

医疗领域人工智能伦理问题的法律规制研究

曾妘熙, 杜禹潼, 宋季桐, 贾思元, 杜单骞翮, 陈洪儒

东北林业大学, 黑龙江 哈尔滨 150000

DOI:10.61369/EST.2026010027

摘 要 : 人工智能正以前所未有的深度和广度融入医疗领域, 凭借其智能高效的优势与海量数据处理能力, 广泛应用于医学影像、辅助诊断、药物研发、非现场医疗等多个核心场景, 显著提升了诊疗效率与质量。然而, 技术的深入应用也同步衍生出亟待破解的伦理与法律规制困境, 包括数据隐私与个体权利侵害、算法“黑箱”导致的决策不透明、医疗资源分配公平性挑战以及责任认定模糊等问题。鉴于此, 开展针对性的法律规制研究具有重要现实意义。本文认为, 应通过构建“理念先行—事前预防—事中监管—事后救济”的纵向长效治理链条, 并贯通“数据安全、算法治理、主体责任与监管机制”的横向协同环节, 形成多维度、系统性的法律治理框架。该框架旨在破解算法“黑箱”, 切实保障患者的自主决定权与数据隐私权, 清晰划分各方责任, 并为医疗人工智能产业的健康、有序、可持续发展筑牢法律制度根基。这不仅是解决当前伦理困境的必要举措, 更是推动实现以人为本的智能化普适医疗、保障医疗服务高质量发展的关键制度保障。

关 键 词 : 医疗人工智能; 系统性监管; 责任划分; 多元化救济

Research on Legal Regulation of Ethical Issues in Medical Artificial Intelligence

Zeng Ranxi, Du Yutong, Song Jitong, Jia Siyuan, Du Shanqianhe, Chen Hongru

Northeast Forestry University, Harbin, Heilongjiang 150000

Abstract : Artificial Intelligence is integrating into the healthcare field with unprecedented depth and breadth. Leveraging its intelligent efficiency and massive data processing capabilities, AI is extensively applied in core scenarios such as medical imaging, assisted diagnosis, drug development, and remote healthcare, significantly enhancing diagnostic and therapeutic efficiency and quality. However, the deepening application of this technology has simultaneously given rise to ethical and legal regulatory dilemmas that urgently require resolution. These include issues such as data privacy and infringement of individual rights, decision-making opacity due to algorithmic "black boxes," threats to fairness in medical resource allocation, and ambiguity in liability attribution. In light of this, targeted research on legal regulation holds significant practical importance. This paper argues for establishing a longitudinal, long-term governance chain based on the principle of "guiding philosophy—preventive measures—ongoing oversight—post-facto remedies." This should be integrated with horizontal coordination across "data security, algorithmic governance, subject liability, and regulatory mechanisms" to form a multi-dimensional, systematic legal governance framework. This framework aims to deconstruct the algorithmic "black box," effectively safeguard patients' right to self-determination and data privacy, clearly delineate responsibilities among stakeholders, and establish a solid foundation in the legal system for the healthy, orderly, and sustainable development of the medical AI industry. This is not only a necessary measure to address current ethical challenges but also a crucial institutional guarantee for advancing people-centered intelligent universal healthcare and ensuring the high-quality development of medical services.

Keywords : medical artificial intelligence; systemic regulation; liability attribution; diversified remedial mechanisms

一、医疗领域人工智能伦理问题的法律规制现状

当前, 医疗人工智能技术正在全球范围内深度重塑传统的医

疗服务模式。我国在普适医疗等相关政策的强力扶持下, 其技术应用得以快速推进, 已深度融入疾病筛查、治疗方案优化、健康管理等诸多环节。特别是在医学影像处理、辅助诊断、药物研

发、基因分析及非现场医疗等核心领域，人工智能发挥着越来越关键的作用，有效提升了医疗服务的精准度与可及性。但与此同时，技术理性与人文价值的碰撞也衍生出复杂多样的伦理与法律问题，对现有治理体系构成了严峻考验，并对构建一种能够兼顾技术创新与人文伦理的新型法律治理模式提出了迫切要求。

这些问题呈现出多层次、多维度的复杂形态。首先，最为直接与显性的是数据隐私与个体权利保护问题，海量医疗数据的收集、处理与应用使得个人信息面临泄露与滥用的高风险。其次，是医疗资源分配领域的公平性难题，即“医疗数字鸿沟”。人工智能技术的应用成本与可及性差异，可能加剧不同地区、不同社会经济地位群体在获取优质医疗服务上的不平等，使得技术红利带有明显的区域性和阶层性。第三，基因数据等特殊敏感信息的应用，已超越个体范畴，可能引发基于基因特征的社会系统性歧视，动摇社会公平正义的根基。第四，AI 系统固有的“黑箱”特性，即其决策过程缺乏透明度与可解释性，这不仅使得医疗风险难以被有效预测和防控，也冲击了传统的知情同意原则，使患者自主决定权难以落实。最后，在非现场医疗等高度依赖 AI 自主决策的场景中，一旦发生错误，可能对患者的生命健康造成不可逆的损害，严重侵蚀公众信任。

从国际规制经验观察，不同法域侧重点各有不同。欧盟的法律框架更侧重于对患者（权利人）的保护，明确规定了人工智能系统的透明度要求与患者的知情同意权。日本政府则侧重于在医疗人工智能的治疗场景中，确立关于公平与道义的伦理标准与社会责任，并通过流程监管来落实相关要求。美国政府的监管重心则放在医疗 AI 设备的开发与销售环节，核心在于强制要求避免算法中可能存在的种族、性别等偏见。

二、医疗领域人工智能伦理法律规制存在的问题

我国在医疗人工智能的伦理治理上面临着治理工具效能不足与理论共识缺失的双重局限。当前的治理模式在很大程度上依赖于行业自律准则、伦理倡议等软法规范，由于缺乏法律强制力，这些柔性社会规范难以跟上技术的快速迭代步伐，导致治理效能显著滞后于实践发展的迫切需求。具体而言，现存问题主要体现于以下四个方面：

（一）规制体系分散且缺乏适配的统率原则

我国在医疗人工智能领域缺乏高位阶的专门性法律，现有规范多为分散的部门规章或规范性文件，法律层级低且不成体系。更为关键的是，现有伦理立法未能确立一套贯穿技术研发、产品准入、临床应用全流程，且深度契合智慧医疗特征与人工智能技术特性的核心伦理原则体系，无法为具体规则的制定与实践提供稳定的价值指引。在规制覆盖范围上，针对算法的规范几乎整体缺位，既没有建立医疗领域算法专用的市场准入与安全审查规则，也缺乏对算法设计阶段数据偏见的事前监管与事后责任追究机制。现有的信息数据规制体系也较为分散，且内容多围绕互联

网场景与网络安全展开，针对医疗这一高风险特殊场景的数据分类分级、全生命周期管理等精细化规则严重不足。

（二）患者权利保障机制不完善

现行法律规制在患者权利保障方面存在显著短板，集中体现在知情同意权的行使受阻与权利救济渠道的单一失衡。在知情同意方面，一方面，医疗人工智能的安全性、可靠性缺乏公认的精准判断标准，导致医疗机构及医务人员难以为患者提供充分、确定的风险信息，知情权的基础被削弱。另一方面，算法的“黑箱”特性使得其决策逻辑难以被人类完全理解，传统的、由医生向患者进行解释说明的知情同意模式在此场景下难以有效运作，患者基于充分理解的自主决定权面临落空的危险。在权利救济方面，当前的纠纷解决模式仍偏重于行政监管与刑事追责，针对患者个体民事权益受损的救济途径不够畅通、成本高昂，未能根据患者在 AI 医疗关系中处于信息与技术双重弱势的地位，构建起倾斜保护、便捷高效的多元化救济体系。

（三）责任认定制度适配性不足

面对医疗人工智能应用可能引发的损害，我国现行法律体系在责任认定上表现出明显的适配性缺陷。首先，责任框架陈旧，仍然主要依赖传统的产品责任与医疗过失侵权责任两类制度，未能针对医疗 AI 涉及算法设计者、产品生产者、软件运营者、医疗机构及医务人员等多方主体的复杂协作关系，构建起权责清晰、层次分明的专门性责任规则，导致事故发生后责任主体模糊、追责困难。其次，风险分散机制缺失。缺乏针对医疗人工智能的专门责任保险制度，使得巨大的赔偿责任风险集中于相关企业或医疗机构，既可能抑制行业创新活力，也可能在发生严重损害时因责任方偿付能力不足而无法使患者获得充分救济。最后，权益平衡机制缺位。法律未对算法透明度的范围与边界作出明确规定，如何在保护企业商业秘密、激励技术创新与保障公众知情权、监督权之间取得平衡，缺乏制度性安排，使得“算法黑箱”问题在责任认定环节依然是无解难题。

（四）技术标准与监管机制滞后

医疗人工智能技术具有高度专业性与特殊性，对其安全性、有效性的检测与认证需要一套专门的技术标准体系。然而，我国当前的相关标准建设仍较为滞后，尚未形成统一、体系化且与临床风险相匹配的特殊标准，难以为监管提供有力抓手。在数据质量监管方面，规范体系存在多重不足：一是现有的法律法规与技术标准之间衔接不畅，难以形成监管合力；二是对医疗数据未能根据其敏感程度进行精细化的分级分类，保护措施“一刀切”，缺乏梯度化的责任设置；三是在发生数据泄露等事件时，传统的侵权责任认定逻辑难以适应智慧医疗场景下多方主体、多重环节的特点，导致溯源难、定责难。

三、医疗人工智能伦理问题的法律规制路径

为系统应对上述挑战，需构建一个纵横结合的立体化法律规制体系。纵向应遵循“理念先行—事前预防—事中监管—事后救济”的风险全流程治理逻辑；横向则需贯通数据安全、算法治

理、主体责任与监管机制等关键环节，形成多维度、系统性的治理合力。

（一）理念基础：确立三项核心伦理与法律原则

构建规制体系，必须首先确立其价值基石。一是“以人为本”原则，这是整个制度的出发点和最高准则，确保技术发展始终服务于人的健康与尊严，防范技术异化。二是“知情同意”原则，将其作为防范伦理风险的前置性屏障，并通过制度创新解决“黑箱”下的同意难题，保障患者的自主权。三是“风险理性”原则，承认医疗 AI 风险具有复杂性和不确定性，摒弃不切实际的“零风险”管控思路，转而建立以风险概率与损害后果综合评价为基础的动态风险评估与管理体系，并运用比例原则平衡技术创新、产业发展与患者安全保护之间的利益。

（二）构建源头防控的法律制度屏障

建立以相称性为核心的医疗数据分级保护制度。应在立法层面为医疗数据制定法定的分级标准，例如可参照《个人信息保护法》，将其划分为非敏感数据（如匿名化统计信息）、一般敏感数据（如常规病历、检验报告）和核心敏感数据（如基因数据、心理治疗记录等）。依据数据等级配置差异化的保护措施，对核心敏感数据实行“数据主体明确同意+专业伦理委员会审核”的双重授权机制，实现保护强度与数据敏感度、潜在危害的正向匹配。

强化前端监管：建立产品与主体的双重准入规制。应以保障医疗安全为核心，构建“产品准入—主体准入—过程监管”一体化的前端风险防控体系。在产品准入方面，需突破传统医疗器械的静态审批模式，建立以“算法安全性”与“临床有效性”为核心指标的动态准入机制，要求申请者提交算法原理、风险管控方案及大样本临床验证数据，并设立“试错期”进行有限范围的应用监测，合格后方可正式上市，并持续进行“后监测”。在主体准入方面，应提高相关从业人员的资格门槛，将人工智能辅助诊疗的操作能力、风险识别能力及必要的医学伦理沟通能力纳入医护人员考核范围。同时，法律规制的范围应拓宽，将 AI 技术研发方、数据处理方等非传统医疗机构主体纳入监管，要求其具备相应资质，净化市场环境。

（三）编织全流程、多维度的动态监管网络

事中监管的核心在于建立覆盖应用全流程的动态化、立体化监控体系。首先，实施持续性穿透式监管，对数据采集、算法调用、决策输出等关键环节进行跟踪监控。其次，引入外部制衡力量，如设立独立的第三方审计机构或医院内部的伦理审查委员会，对算法决策进行定期评估，并开辟患者反馈与投诉渠道。再次，建立灵敏的应急响应与报告机制，对数据泄露、算法故障等突发事件能做到快速预警与协同处置。最后，监管应以“算法规制”为核心导向。思路是推行“数据赋能的嵌入式规制”，将法律对算法公平、透明、可问责的要求，内化到产品标准与诊疗流程中。具体可采取分阶段策略：在设计之初严格清洗训练数据，

减少偏见；在应用过程中，强制要求对算法的公平性、有效性进行持续审计与验证，并探索在特定情况下对算法逻辑进行有限度的解释说明。

（四）构建多元协同的权利救济与责任追究体系

事后救济体系是保障患者权益、惩戒违法行为、维护行业秩序的最终防线。

构建清晰化、多层次的责任认定框架。基于权责对等原则，首先应将算法设计阶段的安全审查义务、算法偏见规避义务等法定化，使设计者对因固有缺陷导致的损害承担首要责任。其次，建立差异化的归责原则：对于当前技术条件下可预见的风险适用过错推定原则；对于即便履行高度注意义务仍无法预见的、因技术内在不确定性导致的损害，可引入以救济受害者和分散风险为核心的严格责任原则，并同步大力发展医疗人工智能专属责任保险，以平衡创新激励与权益保护。最后，通过立法明确算法需公开的信息范围与程度，对于涉及核心技术机密的部分，可强制引入经过认证的第三方机构进行审计，在保护知识产权与保障公众知情权、监督权之间寻求平衡。

发展“以人为本”的多元化权利救济路径。为改变当前救济途径单一的局面，应构建高效、低成本的多元纠纷解决机制。一是强制要求 AI 医疗服务提供方建立规范、透明的内部投诉处理机制。二是大力推广替代性纠纷解决方式（ADR），例如设立由医学、法学、伦理学及人工智能技术专家共同组成的专业仲裁机构。三是在司法诉讼中，推动设立医疗人工智能纠纷合议庭，聘请技术调查官或专家陪审员，解决因技术复杂性导致的事实认定难题。

完善立体化的违法惩戒体系。应突破以行政处罚为主的传统模式，构建行政、民事、刑事及行业自律措施相结合的多维度惩戒体系。在行政处罚上，除罚款、警告外，应丰富惩戒工具，如对严重违规主体实施市场禁入、吊销资质、强制产品召回等。在民事责任上，可针对恶意侵权或严重过失行为，探索引入惩罚性赔偿制度，大幅提高违法成本。在行业自律层面，推动建立行业“黑名单”制度，并将违规记录与企业的市场信誉、融资、招投标等挂钩，形成“法律惩戒+行业监督+社会信用”的综合约束格局。

四、结语

医疗人工智能算法决策的法律规制，其本质是在技术创新的巨大潜力与个体权利的有力保障之间寻求一种精妙的、动态的平衡。当前，由算法“黑箱”引发的责任主体模糊、归责逻辑混乱等问题，已对传统法律体系构成了现实而紧迫的挑战，亟待从制度层面进行系统性的回应与革新。未来的法律规制必须以明确多元参与主体的责任边界为核心基石，否定算法的“拟制人格”，将责任牢固地锚定在设计者、生产者、部署者与使用者等人类主

体之上。需根据不同应用场景（如辅助诊断、手术机器人、健康管理等）区分适用医疗损害责任、产品责任乃至高度危险责任等规则。同时，必须优化举证责任分配，通过举证责任倒置、表见证明等规则，缓解患者因信息与技术不对称所面临的维权困境。在监管层面，必须强化对算法从设计、训练、验证到临床应用的全生命周期合规监管，并特别注意与《个人信息保护法》《数据

安全法》等法律的衔接，严防医疗敏感数据的泄露与滥用。唯有持续完善配套法规，真正推动“伦理先行、依法治理”的理念贯穿于技术发展的全过程，才能既为“AI+ 医疗”这一革新性趋势筑牢法治屏障，又能确保其在以人为本的轨道上稳健、理性地前行，最终造福于全人类的健康事业。

参考文献

[1] 谢亚可. 普适医疗伦理问题研究 [D]. 湖南师范大学, 2017.

[2] SeyedAlinaghi S, Habibi P, Mehraeen E. Ethical Considerations for AI Use in Healthcare Research. [J]. Healthcare informatics research, 2024, 30(3): 286-289. DOI: 10.4258/HIR.2024.30.3.286.

[3] 吴汉东, 张平, 张晓津. 人工智能对知识产权法律保护的挑战 [J]. 中国法律评论, 2018, (02): 1-24. DOI: CNKI: SUN: FLPL.0.2018-02-003.

[4] 陈欣, 金权. 我国医疗人工智能侵权规制的演进、特征及难点探析 [C]// 上海市法学会. 《上海法学研究》集刊 2023 年第 6 卷 --2023 年世界人工智能大会青年论坛论文集. 上海海事大学法学院, 2023: 224-236. DOI: 10.26914/c.cnkihy.2023.016809.

[5] Zhe H, Rui Z, Gao Y, et al. Editorial: Explainable artificial intelligence for critical healthcare applications [J]. Frontiers in Artificial Intelligence, 2023, 6: 1282800-1282800. DOI: 10.3389/frai.2023.1282800.

[6] 谢丰婴. 医疗人工智能算法的法律规制研究 [D]. 中国政法大学, 2021. DOI: 10.27656/d.cnki.gzgzu.2021.000128.

[7] 郭晓雯, 赵平, 高翠巧. 医疗人工智能发展面临的法律与伦理挑战及对策研究 [J]. 中国肿瘤, 2019, 28(07): 509-512.

[8] 倪楠. 人工智能发展过程中的法律规制问题研究 [J]. 人文杂志, 2018, (04): 122-128. DOI: 10.15895/j.cnki.rwzz.2018.04.015.

[9] 陈翎翔. 人工智能医疗器械大数据清洗的法律规制路径 [J/OL]. 东北大学学报 (社会科学版), 1-9 [2025-09-27]. https://doi.org/10.15936/sj.cnki.1008-3758.2025.05.012.

[10] 张强. 面向隐私保护的医疗信息系统设计与实现 [D]. 北京交通大学, 2012.

[11] 罗芳. 医疗人工智能伦理问题及对策研究 [D]. 华中科技大学, 2020. DOI: 10.27157/d.cnki.ghzku.2020.006418.

[12] 石佳友, 李晶晶. 医疗人工智能治理中的人权保障 [J]. 人权法学, 2024, 3(06): 31-57+155-156. DOI: CNKI: SUN: RQFX.0.2024-06-003.

[13] 王贵松. 风险行政与基本权利的动态保护 [J]. 法商研究, 2022, 39(04): 18-31. DOI: 10.16390/j.cnki.issn1672-0393.2022.04.01.

[14] 王轶岭, 王竹. 医疗人工智能侵权责任法律问题研究 [J]. 云南师范大学学报 (哲学社会科学版) 2020, 52(03): 102-110. DOI: CNKI: SUN: YNSF.0.2020-03-014.

[15] 刘云. 论人工智能的法律人格制度需求与多层应对 [J]. 东方法学, 2021, (01): 61-73. DOI: 10.19404/j.cnki.dffx.20210115.002.

[16] 马长山. 智慧社会背景下的“第四代人权”及其保障 [J]. 中国法学, 2019, (05): 5-24. DOI: 10.14111/j.cnki.zgfx.2019.05.001.

[17] 周翔. 算法规制如何场景化 [J]. 东方法学, 2024, (02): 136-150. DOI: 10.19404/j.cnki.dffx.2024.02.011.

[18] Hutan A. Intelligent robots must uphold human rights. [J]. Nature, 2015, 519(7544): 391. DOI: 10.1038/519391a.