effectiveness evidence.

The national strategy therefore establishes a strong innovation mandate. The next stage should be the creation of an equally strong patient-protection architecture. At present, the relevant legal framework is distributed among constitutional guarantees, personal-data legislation, healthcare regulation, general civil-law principles, medical professional responsibility and emerging AI policy. This fragmented approach may be sufficient during early experimental deployment but becomes increasingly problematic as AI begins to influence routine clinical decisions.

10. Proposed Regulatory Model for Uzbekistan

10.1. Risk-Based Classification

Healthcare AI should be classified according to potential clinical consequences. A possible model could distinguish low-risk administrative scheduling and logistics; moderate-risk decision-support systems; high-risk systems materially influencing diagnosis, treatment, prognosis or emergency decision-making; and very high or restricted-risk applications intended to make specified irreversible or highly consequential clinical decisions without meaningful human intervention. Higher-risk systems should be subject to progressively stronger legal requirements.

10.2. Mandatory Clinical and Algorithmic Validation

Before high-risk AI is deployed within the national healthcare system, its safety and effectiveness should be demonstrated. Validation should include technical accuracy; clinical validity; performance across relevant demographic groups; cybersecurity; foreseeable misuse; compatibility with the intended clinical environment; and local or context-sensitive validation where appropriate. Foreign regulatory approval should be relevant but should not automatically eliminate the need to examine whether a system performs adequately within Uzbekistan.

10.3. Healthcare AI Registry

Uzbekistan could establish a national electronic register of high-risk AI systems authorised for clinical use. The register could include system name and developer; intended clinical purpose; approved healthcare settings; regulatory classification; date of authorisation; key performance information; significant known limitations; and post-market safety notices. A register would strengthen transparency for hospitals, clinicians, patients and regulators.

10.4. Meaningful Human Oversight

Human oversight should be legally defined rather than treated as an abstract ethical principle. For high-risk clinical systems, the responsible healthcare professional should have appropriate competence; access to information concerning system limitations; authority to disregard an AI output; sufficient time to review the result; and access to a procedure for reporting suspected algorithmic errors. A formal requirement that “a human remains involved” is insufficient if the human merely confirms an automated result.

10.5. Distributed Liability

Uzbek law should clarify the allocation of responsibility among AI developers, medical institutions and healthcare professionals. Liability should generally follow control over risk. Developers should remain responsible for technology-related defects that a reasonable clinician could not detect. Healthcare organisations should bear responsibility for institutional failures involving procurement, training, integration and monitoring. Clinicians should remain responsible for professional decisions within the scope of meaningful human judgment. This model would better reflect the actual distribution of decision-making than automatically attributing all AI-related clinical harm to the final healthcare professional.

10.6. Post-Market Monitoring and Mandatory Incident Reporting

Pre-market approval cannot predict every real-world problem. Medical AI may perform differently after deployment because of changes in patient populations, software updates, data drift, interaction with different clinical workflows, cybersecurity incidents, or unforeseen patterns of misuse.

High-risk AI should therefore be monitored throughout its operational lifecycle. Healthcare institutions and developers should be required to report serious AI-related incidents to the competent regulatory authority. Where necessary, the regulator should be empowered to demand corrective updates, restrict an authorised use, temporarily suspend deployment, require additional validation, or withdraw authorisation. This would bring AI regulation closer to the logic of pharmacovigilance and medical-device surveillance.

11. Discussion

International AI governance reveals increasing convergence around several principles. WHO, UNESCO, the Council of Europe and the European Union differ in legal authority, scope and institutional design. Nevertheless, they increasingly emphasise the same core regulatory elements: human agency, safety, transparency, high-quality data, non-discrimination, accountability and continuous risk management.

This convergence provides an opportunity for Uzbekistan. The country does not need to wait for a universally harmonised global AI treaty before developing medical-AI regulation. Nor is it necessary to reproduce the EU AI Act word for word.

Instead, Uzbekistan can adopt what may be described as contextual regulatory convergence. Under this approach, the country would incorporate internationally established principles while adapting institutional procedures to domestic healthcare capacity, available regulatory expertise and national digital infrastructure.

An important balance must nevertheless be maintained. Overregulation at an early stage could disproportionately burden universities, hospitals and domestic start-ups and may encourage dependence on large foreign technology providers. Under-regulation, however, may impose even greater long-term costs where unsafe technologies erode public trust or cause preventable patient harm.

Regulatory sandboxes could therefore play a useful transitional role. Selected health-AI technologies could be tested under controlled conditions involving regulators, healthcare organisations, developers and research institutions. However, a sandbox should not constitute an exemption from fundamental patient rights. Requirements concerning safety, confidentiality, informed participation and independent oversight must remain applicable.

12. Conclusion

Artificial intelligence is changing not only medical practice but also the legal architecture surrounding healthcare decision-making. Traditional health law generally assumes identifiable healthcare professionals, relatively stable medical products and established chains of responsibility. AI disrupts each of these assumptions.

The international regulatory response is consequently moving from broad ethical principles toward concrete lifecycle obligations. WHO standards emphasise autonomy, safety, accountability, transparency, inclusiveness and continuous governance. UNESCO places AI within a human-rights and human-dignity framework. The Council of Europe has introduced the first legally binding international AI treaty. The European Union AI Act translates risk-based governance into detailed obligations concerning risk management, data quality, transparency, human oversight, accuracy and cybersecurity.

Uzbekistan has already established an ambitious national strategy for AI development and has designated healthcare as a priority area. The strategic question is therefore no longer whether artificial intelligence will enter the healthcare system, but under what legal conditions this transformation should occur.

This article submits that the next phase of reform should focus on six pillars: risk-based classification of healthcare AI; mandatory pre-market clinical and algorithmic validation; enhanced governance of health data and algorithmic bias; legally meaningful human oversight; distributed responsibility among developers, healthcare institutions and professionals; and continuous post-market monitoring and incident reporting.

Such a framework would not require Uzbekistan to choose between innovation and regulation. On the contrary, predictable regulation can facilitate innovation by providing legal certainty to developers, healthcare institutions, clinicians and patients.

The ultimate objective of medical-AI law should therefore be neither technological restriction nor unconditional technological expansion. It should be to ensure that artificial intelligence remains a tool for advancing the right to health while protecting human dignity, patient autonomy, equality and accountability.

Notes

- [1] World Health Organization, Ethics and Governance of Artificial Intelligence for Health: WHO Guidance, Geneva: WHO, 2021.
- [2] M.M. Mello and N. Guha, “Understanding Liability Risk from Using Health Care Artificial Intelligence Tools”, *New England Journal of Medicine*, Vol. 390, 2024, pp. 271–278. DOI: 10.1056/NEJMHle2308901.
- [3] Resolution of the President of the Republic of Uzbekistan No. PQ-358, 14 October 2024, “On Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030”.
- [4] Government of the Republic of Uzbekistan, official information on expansion of artificial intelligence technologies in economic and social sectors, 2025–2026.
- [5] World Health Organization, Regulatory Considerations on Artificial Intelligence for Health, Geneva: WHO, 2023, ISBN 978-92-4-007887-1.
- [6] World Health Organization, Ethics and Governance of Artificial Intelligence for Health, 2021.
- [7] World Health Organization, Regulatory Considerations on Artificial Intelligence for Health, 2023.
- [8] World Health Organization, Ethics and Governance of Artificial Intelligence for Health: Guidance on Large Multi-Modal Models, Geneva: WHO, 2024/2025, ISBN 978-92-4-008475-9.
- [9] UNESCO, Recommendation on the Ethics of Artificial Intelligence, adopted 23 November 2021, published Paris: UNESCO, 2022.
- [10] Ibid., Policy Area 11: Health and Social Well-Being, paras 121–125.
- [11] Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, opened for signature 5 September 2024.
- [12] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence, 13 June 2024.
- [13] Ibid., Art. 9.
- [14] Ibid., Art. 10.
- [15] Ibid., Art. 13.
- [16] Ibid., Arts. 14–15.
- [17] Constitution of the Republic of Uzbekistan, Arts. 31 and 48.
- [18] Law of the Republic of Uzbekistan No. O‘RQ-547 of 2 July 2019, “On Personal Data”.
- [19] World Health Organization, Regulatory Considerations on Artificial Intelligence for Health, 2023.
- [20] Mello and Guha, *supra* note 2.

- [21] K. Fotheringham and H. Smith, “Accidental Injustice: Healthcare AI Legal Responsibility Must Be Prospectively Planned Prior to Its Adoption”, *Future Healthcare Journal*, Vol. 11, No. 3, 2024, 100181. DOI: 10.1016/j.fhj.2024.100181.
- [22] W.N. Price II, S. Gerke and I.G. Cohen, “Liability for Use of Artificial Intelligence in Medicine”, in B. Solaiman and I.G. Cohen (eds.), *Research Handbook on Health, AI and the Law*, Edward Elgar, 2024. DOI: 10.4337/9781802205657.ch09.
- [23] Presidential Resolution No. PQ-358, *supra* note 3.
- [24] *Ibid.*
- [25] Decree of the President of the Republic of Uzbekistan No. PF-141 of 24 July 2026 concerning strategic planning and state oversight in the field of digital technologies.
- [26] Government of the Republic of Uzbekistan, official information concerning implementation of healthcare AI projects, 2025–2026.

References

1. Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. Strasbourg: Council of Europe.
2. European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
3. Fotheringham, K., & Smith, H. (2024). Accidental injustice: Healthcare AI legal responsibility must be prospectively planned prior to its adoption. *Future Healthcare Journal*, 11(3), 100181. DOI: 10.1016/j.fhj.2024.100181.
4. Mello, M. M., & Guha, N. (2024). Understanding liability risk from using health care artificial intelligence tools. *New England Journal of Medicine*, 390, 271–278. DOI: 10.1056/NEJMHle2308901.
5. Nunnelle, S., Flood, C. M., Da Silva, M., & Horsley, T. (2025). Cracking the code: A scoping review to unite disciplines in tackling legal issues in health artificial intelligence. *BMJ Health & Care Informatics*, 32(1), e101112. DOI: 10.1136/bmjhci-2024-101112.
6. Price, W. N. II, Gerke, S., & Cohen, I. G. (2024). Liability for use of artificial intelligence in medicine. In B. Solaiman & I. G. Cohen (Eds.), *Research Handbook on Health, AI and the Law*. Edward Elgar Publishing. DOI: 10.4337/9781802205657.ch09.
7. Republic of Uzbekistan. (2019). Law No. O'RQ-547 of 2 July 2019, On Personal Data.
8. Republic of Uzbekistan. (2023). Constitution of the Republic of Uzbekistan, Arts. 31, 48.
9. Republic of Uzbekistan. (2024). Resolution of the President No. PQ-358 of 14 October 2024, On Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030.
10. Republic of Uzbekistan. (2026). Presidential Decree No. PF-141 of 24 July 2026 concerning strategic planning and state oversight in the field of digital technologies.
11. UNESCO. (2022). *Recommendation on the Ethics of Artificial Intelligence*. Paris: United Nations Educational, Scientific and Cultural Organization.
12. World Health Organization. (2021). *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance*. Geneva: WHO. ISBN 978-92-4-002920-0.
13. World Health Organization. (2023). *Regulatory Considerations on Artificial Intelligence for Health*. Geneva: WHO. ISBN 978-92-4-007887-1.
14. World Health Organization. (2024/2025). *Ethics and Governance of Artificial Intelligence for Health: Guidance on Large Multi-Modal Models*. Geneva: WHO. ISBN 978-92-4-008475-9.