综述 • Review

可穿戴设备医疗数据安全风险识别及治理研究

李梦琪

（杭州师范大学　浙江　杭州　311121）

摘　要　随着智能可穿戴设备向医疗健康领域深度渗透，其采集的生理参数、生物特征等敏感医疗数据呈爆发式增长，数据安全已成为制约行业高质量发展的核心瓶颈。本文基于数据全生命周期理论，结合《数据安全法》《个人信息保护法》等法规要求，先明确医疗数据保护与共享的辩证价值，再系统识别智能可穿戴设备在技术架构、管理机制与法律适配层面的多重风险，重点剖析医疗数据分级分类缺失、知情同意机制僵化等行业痛点，构建“技术防护 - 管理协同 - 法律保障”三维治理体系，提出动态防护、标准统一、授权优化等可落地路径，为平衡医疗数据保护与共享价值提供理论支撑与实践参考。

关键词　可穿戴设备；医疗数据；数据安全；数据保护；数据共享；风险识别；治理路径；数据治理

文章编号　024-2025-3421

Study on Identification of Medical Data Security Risks and Governance Paths for Wearable Devices

Li Mengqi

Abstract　With the in-depth penetration of intelligent wearable devices into the medical and health field, the sensitive medical data collected such as physiological parameters and biometrics has experienced explosive growth, and data security has become a core bottleneck restricting the high-quality development of the industry. Based on the data lifecycle theory and in accordance with the requirements of laws such as the Data Security Law and the Personal Information Protection Law, this paper first clarifies the dialectical value of medical data protection and sharing, then systematically identifies multiple risks of intelligent wearable devices in terms of technical architecture, management mechanisms, and legal adaptation. It focuses on analyzing industry pain points such as the lack of medical data classification and grading, and the rigidity of the informed consent mechanism. Furthermore, a "three-dimensional governance system (technical protection - management coordination - legal guarantee)" is constructed, and practical paths such as dynamic protection, standard unification, and authorization optimization are proposed. This study provides theoretical support and practical references for balancing the value of medical data protection and sharing.

收稿日期：2025-12-01　**录用日期**：2025-12-10

通讯作者：李梦琪；**单位**：杭州师范大学　浙江　杭州

Keywords Wearable devices; Medical data; Data security; Data protection; Data sharing; Risk identification; Governance paths; Data governance

1 引言

智能可穿戴设备作为融合感知、连接与云服务技术的新型移动终端，已从消费电子产品升级为医疗健康服务体系的核心工具，心率监测手环、血糖监测手表等多款产品通过国家二类医疗器械认证，成为健康管理与临床诊断的重要辅助手段。市场数据显示，2024 年前三季度全球腕戴设备市场出货量达 1.4 亿台，中国市场出货 4576 万台，同比增长 20.1%，随着政策推动，医疗数据共享已成为释放数据价值、推动医学科研进步的关键路径。

医疗数据的保护与共享并非对立关系，而是相辅相成的有机整体 [1]。有效的保护为共享筑牢合法性基础，只有建立健全数据安全保障机制，才能消除用户对隐私泄露的顾虑，提升用户参与数据共享的意愿，进而汇聚足够规模、高质量的数据资源；而规范的共享则为保护赋予社会价值，医疗数据的规模化流动能为医学研究、公共卫生治理、健康产业创新提供核心支撑。在医学科研领域，跨机构共享去标识化的可穿戴设备数据，可帮助科研人员快速挖掘疾病致病因子、优化治疗方案，加速个性化药物研发进程，尤其在应对 COVID-19 疫情等公共卫生危机时，实时汇聚的健康监测数据成为疫情传播趋势研判、防控政策制定的关键依据。在健康服务领域，数据共享打破了医疗机构间的信息壁垒，使医生能获取患者长期连续的生理指标变化，为慢性病管理、术后康复跟踪提供精准参考，提升诊疗服务的针对性与有效性。在产业创新领域，合规共享的医疗数据催生了商业保险精准定价、个性化健康管理服务等新业态，推动健康医疗产业向数字化、智能化转型，为经济社会发展注入新动能。

然而，医疗数据兼具电子数据的通用性风险与健康信息的特殊性风险，在采集、传输、存储、使用全流程中，技术局限性与制度缺失导致隐私泄露、算法歧视、合规性不足等问题频发，既威胁用户核心权益，也阻碍数据要素合理流动。因此，在保障数据安全的前提下实现合规共享，构建覆盖全生命周期的治理体系，已成为智能可穿戴设备行业可持续发展的迫切需求。

2 可穿戴设备数据风险识别

2.1 技术层面风险

可穿戴设备在设计阶段多聚焦功能实现与成本控制，安全防护投入不足，导致全生命周期各环节均存在技术隐患。数据采集环节缺乏有效的访问控制与远程管理功能，设备丢失后无法及时删除或加密数据，易造成隐私信息泄露 [3]；部分设备传感器精度不足且缺乏数据校验机制，导致健康数据准确性存疑，可能引发临床决策偏差。数据传输阶段因缺乏统一标准，不同厂商采用差异化传输协议，信息孤岛现象突出，同时低强度加密算法的普遍应用，使得数据在蓝牙、Wi-Fi 传输过程中易被截获破解，第三方中转平台的合规能力不足进一步放大了泄露风险。

数据存储环节存在本地存储明文化、云端存储访问权限管控不严等问题，密钥管理缺乏金融级安全规范，黑客攻击、越权访问等风险居高不下，而设备报废时的数据清除机制不完善，导致二手设备数据残留成为重要安全隐患。

2.2 管理层面风险

行业数据管理缺乏统一规范，数据分类分级标准混乱，多数厂商未区分普通运动数据与基因、慢性病记录等敏感信息的保护差异，均采用同质化安全措施，导致高敏感数据保护不足、普通数据过度防护的资源错配问题。供应链管理存在明显短板，芯片设计、操作系统开发、应用接入等环节缺乏安全协同机制，中小厂商为降低成本采购不合规元器件，使得供应链各节点均可能成为安全突破口。

数据质量管控机制缺失，采集阶段未建立有效的数据有效性校验规则[2]，传输过程中缺乏完整性验证手段，导致错误数据、篡改数据进入应用系统，不仅影响健康服务质量，还可能引发医疗纠纷。跨部门监管协同不足，网信、市场监管、卫生健康等部门职责划分不清晰，缺乏常态化信息共享与联合执法机制，对数据滥用、非法营销等行为的监管存在盲区，而企业自身应急响应能力薄弱，未建立完善的漏洞修复与数据泄露应急预案，导致风险发生后处置滞后。

2.3 法律合规风险

现行法律法规对医疗数据的针对性规范不足，《信息安全技术健康医疗数据安全指南》未明确智能可穿戴设备数据的具体分类范围与保护标准，导致实践中数据分级缺乏依据，高敏感数据未得到差异化保护。知情同意机制存在形式化问题，多数厂商采用 “一揽子协议” 的一次性授权模式，用户在使用前需统一同意所有数据处理条款，缺乏针对不同用途的差异化授权选项，实质上剥夺了用户的自主控制权[4]。

“单独同意” 制度落实困难，由于医疗数据的关联性与复杂性，敏感信息与一般信息的界限难以精准界定，即使能够区分，厂商也未以通俗易懂的方式向用户说明授权后果，导致用户在信息不对称情况下作出非理性决策。跨境数据传输合规性不足，部分企业向境外传输敏感医疗数据未履行安全评估程序，违反《数据出境安全评估办法》相关要求，而数据所有权与使用权界定模糊，用户对自身数据的查询、更正、删除权行使困难，不符合《个人信息保护法》对用户权益保障的核心要求。

3 可穿戴设备数据治理框架构建

3.1 技术防护体系

强化设备全生命周期的技术安全能力，在硬件设计阶段嵌入 SE 安全芯片，采用多因素认证技术优化存取控制，结合生物特征识别与用户行为模式分析，实现安全与便捷的平衡。升级通信协议安全性能，蓝牙采用 5.0 及以上版本并定期更新，Wi-Fi 采用 WPA2 及更高级别加密标准，数据传输全面应用 TLS1.3 协议，敏感数据传输额外叠加 VPN 加密防护。建立分层加密与动态脱敏机制，设备端采用 AES 等高强度算法加密本地数据，云端存储实施 AES-256 加密，针对不同敏感等级数据匹配差异化加密策略，同时引入动态环境感知技术，当设备检测到用户进入隐私敏感区域时，自动终止不必要的数据采集。

构建区块链存证与追溯系统，通过联盟链记录数据采集、传输、使用全流程日志，实现操作行为不可篡改追溯，结合零信任架构实施动态访问控制，基于用户身份与设备安全状态实时调整访问权限，防范单一认证漏洞风险。这些技术措施既保障了数据安全，又为数据在合规范围内的共享提供了技术支撑，确保数据“可用不可见”，在保护用户隐私的同时释放数据价值。

3.2 管理规范体系

推动行业标准化建设，由行业协会牵头制

定统一的数据格式、传输协议与存储安全标准，采用 JSON 或 XML 等通用格式提升数据兼容性，明确数据存储位置、介质要求与访问权限规范，为跨机构、跨行业数据共享扫清技术障碍。建立数据分类分级动态管理机制，结合数据敏感性、泄露影响程度等指标，构建包含普通、内部、秘密、机密四级的分级体系，引入实时风险评估模型，根据用户健康状况、数据用途变化动态调整敏感等级，匹配差异化保护措施，实现保护与共享的精准平衡。完善供应链安全管理，推行安全开发生命周期（SDLC），在芯片选型、系统开发阶段开展威胁建模，与供应商签订安全协议，明确 15 天内高危漏洞修复责任，保障供应链各环节的数据安全 [5]。

强化数据质量管理，在采集环节建立生理数据范围有效性校验规则，传输过程中利用哈希算法进行完整性验证，构建全流程数据质量监控与反馈机制，定期开展数据质量评价并督促整改，为数据共享提供高质量的数据基础。健全跨部门监管协同机制，明确网信、市场监管、卫生健康部门的监管职责，建立联席会议与信息共享制度，开展定期抽查与安全检测，加大对违法违规行为的处罚力度，同时企业需建立完善的应急预案，配置专业应急团队与技术工具，提升漏洞修复与泄露处置效率，为数据共享营造安全有序的市场环境。

3.3 法律保障体系

完善医疗数据专项立法，细化《数据安全法》《个人信息保护法》相关条款，明确智能可穿戴设备医疗数据的界定范围，将基因数据、心理健康信息等列为高度敏感数据，规定最严格的保护标准，同时明确数据共享的边界、条件与程序，为合规共享提供法律依据 [6]。

厘清数据权益归属，立法明确用户对医疗数据享有所有权，设备制造商与服务提供商仅在授权范围内享有使用权，用户有权随时查询、更正、删除自身数据及撤销授权，建立数据使用审计机制，要求数据处理方定期报告使用情况，既保障用户权益，又为数据共享提供清晰的权利基础。优化知情同意机制，推行动态授权模式，要求厂商以清晰通俗的语言、图示化等直观方式，向用户详细说明数据采集目的、用途、风险及共享范围，在设备功能升级、数据用途变更时及时通知用户并重新征求同意，设置便捷的权限管理界面供用户随时调整授权，让用户在充分知情的前提下自主选择是否共享数据。

落实单独同意制度，对高度敏感数据设立独立授权入口，单独告知用户数据存储期限、共享对象及潜在风险，确保用户在充分知情的前提下作出决策。完善跨境数据传输规则，明确医疗数据出境的安全评估要求与脱敏标准，采用隐私计算技术实现 “可用不可见”，防范跨境传输中的数据泄露风险 [7]，同时建立惩罚性赔偿制度，对违反数据安全法规的行为依法实施高额罚款、停业整顿乃至吊销许可等处罚，为跨境数据共享提供合规保障。

4 治理路径实施保障

4.1 资源投入保障

加大安全研发资金投入，企业应按研发总预算的 5%-8% 配置数据安全建设资源，重点采购硬件安全模块、数据防泄漏系统等核心设备，积极申请工业互联网安全专项资助，为数据保护与共享技术创新提供资金支持。

加强专业人才培养，组建涵盖数据安全工程师、隐私保护专员、法律顾问的跨职能团队，定期开展法规培训与攻防演练，提升团队的合规管理与风险处置能力，为数据保护与共享提供人才支撑。

推动产学研协同创新[8]，鼓励企业与高校、科研机构合作，开展隐私计算、区块链追溯等新技术研发，探索适配可穿戴设备场景的安全共享解决方案，降低技术落地成本，加速技术成果转化。

4.2 行业协同保障

成立智能可穿戴设备数据安全联盟，发布行业自律公约，规范数据收集、使用、共享的行为边界，建立第三方合规认证机制，对符合安全标准的企业颁发认证资质，引导行业良性竞争，营造安全共享的行业生态。

构建漏洞共享与快速响应平台，企业、监管部门、科研机构共同参与，及时通报新型安全威胁与漏洞信息，推动厂商快速修复安全隐患，提升行业整体安全防护水平，为数据共享筑牢安全防线[9]。

加强国际交流合作，借鉴欧盟《通用数据保护条例》、美国 HIPAA 法案的先进经验，结合我国国情完善数据安全与共享标准，参与全球医疗数据治理规则制定，提升国际话语权，促进跨境数据合规流动。

4.3 效果评估保障

建立多维度评估指标体系，技术层面重点考核漏洞修复率、加密覆盖率、数据准确性等指标，管理层面关注合规通过率、应急响应时间、供应链安全达标率，法律层面以用户投诉率、处罚次数、授权合规率为核心指标，同时将数据共享规模、共享效率、科研转化成果等纳入评估体系，全面衡量保护与共享的平衡效果。

采用 FAIR 风险影响评估模型进行量化评估，定期开展安全审计与合规检查，动态调整治理措施，确保治理效果持续优化。加强用户信任建设，通过公开数据安全报告、开展用户教育等方式，提升用户对医疗数据保护与共享的认知水平，增强用户参与数据共享的意愿，实现数据安全、用户信任与价值释放的良性循环[10]。

5 结论

可穿戴设备医疗数据安全治理的核心是实现保护与共享的价值平衡，二者相辅相成、不可偏废。有效的数据保护是共享的前提，能消除用户隐私顾虑、夯实合规基础；规范的数据共享是保护的延伸，能释放数据科研价值、推动产业升级，最终实现个体健康权益与社会公共利益的双赢。当前行业面临的技术漏洞、管理失序、合规不足等多重风险，本质上是保护与共享价值失衡的外在表现。

构建“技术 - 管理 - 法律”三维治理体系，通过强化全生命周期技术防护、建立统一行业标准、完善专项法律规范，能够有效化解数据安全风险，为数据合规共享搭建可靠框架。

未来治理需重点关注动态分级保护、智能授权机制等关键领域，推动隐私计算、区块链等新技术的深度应用，深化跨部门、跨行业协同治理，在守住安全底线的前提下充分释放医疗数据的科研价值与社会价值。随着治理体系的不断完善，智能可穿戴设备将为“健康中国 2030”战略提供更安全、高效的数据支撑，推动智慧医疗产业高质量发展，让医疗数据在安全保护中实现价值最大化。

参考文献

[1] 邓瀚卓, 罗涵, 孙永祥。智能可穿戴设备医疗数据安全风险识别及治理路径研究 [J]. 医学与法学, 2025.

[2] 符雨嫣, 何达, 罗雅双, 等。可穿戴医疗设备的卫生技术评估方法学研究 [J]. 中国卫生质量管理, 2024,31 (10):86-90+106.

[3] 王雪, 夏义堃。健康医疗数据利用中数据权益保障的现实困境与完善对策: 以欧盟健康数据空间为例 [J]. 图书与情报, 2024 (2):55-68.

[4] 张汉成。健康医疗数据共享的现实困境与合规因应 [J]. 医学与哲学, 2024,45 (17):52-57.

[5] 满洪杰, 郭露露。可穿戴设备中的个人健康信息保护: 以同意为核心的研究 [J]. 法学论坛, 2023,38 (2):121-131.

[6] 李薇, 赵瑞兴, 王柏鸿。医疗敏感数据隐私安全保护的研究 [J]. 网络安全和信息化, 2024 (10):25-27.

[7] 金涛, 张平。可穿戴智能设备数据安全研究 [J]. 信息技术与标准化, 2024 (9):43-50.

[8] 任颖。医疗数据使用权的理论证成与立法平衡 [J]. 法学评论, 2024,42 (4):150-159.

[9] 王冲。个人信息保护合规审计的理论逻辑与制度构建 [J]. 网络安全与数据治理, 2024,43 (1):65-72+78.

[10] 王俐智。隐私政策 “知情同意困境” 的反思与出路 [J]. 法制与社会发展, 2023,29 (2):210-224.