



健康医疗大数据应用的法治风险与规制路径*

杨金铭^{①,2}, 方艳³, 匡亚岚^{1,2}, 张伟^{1,2}, 胡业勋^{④△}

1. 四川大学华西医院 生物医学大数据研究院(成都 610041); 2. 四川大学“医学+信息”中心(成都 610041);

3. 烟台大学 生命科学院线粒体与健康衰老研究中心(烟台 264005);

4. 中共四川省委党校(四川行政学院)法学教研部(成都 610071)

【摘要】 随着健康医疗大数据被提升为“国家重要基础性战略资源”,其在公共健康治理、个体权利保障与资源配置优化中的法治意义日益凸显。世界卫生组织(World Health Organization, WHO)《全球数字健康战略(2020–2027年)》提出,数字健康发展应遵循伦理、安全、公平与可持续原则,将数据治理作为实现全民健康权的重要支撑;我国出台《人工智能科技伦理审查与服务办法(试行)》,将生命健康、公共秩序及算法决策等高风险领域纳入全流程伦理审查,初步构建“法治+伦理”的双重规制框架。然而,技术逻辑与法治价值之间仍存在结构性张力,健康医疗大数据应用中逐渐显现出匿名化失灵、算法歧视、数据利益失衡及伦理失范等多重风险。基于此,本文从场景化视角出发,系统识别核心法治风险,并提出分类分级保护、动态匿名化、算法审计及公共利益返还等规制路径,以期在释放数据价值的同时维护数字时代的生命尊严与公共卫生安全。

【关键词】 健康医疗大数据 法治风险 隐私保护 算法风险 公共卫生

Legal Risks and Regulatory Pathways for the Application of Health and Medical Big Data

YANG Jinming^{①,2}, FANG Yan³, KUANG Yalan^{1,2}, ZHANG Wei^{1,2}, HU Yexun^{④△}. 1. West China Biomedical Big Data Center, West China Hospital, Sichuan University, Chengdu 610041, China; 2. Med-X Center for Informatics, Sichuan University, Chengdu 610041, China; 3. Mitochondrial and Healthy Aging Research Center, College of Life Sciences, Yantai University, Yantai 264005, China; 4. Department of Law Teaching and Research, Party School of the CPC Sichuan Provincial Committee (Sichuan Administration Institute), Chengdu 610071, China

△ Corresponding author, E-mail: 26925480@qq.com

This work was supported by the Sichuan Soft Science Project (No. SCJJ25RKX163).

【Abstract】 As health and medical big data is elevated to a “national key strategic resource,” its legal significance in public health governance, individual rights protection, and resource allocation optimization has become increasingly prominent. The World Health Organization (WHO) *Global Strategy on Digital Health 2020–2027* states that digital health development should adhere to the principles of ethics, security, equity, and sustainability, with data governance serving as critical support for realizing the universal right to health. China has issued the *Measures for Ethical Review and Service of Artificial Intelligence Technology (for Trial Implementation)*, which incorporates high-risk areas such as life and health, public order, and algorithmic decision-making into a full-process ethical review, thereby initially establishing a dual regulatory framework of “rule of law + ethics.” However, a structural tension remains between technological logic and rule-of-law values. In the application of health and medical big data, multiple risks have gradually emerged, including de-anonymization failures, algorithmic discrimination, imbalances in data-related interests, and ethical misconduct. In light of this, from a scenario-based perspective, this paper systematically identifies the core legal risks and proposes regulatory pathways such as classified and graded protection, dynamic anonymization, algorithm auditing, and the return of public interests, aiming to safeguard human dignity and public health security in the digital era while unlocking the value of data.

【Key words】 Health and medical big data Legal risks Privacy protection Algorithmic risks Public health

《“健康中国2030”规划纲要》明确提出推进健康医疗大数据应用,强调加强健康医疗大数据相关法规和标准

体系建设,强化数据安全和患者隐私保护^[1]。国务院办公厅《关于促进和规范健康医疗大数据应用发展的指导意见》和国家卫生健康委《国家健康医疗大数据标准、安全和服务管理办法(试行)》将健康医疗大数据定位为“国家重要基础性战略资源”^[2]。WHO《全球数字健康战略

* 四川省软科学课题(No. SCJJ25RKX163)资助

△ 通信作者, E-mail: 26925480@qq.com

出版日期: 2026-05-20

(2020–2027年)》强调,数字健康发展应以伦理、安全、公平和可持续为基本原则^[3]。我国《人工智能科技伦理审查与服务办法(试行)》则进一步将生命健康、公共秩序、算法决策等高风险领域纳入伦理审查框架^[4]。国务院发布《促进大数据发展行动纲要》,医疗健康服务大数据属于公共服务大数据体系的重要组成部分,涉及公共卫生、医疗服务、医疗保障、药品供应、计划生育和综合管理业务等医疗健康多个领域^[5]。

为规范人工智能科技活动伦理治理、防范技术滥用风险,我国正式施行《人工智能科技伦理审查与服务办法(试行)》,明确将对人类生命健康具有较强影响的人机融合系统、具有社会意识引导能力的算法模型、面向高风险场景的高度自主自动化决策系统等纳入伦理审查与专家复核范围,要求遵循增进人类福祉、尊重生命权利、坚持公平公正、合理控制风险、保护隐私安全、确保可控可信等伦理原则,实行全流程伦理审查、跟踪监管与应急审查机制^[4]。健康医疗大数据兼具技术共性与法治特殊性,其应用正重塑“风险社会”的法治图景:一是传统知情同意原则在海量数据二次利用中面临功能性失灵,隐私保护防线趋于松动^[6–8];二是技术的黑箱化特征使算法决策可能隐匿歧视与偏见,挑战社会公平正义底线^[9–10];三是当健康数据被视为国家战略资源时,其跨国流动与商业化利用已超出私法范畴,牵动数据主权与国家安全^[11–14]。这三重风险相互交织,亟待法治予以系统性回应。

1 健康医疗大数据应用的法治价值

1.1 赋能公共健康治理的价值

健康医疗大数据是公共卫生监测—预警—处置的核心支撑,推动公共卫生推动治理模式由“事后应对”向“事前预测”转型^[6]。在宏观层面,通过对人口健康指标、病原特征及环境因素的动态整合分析,政府能够实现风险区域精准识别与医疗资源科学调配。作为具有显著公共属性的数据资源,其在本质上构成国家履行健康权保障义务的重要工具^[11, 15]。根据《中华人民共和国宪法》及相关法律的精神,国家负有保障公民健康权的国家保护义务,大数据为传染病监测、风险区域划定、医疗资源调度提供精准依据^[7]。WHO在《全球数字健康战略(2020–2027)》中指出,数据驱动的公共卫生治理能够显著提升应急响应效率,是国家履行健康权保障义务的重要技术路径^[3]。依托全人群健康监测、病原特征与环境关联分析,政府可精准划定风险区域、优化资源配置,以最小权利克减实现公共利益最大化,构建数字时代公共卫生安全屏障。

美国国家科学院(National Research Council)在*Science, Medicine, and Animals*中强调,医学研究必须兼顾科研创新与伦理底线,保障受试者及实验对象权益^[16]。我国《人工智能科技伦理审查与服务办法(试行)》的实施,则标志着生命伦理审查框架正逐步向人工智能、医疗大数据等新兴技术领域延伸。如相关研究所指出的,科技伦理审查在跨领域适用时面临功能定位模糊与审查形式化风险,亟需结合健康医疗大数据的具体应用场景进行适配性重塑,以确保伦理审查在数字化转型中持续守护生命权与健康权的底线^[15]。《人工智能科技伦理审查制度的体系化建构》中所指出,科技伦理审查的核心在于明确制度功能定位、实现跨领域治理协同,避免审查形式化与虚置化问题^[11]。源自生命医学领域、以生命伦理为底色的科技伦理审查框架,逐步拓展至人工智能、医疗大数据、智能诊疗系统等新兴技术领域时,亟需对科技伦理审查的功能定位、审查标准与实施机制进行医学场景适配性重塑,推动伦理审查在生命科学、临床医学、人工智能医疗应用等领域形成理念共通、规则衔接、程序协同的一体化治理逻辑,从而在医疗数智化转型中持续坚守对生命权、健康权与人格尊严的底线保障。

1.2 促进个体生命权保障与临床科研创新

生命权作为公民最基本的人格权利,其保障程度高度依赖医学科技与数据治理能力的持续提升。健康医疗大数据打破传统医学研究中的“信息孤岛”,为真实世界研究与精准医疗提供支撑^[8, 17]。有研究表明,医疗大数据与人工智能技术有助于缩短新药研发周期并降低研发成本^[10]。大数据推动法权保障从“群体概括”走向“精准个体”,同时为医疗损害责任认定提供科学证据,实现程序正义与实质救济统一。WHO于2021年发布的*Ethics and Governance of Artificial Intelligence for Health*指出,科研数据利用必须以保护隐私与尊重人格为前提,构建数据主体、机构与研究者之间的权利平衡机制^[18]。这一价值转换在为科研机构 and 医疗企业利用数据进行新药研发、罕见病攻关以及精准医疗推演提供了坚实的正当性基础,本质上是在数字空间内通过知识生产的加速来延长人类生命的长度与质量。

同时,大数据还重塑了医疗损害责任认定的证据结构。在复杂医疗纠纷中,基于海量案例的算法分析可提供更具客观性的诊疗参照,促进程序正义与实质正义的统一。在权利结构层面,健康医疗数据的利用亦推动形成“数据利益共享”机制。在去标识化与合规利用前提下,数据得以进入科研体系,实现个人信息自决权与科学研究自由之间的动态平衡,使个体从被动的数据提供者

转变为医学进步的参与者。

1.3 实现医疗资源分配公平

健康医疗大数据的深度应用,为法治视域下的分配正义提供了一种精准的量化路径,其核心价值在于通过消除信息不对称来矫正医疗资源的结构性失衡^[19-20]。在传统的医疗法律关系中,由于缺乏对疾病分布、就医流向及资源负载的实时掌控,医疗资源的配置往往带有一定的盲目性,城乡、区域及阶层间出现了“健康鸿沟”^[10]。而大数据的价值在于,通过对全国范围内患病率、就诊半径、药品消耗及医保支付数据的动态分析,提升信息透明度与可计算性,有效矫正医疗资源配置中的结构性失衡。WHO在2022年公平与健康报告指出,数据赋能可显著提升基层医疗服务可及性,推动优质资源下沉^[19]。在医保基金监管中,大数据可智能识别骗保、过度诊疗等行为,保障医保基金安全;在分级诊疗与远程医疗中,算法模型将三甲医院诊疗经验向基层延伸,保障公民平等享有优质医疗服务,实现“健康正义”^[12, 20-21]。

这种社会正义价值在医保基金监管与分级诊疗制度中表现得尤为突出。在大数据技术的支撑下,国家能够建立起严密的智能审核体系,有效遏制骗保、套保及过度医疗等侵害公共福利资产的行为。这种监管效能的提升,本质上是捍卫了社会保障权的“公平契约”,确保了医保这一公共池塘资源的合规分配。同时,大数据通过赋能远程医疗与基层诊断辅助系统,打破了实体医疗机构的物理边界,原本沉淀在大型三甲医院的优质诊疗经验通过算法模型向基层输送,这在法律层面回应了公民对于平等享有高质量医疗服务权的需求。因此,健康医疗大数据的社会正义价值不仅在于效率的提高,更在于其通过数据赋能,为构建普惠、均衡且具备包容性的数字法治秩序提供了底层逻辑,确保了“健康中国”的建设成果能够跨越数字鸿沟,公平地惠及每一个社会成员^[20]。

2 健康医疗大数据应用的核心风险

2.1 临床隐私泄露风险:匿名化失灵与重识别

在健康医疗大数据治理体系中,“匿名化”长期被视为平衡数据流动效率与隐私保护的重要技术路径。在数智化环境下,健康医疗数据的高维、稀疏及强关联特征,使得传统匿名化机制面临“重识别”风险^[8, 13, 22]。根据《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)的规定,经过匿名化处理后的信息因无法识别特定自然人且不能复原,不再被视为个人信息,从而豁免了收集与使用的知情同意义务。然而,在数智化环境的实际应用中,健康医疗大数据的“重识别风险”正使得这一

法律隔离墙面临体系性崩塌。健康医疗数据具有高维、稀疏且高度关联的特征,这导致传统法律定义的不可复原在技术层面变得极度脆弱。

首先,“匿名化”定义的法律效力在重识别技术面前陷入崩塌。依据《个人信息保护法》第73条,匿名化需达到“无法识别且不能复原”的绝对标准,但在高维、稀疏的医疗数据面前,攻击者通过辅助信息进行多维碰撞,使得“不可复原性”在技术层面极度脆弱。一旦发生重识别,数据将重新落入敏感个人信息范畴,从而触发更严格的合规义务,形成所谓“规则倒灌”效应。其次,在科学研究与公共卫生场景下,虽存在《个人信息保护法》第13条规定的“法定豁免”事由,但风险在于“目的限制原则”的虚化:一旦采集端以公卫或科研之名获取数据,而在流转端缺乏严格的完整性约束,个体的生物性状与疾病史便可能脱离原始场景,陷入重识威胁。这种从“身份识别”到“特质关联”的风险演变,使得个体的知情自决权在复杂的长链条流转中被实质性剥离,动摇了医疗大数据利用的正当性基础。

这种“匿名化失灵”不仅威胁到个体的人格尊严与生命安全(如因病史泄露导致的就业或保险歧视),更动摇了整个医疗大数据应用的正当性基础。如果法律继续固守单一的、静态的匿名化认定标准,而不转向基于动态风险评估的治理模式,那么所谓的“数据要素市场化”将不可避免地建立在对公民基本权利的超限克减之上。因此,如何在算法重识技术日新月异的背景下,重构法律意义上的“识别性”定义,并从技术治理转向法律责任的归位,已成为健康医疗大数据法治风险治理的首要命题。

根据《个人信息保护法》第73条,匿名化与去标识化具有严格法规差异:匿名化,指无法识别且不可复原,不属于个人信息;去标识化,是指不借助额外信息无法识别,仍属个人信息,受全流程监管。SWEENEY^[22]经典研究发现,仅通过出生日期、性别及邮政编码三项信息,即可识别美国87%以上人口身份。研究表明即便医疗数据经过去标识化处理,攻击者仍可能通过辅助信息进行多维碰撞,从而重新识别特定个体。WHO《Data Privacy Framework for Health Data》特别指出,健康医疗数据的重识别风险远高于普通个人信息,必须实施更高等级的数据保护措施^[13]。在科研、公卫、商业场景中,合法性基础应严格区分:公卫与科研可适用法定豁免,但严禁目的漂移与跨场景滥用;商业利用必须坚持单独同意,禁止以公益名义攫取私益^[6-8]。

2.2 数智技术风险:算法黑箱与数字歧视

当健康医疗大数据从单纯的存储资源转化为驱动临

床决策与公共管理的算法模型时,法治风险也随之从数据安全层面跃升至分配正义层面^[9-10]。OBERMEYER等^[9]研究发现,美国医疗资源分配算法存在明显种族偏差,同等健康状况下,黑人患者获得高风险评估的概率显著低于白人患者。患者算法偏见并非单纯的技术偶发事件,而是社会既有偏见在数字空间的镜像投射与放大,在医疗场景下,这种偏见往往转化为系统性的“数字歧视”,严重侵蚀了法治社会关于平等权与公正原则的底线。

算法偏见的危机首先源于样本偏差导致的结果不公。如果训练医疗人工智能(AI)的数据集主要源于特定经济水平或族裔群体,那么算法在面对边缘群体或少数民族群时,其预测精度将显著下降。例如,若心脏病预测模型主要基于男性数据,则可能在女性患者身上表现出极高的误诊率。这种基于身份特征的差异化对待,在法律上构成了间接歧视。更为严峻的是,这种歧视往往隐匿在“黑箱”式的算法逻辑中,具有极强的隐蔽性与不可追责性。当医院利用算法分配重症监护室(ICU)病床,或保险公司利用大数据预测个体的长期患病风险并据此实行差异化定价时,个体往往无法感知自己正处于不公正的待遇中。算法“黑箱”特征使患者难以理解医疗决策逻辑,进一步压缩患者知情权、申诉权及公平医疗权^[10, 18]。WHO在*Ethics and Governance of Artificial Intelligence for Health*中指出,医疗AI治理必须强调可解释性、公平性与可追责性,以避免形成新的数字等级制度^[18]。

这种数字歧视直接挑战了现代法治的责任归属体系。传统法律体系建立在“过错归责”基础之上,要求受害方证明加害方的恶意或疏忽,然而,在算法驱动的医疗决策中,歧视往往是自动生成的,甚至连算法开发人员也难以解释决策的因果链条。这种决策的不可解释性,导致患者的知情权与申诉权在技术壁垒面前全面溃缩。如果法律不能确立算法的可解释性标准,那么健康医疗大数据的广泛应用极易形成一种新型的数字等级制度。

2.3 数据流转风险:生物安全与公共利益流失

从宏观维度审视,健康医疗大数据因其“国家重要基础性战略资源”的定性,其风险边界已大幅超越了个体私权的范畴,上升至国家主权安全与公共利益分配的高度^[8]。在数据要素的频繁流转与跨境应用中,如何防范核心战略资源的流失与异化,构成了法治风险解析中不可忽视的命题。

健康医疗大数据不仅关涉个体隐私,更涉及国家数字主权、生物安全与公共利益分配问题^[11-14]。WHO在全球健康安全相关报告中强调,健康数据跨境流动必须经过严格安全评估,防范种群遗传信息泄露与滥用^[13]。健

康数据不仅包含个体的临床记录,更涵盖了大规模的种群遗传信息、基因序列及生物族群的分布特征。在数据要素市场化背景下,若缺乏收益返还机制,则容易导致“公共资源私有化”,形成公众承担隐私风险、资本独占数据收益的失衡风险^[14, 17]。健康医疗大数据的原始积累主要依赖于公共医疗卫生体系的长期投入,具有显著的公共资源属性。然而,在当前的流转实践中,医疗机构往往作为数据的“守门人”与科技巨头开展商业合作。倘若缺乏完善的收益分配法律规则,这些由全体国民贡献、利用公共资源采集的数据红利,极易被少数资本与技术寡头掌握。

这种利益分配的不对称引发了深层的正义问题:公众承担了数据贡献带来的隐私风险,却未能公平地享受到数据驱动下的低价医疗或普惠福利。这种“公共资源私有化”的倾向,不仅导致了社会公共利益的减损,更可能引发公众对技术应用的不信任,动摇数据治理的合法性基础。因此,健康医疗大数据的流转风险不仅在于安全维度的“被窃取”,更在于分配维度的“被收割”。如何在保障数据流转效率的同时,构建一套确保数据价值公平返还社会的法治路径,已成为维护公共利益正当性的关键挑战。

数据公共资源属性与商业化存在张力:公共投入形成的数据红利易被资本垄断,公众承担隐私风险却无法公平获益,形成“公共资源私有化”。WHO相关治理文件进一步提出,健康数据治理应坚持公共性与普惠性原则,确保数据红利能够公平返还社会^[3, 18]。

3 健康医疗大数据应用法治规制路径

3.1 分类分级保护机制与动态匿名化标准

面对健康医疗大数据“匿名化失灵”的技术现实,法律规制逻辑应从“绝对安全”的虚置目标转向“基于风险的受限流转”。其核心路径是构建以《中华人民共和国数据安全法》(以下简称《数据安全法》)第21条为基石的分类分级机制,并配合动态风险评估标准,实现法益平衡。

第一,建构基于法益冲突强度的分类分级治理体系。一是“核心数据”,包括主权数据与安全数据,针对涉及种群安全的原始基因序列、大规模传染病监控数据,应定性为“国家核心数据”。依据《数据安全法》,此类数据应适用最严苛的物理隔离与出境禁止义务,其法理基础在于“国家安全优先原则”。二是“重要数据”,如公共利益相关的数据,包括区域性电子病历、大规模临床试验数据等,虽匿名化程度较高但仍具重识别潜力。应确立“可用不可见”的法律强制要求,将其处理行为限定在受控的

计算环境中(如隐私计算平台),以满足《个人信息保护法》对敏感个人信息的特殊保护要求。三是“一般数据”,通常也是要素流通数据,对于低敏感的生理指标或经高度聚合的统计数据,应允许其在履行《个人信息保护法》第51条规定的安全保护义务后,依法定程序进入数据要素市场。这种分级模式通过比例原则精准配置监管资源,避免泛安全化导致的资源闲置。

第二,确立从“静态定义”转向“概率评估”的动态匿名化标准。现行《个人信息保护法》第73条对匿名化“不可复原”的界定在重识别技术面前存在解释困境。建议在解释论层面,将匿名化从“结果性结论”转化为“过程性风险阈值”。即不再追求绝对的“零识别”,而是引入“重识别风险阈值”机制。当数据处理者证明其已采取当前技术环境下的主流隐私增强技术(如差分隐私、同态加密),且攻击者的重识别成本远超获益时,应在法理上推定其履行了匿名化义务。此外,法律应明确,数据处理者的合规责任不因初次脱敏而消灭。基于健康数据的高度敏感性,处理者需承担持续性的动态监测义务。一旦发生技术环境剧变导致重识别风险激增,处理者若未履行立即阻断流转的“保证人义务”,则需承担由此引发的侵权责任或行政法律后果。这种从“一次性审批”向“全生命周期监管”的转变,是应对技术不确定性的必然选择。

3.2 重构知情同意原则与引入“场景化规制”

在健康医疗大数据长链条、多节点的流转应用中,传统私法意义上“一事一同意”的规则正面临功能性失灵。数据二次开发具有目的模糊性,机械套用明示同意不仅会产生极高的交易成本,亦会导致公共卫生决策陷入“同意困境”。因此,法律规制应从静态的“形式授权”转向实质的“场景化规制”,重构告知同意的适用位阶。

第一,建构“知情同意”与“法定豁免”的二元授权路径。应基于《个人信息保护法》第13条的体系框架,对健康医疗数据的处理场景进行类型化区分:一是私益处理场景,即明示同意场景,对于临床诊断、商业保险核保等直接涉及个人重大利益的初始采集,应严格执行“告知-单独同意”规则,确保个体的自决权。二是公益处理场景,即法定豁免与概括授权场景,针对流行病监测、公共卫生科研等具有显著正外部性的场景,应激活《个人信息保护法》第13条第3至6项的适用。法律应明确,在已履行去标识化义务且符合“为公共利益实施新闻报道、舆论监督”或“公共卫生行动”等法定情形时,允许以“概括授权”或“选择退出”机制替代逐项明示同意。

第二,引入“场景化规制”框架,强化数据利用端的流向管控。信息的隐私法益取决于其所处的具体脉络。法

律监管的重心应从前端的“权限准入”后移至后端的“用途合规”。一是法律应严禁跨场景的“目的漂移”。例如,在保险核保场景中,应明确禁止保险公司通过科研合作渠道获取个体的基因缺陷数据进行逆向画像。此种行为应定性为“超出合理关联范围的处理”,违反《个人信息保护法》第6条的必要原则。二是引入“数据受托人”概念。在科研、政务等复杂场景中,数据利用方应对主体承担信义义务。这意味着即使获得了初步授权,利用方仍负有“不损害受托人利益”的消极义务与“保障数据安全”的积极义务。三是建议在立法层面强化“禁止歧视”与“算法解释”义务。当数据利用导致个体在就业、医疗、保险等场景中遭受不公正待遇时,应由利用方承担举证责任倒置,证明其数据处理符合该场景的信息分配准则。

3.3 强化算法可解释与建立第三方审计制度

当健康医疗大数据的价值通过算法模型转化为诊疗建议、分诊排序或资源调配决策时,算法决策的“黑箱”特征构成了对患者知情权、自主决定权以及平等医疗权的实质性威胁。为应对这一风险,法治规制应从“前端准入管控”转向“后端算法问责”,确立以透明度义务与审计监督为核心的正当程序机制。

第一,建立基于风险分级的算法可解释性标准。可解释性并非要求公开全部算法源代码,而是要求决策逻辑具备可被非专业人员理解的说明能力。根据医疗场景的风险等级差异,可解释性义务应区分为三个层次:其一,高风险场景(如肿瘤辅助诊断、ICU床位分配、急诊分诊排序),算法提供者须强制披露模型的关键影响因子、决策逻辑摘要以及已知局限性,确保临床医生与患者能够理解决策依据,从而有效行使知情同意与异议申诉权。其二,中风险场景(如慢病随访、健康风险预测),应公开数据来源与训练集特征,并说明模型适用人群与潜在偏差。其三,低风险场景(如健康管理建议、运动处方),仅需提供基本的算法功能说明。这一分级标准可参照《人工智能科技伦理审查与服务办法(试行)》关于高风险算法的界定,并与医疗器械软件监管分类实现制度衔接。

第二,构建独立第三方算法审计制度。医疗AI产品的安全性与公平性不应仅依赖开发者自证合规。建议在法律层面确立由独立第三方机构实施的算法审计制度,审计主体须具备医学、法学、信息科学等多学科背景,并经国家卫生健康主管部门或数据监管机构资质认定。审计内容应涵盖:训练数据的代表性与偏差评估、模型在不同亚群体中的性能差异、对抗性攻击的鲁棒性测试以及隐私保护措施的有效性验证。审计结论应赋予双重法律效力:在行政监管层面,通过审计的产品可获得市场准入

优先审查资格,未通过审计或拒绝接受审计的,监管部门可限制其临床应用范围或要求补充验证;在司法层面,已通过合规审计可作为算法提供者在侵权诉讼中的初步抗辩事由,但若原告能举证存在歧视性后果的初步证据,则实行举证责任倒置,由算法提供者证明其决策未违反平等保护原则。对于故意利用算法实施歧视或隐匿安全缺陷的行为,应引入惩罚性赔偿机制,以强化算法提供者的注意义务。

第三,推动审计结论的公开与可追溯。为保障公众知情权与社会监督,审计报告的核心结论(不含商业秘密部分)应向医疗机构、患者组织及学术研究开放查询,并建立算法安全事件的强制报告与召回制度。通过透明度倒逼算法向善,使技术应用始终处于法治的审视之下^[15]。

3.4 完善收益分配机制与数据资源公共性保障

健康医疗大数据作为“国家重要基础性战略资源”,其红利分配不应陷入资本垄断。法治应对的核心在于依据“数据二十条”确立的产权框架,构建兼顾创新激励与社会公平的收益分配机制,防止“公共资源私有化”。

第一,确立“数据资源持有权”与“经营权”分离下的利益返还机制。医疗机构作为数据的原始采集者,其持有的健康数据具有极强的公共属性与患者贡献背景。法律应界定医疗机构行使的是“数据资源持有权”,而第三方企业通过开发获得的是“数据产品经营权”。在医疗机构与企业开展数据协作时,法律应通过标准合同强制规定“红利返还”义务。这种返还不应仅视为商业谈判,而应定性为对公共投入的法定补偿。具体制度设计可表现为:企业必须向数据源医院提供算法终身免费授权、对相关罕见病药物研发实施价格限制,或按比例提取利润至“数字健康发展基金”。这一机制的法理基础在于共惠原则,即数据利用不能脱离其原始公共投入的合法性来源。

第二,建立公益性利用的“法定许可”与优先准入制度。借鉴知识产权法中的强制许可制度,在公共卫生安全、传染病防控、医保基金精算等特定公共利益场景下,建立健康医疗大数据“法定许可”利用机制。依据《中华人民共和国民法典》关于公共利益限制私权的精神,当战略资源的私有化利用与社会生存权保障冲突时,法律应赋予政府及非营利科研机构对核心数据集的“优先低成本准入权”。此时,数据持有者不得以商业秘密为由拒绝提供,但可依法获得合理的行政补偿。这确保了公共卫生决策不因技术壁垒而产生“算法寻租”。

第三,强化数据产品准入的“普惠性评估”与社会责任审计。改变单一的后端利润审计,转向前端的市场准入规制。对于完全依赖公共数据集训练的医疗AI产品,

监管部门在核准其价格与医保目录准入时,应引入“公众贡献抵减系数”。若数据利用方未能履行普惠性承诺(如通过算法锁定抬高药价),监管部门应依据《数据安全法》关于保护公共利益的规定,实施信用惩戒或限制其后续获取公共数据的资格。

4 结语

深入解析健康医疗大数据应用中的法治风险,本质上是在数字文明的十字路口,探求如何在赋能公共卫生治理与保护个体人格利益之间、在促进技术创新与防范伦理风险之间,建立起相应的法治风险治理体系。这不仅是为了给大数据应用套上法律的“缰绳”,更是为了在确立规则边界的基础上,释放数据作为战略资源的巨大潜能,确保“健康中国”战略在法治的轨道上实现从数据红利向全民福祉的平稳转换。

健康医疗大数据既是医学进步的重要支撑,也是数字法治体系面临的重要挑战。其核心问题在于技术发展、医学伦理与法律规范之间的动态失衡。当前,隐私泄露、算法歧视及公共利益流失构成最突出的风险类型。应以医学实践为中心,构建分类分级保护、动态匿名化、场景化授权、算法审计与利益返还相结合的综合规制体系,在释放数据价值的同时守住隐私安全、医疗公平与国家生物安全底线,推动健康医疗大数据在法治轨道上实现高质量发展。健康医疗大数据治理的最终目标,并非限制技术发展,而是在数字文明演进过程中重构技术理性与法治价值之间的平衡秩序。

* * *

作者贡献声明 杨金铭负责论文构思、数据审编、正式分析、调查研究、研究方法和初稿写作,方艳负责数据审编、调查研究和研究方法,匡亚岚负责调查研究和研究方法,张伟负责论文构思、监督指导和审读与编辑写作,胡业勋负责论文构思、经费获取、研究方法、监督指导和审读与编辑写作。所有作者已经同意将文章提交给本刊,且对将要发表的版本进行最终定稿,并同意对工作的所有方面负责。

Author Contribution YANG Jinming is responsible for conceptualization, data curation, formal analysis, investigation, methodology, and writing--original draft. FANG Yan is responsible for data curation, investigation, and methodology. KUANG Yalan is responsible for investigation and methodology. ZHANG Wei is responsible for conceptualization, supervision, and writing--review and editing. HU Yexun is responsible for conceptualization, funding acquisition, methodology, supervision, and writing--review and editing. All authors consented to the submission of the article to the Journal. All authors approved the final version to be published and agreed to take responsibility for all aspects of the work.

利益冲突 本文作者张伟是本刊编委会编委。该文在编辑评审过程中所有流程严格按照期刊政策进行,且未经其本人经手处理。除此之外,

所有作者均声明不存在利益冲突。

Declaration of Conflicting Interests ZHANG Wei is a member of the Editorial Board of the journal. All processes involved in the editing and reviewing of this article were carried out in strict compliance with the journal's policies and there was no inappropriate personal involvement by the author. Other than this, all authors declare no competing interests.

参 考 文 献

- [1] 中共中央 国务院. “健康中国2030”规划纲要. (2016-10-25)[2026-04-16]. https://www.gov.cn/zhengce/2016-10/25/content_5124174.htm.
- [2] 国务院办公厅. 国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见. (2016-06-24)[2026-04-16]. https://www.gov.cn/zhengce/content/2016-06/24/content_5085091.htm.
- [3] World Health Organization. Global strategy on digital health 2020-2027. (2025)[2026-04-16]. <https://www.who.int/publications/i/item/9789240116870>.
- [4] 工业和信息化部, 等. 工业和信息化部等十部门关于印发《人工智能科技伦理审查与服务办法(试行)》的通知. (2026-03-20)[2026-04-16]. https://www.miit.gov.cn/jgsj/kjs/wjfb/art/2026/art_2995f16b28504ddcbb604e918eb15759.html.
- [5] 国务院. 国务院关于印发促进大数据发展行动纲要的通知. (2015-09-05)[2026-04-16]. https://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm.
- [6] 汤建华. 健康医疗大数据共享风险及法治因应. *学习与实践*, 2023(8): 54-60. doi: 10.19624/j.cnki.cn42-1005/c.2023.08.002.
TANG J H. Risks and legal responses to healthcare big data sharing. *Stud Pract*, 2023(8): 54-60. doi: 10.19624/j.cnki.cn42-1005/c.2023.08.002.
- [7] 殷明雪. 健康医疗大数据建设与隐私保护之冲突与协调. *医学与社会*, 2023, 36(2): 125-131. doi: 10.13723/j.yxysh.2023.02.023.
YIN M X. Conflict and reconciliation in big data construction and privacy protection in health care. *Med Soc*, 2023, 36(2): 125-131. doi: 10.13723/j.yxysh.2023.02.023.
- [8] PRICE W N 2nd, COHEN I G. Privacy in the age of medical big data. *Nat Med*, 2019, 25(1): 37-43. doi: 10.1038/s41591-018-0272-7.
- [9] OBERMEYER Z, POWERS B, VOGELI C, et al. Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 2019, 366(6464): 447-453. doi: 10.1126/science.aax2342.
- [10] PHAM T. Ethical and legal considerations in healthcare AI: innovation and policy for safe and fair use. *R Soc Open Sci*, 2025, 12(5): 241873. doi: 10.1098/rsos.241873.
- [11] 满洪杰. 健康医疗大数据治理的健康权面向. *求是学刊*, 2024, 51(2): 103-112. doi: 10.19667/j.cnki.cn23-1070/c.2024.02.010.
MAN H J. The right to health orientation of big data governance in healthcare. *Qiushi xuekan*, 2024, 51(2): 103-112. doi: 10.19667/j.cnki.cn23-1070/c.2024.02.010.
- [12] 姜晓萍, 郭宁. 卫生服务数字化转型政策的价值与工具——基于健康医疗大数据的政策分析. *学海*, 2023(1): 103-113. doi: 10.16091/j.cnki.cn32-1308/c.2023.01.022.
JIANG X P, GUO N. The value and tools of digital transformation policy in health services: a policy analysis based on health and medical big data. *Acad Bimest*, 2023(1): 103-113. doi: 10.16091/j.cnki.cn32-1308/c.2023.01.022.
- [13] WHO. Data privacy framework for health data: technical note[M]. Geneva: World Health Organization, 2021.
- [14] 屈佳. 健康医疗数据治理体系建构的困境及对策. *医学与社会*, 2023, 36(12): 7-13. doi: 10.13723/j.yxysh.2023.12.002.
QU J. Dilemmas and countermeasures in the construction of health and medical data governance system. *Med Soc*, 2023, 36(12): 7-13. doi: 10.13723/j.yxysh.2023.12.002.
- [15] 王蔚. 人类健康权的实现及其限制. *政法论丛*, 2024(3): 58-72.
WANG W. Realization and limitation of the human right to health. *J Political Sci Law*, 2024(3): 58-72.
- [16] National Research Council. Science, medicine, and animals. Washington, DC: National Academies Press, 2004: 33-45.
- [17] 石旭雯. 医疗大数据利益调整框架的权利构建. *医学与社会*, 2022, 35(1): 50-55. doi: 10.13723/j.yxysh.2022.01.011.
SHI X W. Right construction of benefit adjustment framework in medical big data. *Med Soc*, 2022, 35(1): 50-55. doi: 10.13723/j.yxysh.2022.01.011.
- [18] World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. Geneva: World Health Organization, 2021.
- [19] World Health Organization. Equity within digital health technology within the WHO European Region: a scoping review. (2022)[2026-04-16]. <https://www.who.int/europe/publications/i/item/WHO-EURO-2022-6810-46576-67595>.
- [20] 魏玖长, 洪海鹏, 张康宁, 等. 健康医疗大数据治理赋能大健康产业升级. *中国卫生信息管理杂志*, 2022, 19(2): 189-194.
WEI J C, HONG H O, ZHANG K N, et al. Healthcare big data governance enabling and upgrading the healthcare industry. *Chin J Health Inform Manag*, 2022, 19(2): 189-194.
- [21] 段金宁. “互联网+”医疗环境下的健康医疗大数据应用. *中华医学图书情报杂志*, 2018, 27(6): 49-53.
DUAN J N. Application of healthcare big data in "Internet+" healthcare. *Chin J Med Libr Inf Sci*, 2018, 27(6): 49-53.
- [22] SWEENEY L. Simple demographics often identify people uniquely. Pittsburgh: Carnegie Mellon University, Data Privacy Working Paper 3, 2000.

(2026-02-12收稿, 2026-04-16修回)

编辑 姜 恬



开放获取 本文使用遵循知识共享署名—非商业性使用 4.0国际许可协议(CC BY-NC 4.0), 详细信息请访问

<https://creativecommons.org/licenses/by-nc/4.0/>。

OPEN ACCESS This article is licensed for use under Creative Commons Attribution-NonCommercial 4.0 International license (CC BY-NC 4.0). For more information, visit <https://creativecommons.org/licenses/by-nc/4.0/>.

© 2026 《四川大学学报(医学版)》编辑部

Editorial Office of Journal of Sichuan University (Medical Sciences)