Science of Law Journal (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2025.040602
ISSN 2616-2296 Vol. 4 Num. 6

Legal Risks and Regulatory Strategies in the Clinical Application of Medical Artificial Intelligence

Lianti Jiang

Grandall Law Firm (Tianjin), Tianjin, 300042, China

Keywords: Medical Artificial Intelligence; Legal Risks; Regulatory Strategies; Data Compliance

Abstract: Although the large-scale clinical application of medical artificial intelligence has driven revolutionary changes in medical services, it has also triggered a complex web of legal risks. This article conducts a comprehensive analysis of typical risks inherent in medical artificial intelligence, such as product liability, medical injury, data security, and responsibility attribution, and then evaluates the insufficiencies of current law, including its contradictions in allocating liability, continued frictions in data-compliance rules, and overall delays in regulatory adaptation. Upon this foundation, the article promotes a holistic regulatory strategy with four practical dimensions: clarifying rules on responsibility allocation, enhancing full-chain data governance, speeding up the formulation of dedicated laws, and building a co-governance model. Combined with each other, these four dimensions should provide a theoretical reference for regulating the development of medical AI in a dual-sided innovation-risk control.

1. Introduction

As artificial intelligence technology gradually enters and transforms the medical field, the legal risks posed by increasingly complex medical AI in improving medical efficiency and accuracy are also emerging. This study attempts to make an integrated analysis of diverse legal risks that may be triggered in the clinical use of medical AI in four aspects: product liability, medical injury, data security, and attribution rules. The article also questions the points of friction and deficiency in the current regulatory order. Based on the above research findings, this article further proposes a regulatory order that coordinates technological innovation and risk prevention in four dimensions: responsibility rules, data order, legislative standards, and collaborative oversight to promote the healthy and sustainable development of medical AI.

2. Analysis of Legal Risks in the Clinical Application of Medical Artificial Intelligence

2.1 Product Liability Risks

Discussants agreed that risks of medical AI products under product liability law arise primarily from defects inherent in the medical AI products as “conceived” or “designed.” On one side, the “algorithmic black box” surrounding the decision logic of medical AI systems creates the possibility

that harm-causing biases in diagnosis or inaccurate predictions not detectable to clinicians could exist and remain latent; and defects in the training data that do not reflect diversity in population could give rise to discriminatory output, a design defect[1]. On the other side, as hybrid products containing hardware and software, the medical AI products themselves could be rendered dysfunctional due to software coding errors, sensor malfunction, or hardware defects. Under the Product Quality Law and accompanying regulations, manufacturers could be strictly liable for harm caused to patients using such defective products. However, AI's ability to learn and evolve raises a more complex question. As AI's "baseline" or the standard against which what might amount to a "defect" at the time the product was released becomes fuzzier, the question of whether harm arises from an initial defect in design, a defective software update, or misused by a medical institution becomes increasingly analytically difficult and legally fraught.

2.2 Medical Injury Liability Risks

This category includes situations in which harmful patient outcomes caused by incorrect outputs from AI-assisted clinical decision-making processes usefully force us to confront questions of care standard and fault attribution[2]. Because clinicians who over-rely on or blindly follow AI advice are committing negligence by failing to fulfill the traditional standard of duty, courts must decide whether and how to recalibrate standards of professional duty in the digital age. Traditional doctrines of medical injury liability have focused on health care professionals; but when the injury stems from unseen or unanticipated mistakes in AI assistance, placing the full burden of responsibility on clinicians would be unfair. The ensuing clinician dilemmas- clinicians liable if they strayed from a correct AI suggestion? Clinicians liable if they followed an incorrect AI suggestion?-shake the traditional patient-provider tort world and raise significant questions about the viability of medical injury clauses of the Civil Code, prompting a need to clarify fault-allocation principles in human–AI collaborative practice.

2.3 Data and Privacy Security Risks

Since both the development and operation of medical AI are fundamentally based on large amounts of patients' health information, they are intrinsically prone to data-security and privacy attacks. In terms of data collection, if informed-consent procedures are not properly implemented, the scope of authorization would be ambiguous at best, and the consent would be invalid at worst[3]. In terms of data processing and model training, even large datasets that have undergone anonymization can be re-identified due to sophisticated analytical methods, which would lead to privacy breaches. At the operation stage, medical AI may also be attacked by cyberattacks and the attacked health information would be stolen or manipulated. All of these risks would collectively lead to non-compliance with mandatory obligations under the Personal Information Protection Law and the Data Security Law, such as the obligation to obtain explicit and separate consent when processing sensitive personal information and the obligation to adopt strict protective measures. Non-compliance would lead to heavy administrative penalties and civil liabilities for healthcare institutions or operators, as well as the demise of their clients-trust.

2.4 Risks in Identifying Responsible Actors

Given the multilayered network of actors involved in the clinical use of medical AI - ranging from algorithm developers, hardware manufacturers, software operators, medical institutions and clinicians - it becomes very challenging to attribute responsibility when harm arises[4]. The linear responsibility model breaks down in such multilayered systems and may lead to gaps in

accountability as well as expansive diffusion of joint liability. For example, if the patient is harmed due to a flaw in the algorithmic design, should the legal liability of the algorithmic developer be traced? Or should it instead run all the way up to the hospital that should have ensured the validity checks of AI outputs? If there are multiple factors that jointly contribute to the injury, how should causal responsibility be divided? These attributional challenges not only hinder patients' chances of obtaining compensation but also exacerbate legal uncertainty for stakeholders, depressing incentives for technological innovation. An accountability framework that can navigate through these multiple layers and allocate liability in a fair and predictable way is an indispensable component of any regulatory system.

3. Limitations and Challenges in the Existing Legal and Regulatory Framework

3.1 Conflicts in the Application of Product Liability and Medical Liability

Under today's laws, litigating harm from medical AI will face a fundamental collision between the Product Quality Law and the Medical Injury Liability Regulations. If AI is classified as a "product," the Product Quality Law subjects manufacturers to strict liability and enables victims to seek compensation from manufacturers-yet those victims may nevertheless fail at that point and be barred from securing compensation, under the "development risks defense" that immunizes producers from liability for the foreseeable limitations of their products. Alternatively, if AI remains classified as merely an instrument attached to medical services, the fault-based liability regime applies, and medical institutions and practitioners bear the burden. In this scenario, victims need to prove that clinicians fell below the standard of care expected of a reasonable practitioner in light of modern medical standards-a requirement almost impossible to meet[5]. Thus, the definitional swinging allows for either overly heavy costs borne by manufacturers and stifling of innovation, or, alternatively, watered-down accountability for medical institutions, undermining of patient rights and creation of a gap in tort law.

3.2 Practical Dilemmas in Data Compliance and Authorization

Due to the heavy reliance on health information throughout both the training and deployment of medical AI, real-world medical AI development often faces a layered compliance dilemma. First, the prevailing "informed consent" model, which is a one-time ex ante consent for a specific purpose at a specific time, is not fit for the iterative life cycle of AI development where reuse of data is often necessary for the fine tuning of a model. This gives rise to the latent risk that "one time consent will permit perpetual use," which may trigger statutory breach. Second, although anonymization is practiced to protect the generalizability of AI models, the technical barrier of "non-identifiability" is weak given the speedy development of re-identification techniques, making the anonymized data sets almost indistinguishable from personal information. Furthermore, when R&D is conducted across institutions, the legal basis for cross-institutional flows of data within a domestic cluster and cross-border flows to overseas collaborators are both unclear, making compliance very precarious and driving developers to walk on a tightrope between data utility and regulatory safety.

3.3 Legislative Vacuums in Recognizing AI as a Legal Subject

China's rigid two-tier classification of legal subjects-natural persons and legal or non-legal organizations-confers no legal personality on artificial intelligence as an independent sovereign. The gap is fatal. When an AI-enabled diagnostic system makes a decision different from the developer's original design specification due to its ability to learn autonomously, and its decisions

injure someone, the system cannot be designated as a defendant and cannot be made to bear civil or criminal liability. Instead, the risk must be borne by human actors-developers, users, or owners-whether or not it proves substantively fair or yields coherent doctrinal analysis. Whether China should concede to new debates about "electronic personhood" and confer limited legal status on highly autonomous AI systems-capable of holding rights and bearing responsibilities- is a foundational and difficult question that cannot be ducked by future laws.

3.4 Lagging Technical Review and Regulatory Standards

In the midst of such incredible technological change, current regulatory and technical review processes for medical devices are woefully behind the times. Static, batch review models are not suited to judge the performance of adaptive and always-self-learning AI algorithms. Most current reviews of performance are still focused on hardware performance and static software functions, leaving gaps in the assessment of algorithmic robustness, data bias mitigation, and clinical risk assessment. Finally, we still operate under a regulatory paradigm where most medical devices are granted a "once-and-for-all" license and then monitored passively in the market–even though AI products are likely to exhibit performance drift, model decay, and behavioral changes unseen during training as they are put to use by patients and physicians.

4. Constructing a Multifaceted Regulatory Strategy for Medical Artificial Intelligence

4.1 Clarifying Rules for Liability Attribution and Apportionment

On the theoretical level, it is vital to break out of the "either–or" mindset in attributing responsibility and instead construct a dynamic liability regime focusing on risk-sharing, accompanied by a presumption of fault doctrine. Based on differential classification of AI products according to their degree of autonomy and concrete clinical scenarios, corresponding liability rules can be rationally calibrated. With respect to highly autonomous systems, the responsibility of the producer may have to include-at least in a reasonable range-post-deployment learning usage. While, in concrete clinical scenarios using AI for making decisions, those who invoke AI to treat patients should be subjected to a presumption of fault, i.e. presumed negligent and required to exercise due care. Only through such rule-calibration based on differentiated classification of AI systems, can we achieve a more balanced and proportional distribution of responsibility in human–AI collaborative endeavors, which could prevent the diffusion of accountability and splitting of liability across actors.

In addition, a scenario-based liability allocation mechanism can be further embedded into the above rule-calibration mechanism for more operational implementation. For instance, in the concrete scenario of AI application in assisting radiologists to diagnose lung cancer, if AI misses the early-stage lung cancer due to its design fault (i.e. biased training data or insufficiently representative training sample), then the manufacturer should be allocated product liability. On the other hand, if the AI flagged a suspicious nodule on the CT image but the attending physician failed to acknowledge or further investigate the flag, leading to the eventual harm, the physician should be presumed negligent and liable under medical malpractice principles. Similarly, in the concrete scenario of robotic surgery, if the hardware failure led to operative failure, then the liability should clearly lie with the manufacturer; however, if there is complication due to the surgeon deviating from the standard procedure or ignoring the safety warnings emitted by the robot system, then the liability should be properly allocated to the physician. Through such detailed rule-calibration based on concrete scenarios, the rights and obligations of various actors could be demarcated clearly, and provide the courts with an operational mechanism to adjudicate concrete cases.

4.2 Strengthening Full-Lifecycle Data Compliance and Governance

At the conceptual level, we need to go beyond the static paradigm of "end-point compliance" and build a dynamic governance system along the entire data life cycle-from data generation and storage to processing and transmission and eventual deletion. The most important requirement is to embed the ideas of compliance by design and compliance by default into the architecture of AI systems, and connect technical safeguards and legal requirements in a profound and integrated manner. Through this connection, data protection can be transformed from a static, post hoc defensive measure into a dynamic, intrinsically embedded one. Only in this way can data protection become an inherent property of system functionality rather than an exogenous layer.

In practice, there are several possible scenarios. In the research and development phase, when hospitals collaborate with AI companies to train clinical prediction models, strong anonymization techniques should be applied at the point of data generation. Privacy-preserving computing approaches, such as federated learning, should be adopted so that raw data never leaves the hospital and thus there are no leakage issues at the technical level. In the clinical application phase, when the system calls up patient information to support clinical decision making for disease diagnosis, very strict "minimum necessary" access control and real-time audit logs should be applied. When incremental data sets that need to be used for model retraining are called up from the hospital, users should be contacted dynamically to obtain their consent via authorization management mechanisms, and user-friendly methods should be provided for withdrawing consent.

For instance, after the authorization period expires, an intelligent health management application should automatically trigger data-isolation and encrypted archiving procedures, rather than simply deleting information. This not only fulfills statutory requirements, but also reserves the possibility of conducting research under lawful conditions in the future. Through such technical means, we can fundamentally resolve the historical issues related to data compliance for medical AI.

4.3 Accelerating Specialized Legislation and Standards Development

On the theoretical level, it is essential that we not fall back into the habit of treating medical AI as subsumed under the traditional regime of medical device laws. Rather, we should promote the development of a legislative regime that is both innovative and attuned to the technological characteristics of AI. The fundamental goal should be to create a full-chain regulatory model that guides the admission of algorithms, clinical use of AI, continuous auditing throughout its lifecycle, and eventual withdrawal from the market. In turn, this model should offer "exception rules" for liability that arises from highly autonomous systems. Additionally, the interdepartmental standards architecture that the system should create should use mandatory national standards to ensure the bottom line of safety for AI, and industry standards to guide technological development. Only then can the law create stable and predictable regulatory expectations for both industrial development and clinical use.

In practice, future legislation could make three categories of regulatory standards mandatory. First, an algorithm-registration and transparency standard: suppose an AI diagnostic product were to seek approval for sale. In addition to a dossier demonstrating clinical efficacy, the product would need to disclose the logic of its algorithm and approaches to mitigating bias (and these would be subject to technical auditing). Second, we should establish dynamic performance-monitoring and early-warning standards that would require continuous surveillance of consistency of diagnostic use for AI systems already in service. If there were measurable "performance drift" (e.g., a discernable decline in the accuracy of recognizing patients with darker skin tones), an alert would be generated and the system would need to report to regulators. Third, we should establish explicit intervention and withdrawal standards. If an audit revealed that a surgical-planning AI was deviating from the

consensus of experts in more than 3% of cases in which there was clinical risk of bias, regulators would have the authority to suspend relevant functions until corrective action was taken. These would create a feedback loop that is tightly coupled.

4.4 Building a New Collaborative Governance Framework

At the conceptual level, we must rise above the old model in which regulatory authority places almost exclusive trust in government administrative control. Instead, we should build a multi-actor governance system in which government leadership, industry self-discipline, market-based incentives, and societal oversight combine to give rise to an ecosystem of co-governance. The key logic of this design is to clarify responsibilities and promote a maximized information-sharing mechanism that diffuses regulatory pressure among all links in the industrial chain. Through this structural coupling, the system achieves an optimal balance between innovation and risk control at a much lower social cost.

It is not clear what the concrete implementation pathway will look like, but it might proceed through the following layers. At the level of national drug- and device-regulatory authorities, a common AI medical-device supervision platform and basic legal framework should be established. Under this design, industry associations might lead in developing detailed technical-ethical guidelines and industry standards (e.g., member enterprises must carry out algorithmic impact assessments and publish regular transparency reports), or third-party certification institutions might be introduced to issue credibility labels for AI systems that pass external testing, such that medical institutions can use the certification as one of their procurement criteria, thereby forming a market mechanism for selecting the best-performing enterprises. Finally, a quick-response feedback and reporting system for clinicians and patients should be established, such that any suspected AI adverse event can be reported directly to the national regulatory platform for supervision and investigation.

This multidimensional structure-government establishing the rules, industry setting standards, markets selecting the best performers, and society conducting oversight-forms a complete and dynamic governance network that can respond to full-range medical-AI risks.

5. Conclusion

This study offers an integrated examination of diverse legal risks associated with the clinical use of medical artificial intelligence, ranging from product liability and determination of medical injury to security and fragmentation of responsibility among multiple entities. It then reveals the deficiencies of the current legal regime, manifested in liability law, data-compliance law, the legal framework for subject-status of AI entities, and technical regulation. In response to these challenges, an integrated regulatory strategy should be adopted: clarifying responsibility allocation, enhancing full-lifecycle data governance, promoting the establishment of specialized laws and standards, and ultimately establishing a cooperative governance regime. Only through the constructive integration of legal norms and technical development can we simultaneously protect patients' rights and ensure their safety as well as provide a stable and foreseeable regulatory environment for AI medical technologies, allowing medical artificial intelligence to develop in a healthy and orderly way and benefit humanity.

References

[1] Zhang, R. (2025). A study on the risks and regulatory mechanisms for medical institutions applying artificial intelligence technologies under the context of localized DeepSeek deployment. Health Development and Policy

Research, 28(5), 493–500.
[2] Zhu, W., & Yan, Z. (2025). Ethical governance pathways of generative artificial intelligence in the German medical field and their implications. Medicine and Philosophy, 46(19), 27–31.
[3] Han, L., & Yue, Y. (2025). The occurrence logic and legal regulation of algorithmic discrimination in intelligent healthcare. Medicine and Society, 38(9), 47–53.
[4] Wang, Y., Ge, J., & Xu, Q. (2025). Legal liability and ethical challenges of artificial intelligence in medical decision-making: An analysis based on clinical scenarios. Journal of Naval Medical University, 46(8), 977–981.
[5] Bi, D., & Chang, L. (2025). Mechanisms for protecting patients' privacy rights in AI-based medical data analysis. Chinese Medical Ethics, 38(9), 1184–1190.