Open Journal of Legal Science 法学, 2024, 12(6), 3623-3628
Published Online June 2024 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2024.126516

Hans汉斯

医疗大数据安全法治与监管

赵轩莹

新疆财经大学法学院，新疆 乌鲁木齐

收稿日期：2024年3月28日；录用日期：2024年5月7日；发布日期：2024年6月19日

摘　要

当前人工智能与医疗健康深度融合，作为智能医疗根基的医疗数据得到各界广泛关注。一方面，医疗数据所涉甚广，一旦数据系统瘫痪，数据被损害或泄露将会对个人隐私权、基因安全、国家安全等领域产生极大威胁；另一方面，医疗数据具有极大开发潜力，然而当前数据处理与共享监管缺位，开发利用程度低，数据资源极大浪费，因此加快医疗数据安全法治与监管迫在眉睫。本文结合当下医疗大数据应用的实际情况，剖析医疗大数据的现实应用困境，并从法律法规完善、风险意识培育、监管机构建立、共享平台建设等角度提出优化策略，以求实现对医疗大数据安全的法治建设与有力监管，从而畅通医疗数据共享，推动我国医疗卫生事业现代化进程。

关键词

医疗数据，数据安全，数据共享

Medical Big Data Security Rule of Law and Supervision

Xuanying Zhao

Law School, Xinjiang University of Finance and Economics, Urumqi Xinjiang

Received: Mar. 28th, 2024; accepted: May 7th, 2024; published: Jun. 19th, 2024

Abstract

At present, artificial intelligence and medical health are deeply integrated, and medical data, as the foundation of intelligent medical care, has received wide attention from all walks of life. On the one hand, medical data is widely involved. Once the data system breaks down, data damage or disclosure will pose a great threat to personal privacy, genetic security, national security and other fields. On the other hand, medical data has great development potential, but the current data processing and sharing supervision is absent, the development and utilization degree is low, and

文章引用: 赵轩莹. 医疗大数据安全法治与监管[J]. 法学, 2024, 12(6): 3623-3628. DOI: 10.12677/ojls.2024.126516

the data resources are greatly wasted. Therefore, it is urgent to accelerate the rule of law and supervision of medical data security. Based on the current actual situation of medical big data application, this paper analyzes the practical application difficulties of medical big data, and proposes optimization strategies from the perspectives of improving laws and regulations, cultivating risk awareness, establishing regulatory agencies, and building sharing platforms, to realize the rule of law construction and strong supervision of medical big data security, to smooth the sharing of medical data. Promoting the modernization of medical and health undertakings.

Keywords

Medical Data, Data Security, Data Sharing

1. 健康医疗大数据概述

国务院发布的《促进和规范健康医疗大数据应用发展的指导意见》，将“健康医疗大数据”定义为以个体为中心、基于个人健康信息数据的全生命周期管理、综合分析、智能应用等技术，以及促进人类健康、预防疾病、改善医疗、降低医疗成本、推动医疗创新为目标的大数据。《国家健康医疗大数据标准、安全和服务管理办法(试行)》认定“医疗数据安全”为“在医疗数据采集、存储、挖掘、应用、运营、传输等多个环节中的管理安全”[1]。可见，医疗数据安全并非依靠单点系统防护就得以实现，而是应当建立起关于数据全生命周期的动态保护体系。由此，数据安全理念由传统侧重于静态存储安全转向兼顾静态存储安全与动态开放共享安全是实现医疗数据安全的题中应有之义。

2. 医疗大数据现实应用困境

当前健康医疗大数据利用存在，诸如数据防护系统不完善、数据安全意识薄弱、数据保护能力欠缺、数据泄露侵害隐私权、数据共享安全危机等问题。通过对医疗数据现实困境分析研究，才能突破数据利用掣肘状态，实现医疗数据价值最大化。

(一) 相关法律规范尚不完善

目前《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《关于构建数据基础制度更好发挥数据要素作用的意见》《数据出境安全评估办法》等法律法规的出台充分肯定了健康医疗大数据作为国家基础性战略资源的重要作用，为医疗数据安全管理提供理论指导。但从立法角度来看仍有亟待完善之处，主要表现为：其一我国目前尚未出台关于医疗数据保护的专门性法规；其二现有立法侧重于原则性指引，无法实际应对实践活动中的数据问题。

1) 未出台专门性法律法规

当前，世界范围内许多国家通常都出台了就个人健康医疗数据治理与保护的专门性法律法规。如以奥地利《使用电子健康数据时的数据保障措施联邦法》和日本《次世代医疗基础法》为代表的专门性医疗数据立法；以美国的《健康保险携带和责任法案》和荷兰《医疗合同法》为代表，在医事法中对医疗数据予以单独规定。我国目前尚未在医疗数据安全领域进行专门立法，现有涉及医疗数据保护的规定也散见于一些法律、部门规章、地方法规之中。

2) 现有法律规范难以指导具体实践

涉及数据安全的众多法律规范，内容较为概括笼统、实践中缺乏可操作性、难以在概括性规范指引下建立起符合医疗卫生领域特点的数据安全保护制度。以《数据安全法》为例，该法总体侧重于对域外经验的形式性借鉴与制度性应对，但在数据战略谋划层面缺乏可操作性，尚未形成较为明确的数据战略与系统的制度安排[2]。

(二) 医疗数据监管机制尚不健全

当前，我国医疗卫生领域医疗数据监管机制明显缺陷，主要体现在内部监管不力导致数据泄露事件频发，外部监管缺位致使难以系统防范数据泄露事件。

1) 内部监管不力

医疗数据有高额经济价值，由于数据安全意识淡薄，医疗机构等相关从业人员或出于逐利性目的窃取医疗数据进行交易。此外，由于数据处理具有专业性，在构建信息化平台时，医疗机构往往选择与第三方合作或将部分服务外包，实践中，由于信息处理技术存在专业壁垒且医疗机构等相关机构未严格要求第三方资质，致使难以对第三方的数据处理行为加以监管，扩大了数据泄露的风险。

2) 外部监管缺位

《数据安全法》第六条明确规定卫生健康主管部门承担医疗领域的数据监管职责，公安机关、国安机关、网信部门等有关部门依照相关规定，在各自职责范围内承担相应数据安全监管职责。集中表现为，卫健委主要负责监督病历信息的管理和使用；工信部门则负责保障数据信息安全[3]。但在实践中，由于我国医疗数据保护仍处于起步阶段，监管职权存在交叉重叠且无具体实施细则予以指引，导致外部监管权责不明，职权混乱，监管缺位。

(三) 数据静态系统安全维护困难

医疗数据存储系统的静态数据安全很大程度上依赖于网络技术及系统管理的成熟度。现下，医疗系统网络安全能力建设尚不成熟，2018 年《医疗互联网服务敏感数据泄漏风险调查报告》显示，当前我国医疗网络服务系统普遍存在逻辑漏洞、敏感端口开放较多、核心业务资产直接对外暴露等安全问题。2020 年有数据表明，医疗卫生行业首次成为全球黑客网络攻击与侵袭活动的首要攻击目标，其目的主要在于获取客户信息[4]。

疫情期间，我国的卫生医疗系统、疫苗研究机构、科研院所等也频繁遭遇网络入侵攻击。医疗大数据时代，医疗数据的高价值驱动的逐利性目的下，侵权主体更为广泛，侵权途径更为多元，侵权者或通过攻击医疗数据的存储数据库，或通过植入病毒医疗数据共享流程，以窃取或者利诱的方式获得大批量的患者信息，进行利用或倒卖。

(四) 数据开放共享条件尚不成熟

《个人信息保护法》第十三条与第二十八条规定表明，自然人的个人信息利用开发共享具有法律上的正当性，这是开展后续数据处理的前提。然而，当前责任主体数据保护能力不足，去标识化处理技术不成熟，处理后的数据仍有可能再次经过组合分析等流程回溯识别得出个人敏感信息[5]。例如，国务院 2019 年颁布的《中华人民共和国人类遗传资源管理条例》(国令第 717 号)，将生物医学大数据上升至国家战略资源进行管理，规定人类遗传资源信息材料在符合特定目的时可对其开展利用，但文中鲜少涉及规制医疗大数据研究使用行为以及二次挖掘数据时患者隐私保护等方面内容。

3. 维护医疗数据安全的法治因应

医疗数据寻求的法治安全是复合概念，一方面，医疗数据安全既涉及患者个体权益，又涵盖社会公共安全与国家安全。另一方面，医疗数据安全要求在静态系统与动态开放双阶段实现安全状态。

(一) 制定专门性法规与配套实施细则

当前关于数据保护的立法仅为一般性，概括性立法，笔者认为可以考虑在一般性法律的基础上，结合医疗数据特性，制定关于医疗数据治理、共享等方面的专门性法规、规章，完善医疗数据保护实施细则，以指导实践中医疗数据使用和研究行为。

(二) 建立内外部协同监管体制

1) 内部监管

其一，内部系统层面，医疗机构作为数据收集源头，应当严格采取安全措施，将医疗数据安全纳入规划。加大资金投入支持，引进先进的医疗数据管理系统，加强安全防护的硬件配置与软件开发，贯彻事前预防机制，通过数据风险检测、风险评估等手段防范风险，从源头上避免数据泄露。

其二，人员配置层面，可以考虑开设专门的数据管理与安全监督部门。根据《个人信息保护法》第五十八条规定，个人信息处理者应当成立专门的独立机构对组织机构的个人保护状况予以监督，其职责主要在于：一是专业化管理，实时观测数据状态，及时处理异常状态；二是强化内部监管，定期对从业人员开展业务培训，提高从业人员数据安全意识与风险应对能力，合理规制医疗机构内部数据处理者的行为。

其三，在技术层面，可借鉴哈佛大学遗传学教授 George Church 将区块链技术带到了基因组学革命的中心这一做法，应用区块链技术实现医疗数据来源的透明化，保障数据来源可追溯，去向可追踪，实现医疗数据全自动化管理和监管。

2) 外部监管

《数据安全法》明确规定由卫生健康主管部门承担医疗领域的数据监管职责，公安机关、国安机关、国家网信部门则在各自职责范围内承担数据安全监管职责。《管理办法》第六条认定卫生健康行政部门为本行政区域内健康医疗大数据安全和应用管理的监管单位。各级各类医疗卫生机构和相关企事业单位是健康医疗大数据安全和应用管理的责任单位。因此，可以考虑建立起由卫生健康委员会牵头，联合工信部、公安部等部门的数据监管信息处理平台。各级卫生行政部门作为第一责任人，协同工信部门及公安部门等相关部门起到政府主导作用。此外，应当充分认识到医疗数据的技术性、复杂性特征与政府作为行政管理部门存在科技知识储备不足的客观障碍，因此，必须吸纳和借助各级各类医疗卫生机构及相关企事业单位等第三方社会力量，统筹规划，建立起主体多元，职权分立，协调统一，动态监管的医疗数据监管处理系统。

(三) 加快医疗信息库安全建设与责任主体安全培训

一方面，对系统内现有存储数据再次进行加密处理。严格访问资格限制政策建设，明确限定访问群体、访问资格、访问时间、访问级别，另一方面，培育相关主体风险责任意识。健康医疗数据主体涵盖：健康医疗数据产生者(个人、患者)、健康医疗数据控制者(医院、医保机构、政府机构、科研机构等)、健康医疗数据处理者(系统供应商、数据分析公司等)、健康医疗数据使用者。从风险产生的后果看，健康医疗大数据安全风险之间存在连环效应，某一风险的发生极易引发其他风险，由此可能同时侵害不同主体的若干法益，这种连环效应意味着，医疗数据安全各相关主体均需培育风险意识与责任主体意识，一方面，在本环节应当依法有序利用医疗数据，另一方面，也要做好协同配合工作，警惕因本环节工作失误而引发多米诺骨牌效应造成风险外溢。具体到各主体而言如下：

1) 个人健康医疗数据主体

个人作为健康医疗数据安全的第一责任人，维护数据安全首先需要数据提供者充分认识到健康医疗大数据的重要性，提升自身数据安全防范意识，经过充分评估潜在风险后，谨慎上传、共享信息。

2) 健康医疗数据控制者

政府作为健康医疗数据控制者中最具权威的一方，在维护医疗数据健康层面，传统的法律后置模式

在数据安全领域存在失灵与降效现象，因此应当变以追责为核心的法律后置模式为以强化风险防范和法律代码化为核心的法律前置模式[6]，最大程度上防范数据安全事故发生。此外，应当积极发挥主导作用，开展法治宣传工作，积极普法宣传，强化私主体合法上传健康医疗大数据意识，以期减少医疗数据安全事件发生。

医疗机构及第三方组织作为健康医疗数据控制者中掌控数据最多的主体，应当严格参照医学伦理学标准，保证从业人员严格自律，规范其从业行为，预防规避数据风险。牢牢树立隐私信息的信息所有权归患者所有，取得数据必须要经过患者明确授权的观念。在医疗服务中，医方应当明确告知患者收集信息的必要性、为防范数据泄露所采取必要措施等事项。

3) 健康数据处理者

根据威瑞森 2018 年《数据泄露调查报告》(DBIR)显示，全球超 1/4 的数据泄露都由内部人员所致[7]，由此医疗数据处理单位应当注重培育员工的数据安全意识。系统供应商、数据分析公司、诊疗方案供应商等主体的从业人员，对于去标识化后形成的大数据应当视为公共资源，必须严格依照公共授权加以利用，不得随意处置数据。

(四) 建立统一共享平台

纵然当前数据利用与保护存在诸多问题，但同样应当意识到医疗大数据作为社会治理与医疗环境改善的重要工具，具有公共属性与极大经济价值。因此应当在保护个人权益的同时，强化规范医疗数据开放共享，以实现公平与利益的均衡状态。

医疗数据的质量与数据标注的准确性决定了人工智能算法的实效性，数据质量与标注工作事关患者生命安全，数据质量参差不齐，标注工作无统一监管可能导致临床误诊漏诊，可能侵犯患者生命权益。2023 年我国将正式实施首批人工智能医疗器械行业标准，其中重点强调了数据集的质量要求与评价。为实现智能医疗数据动态安全之共享利用安全，应当着重强调把控输入医疗数据质量，严格制定数据收集标准，以核查数据真实性、代表性、可信性。《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》中强调：“支持第三方机构、中介服务组织加强数据采集和质量评估标准制定，推动数据产品标准化，发展数据分析、数据服务等产业”[8]。因此，为保证数据质量推动数据开发共享，应当加强对第三方机构、中介服务组织开展数据采集和质量评估工作的审查，其中特别注意数据标注环节建设，确保实现标注对象与标注主体可追溯性。

具体到共享环节而言，首先，应当考虑建立医疗数据共享中心，为实现跨区域数据共享创造条件。其次，应当完善共享标准。标准化是发挥医疗数据优势，实现跨区域共享的前提。当前医疗数据利用缺乏统一标准，存在“信息孤岛”困境，导致数据利用率低，造成医疗数据浪费。《数据安全法》明确规定了卫生健康主管部门的数据监管职责，因此应当由国家卫健委牵头出台关于医疗数据共享的规章，对于共享标准做出统一规定；地方各级政府及卫生部门根据地方实际情况进行细化落实，推动跨区域医疗数据整合利用。再者，应当规制各主体数据共享行为。发挥共享协议在风险治理中的责任追溯功能。最后，应当严格数据侵权主体法律责任。健康医疗数据牵涉主体甚广，法律关系错综复杂，除继续适用传统民事合同制度关于民事法律主体之间的权利义务关系，还应当考虑到健康医疗数据的特殊性，针对性出台关于数据合同的法规或司法解释，加以引导，以全面规制医疗数据利用与共享行为。

4. 结论

健康医疗大数据是重要的战略资源，有极高应用价值。党中央、国务院高度重视医疗数据产业的安全与发展，强调加快健康医疗数据体系规划与智慧医院建设。然而需要注意，在健康医疗数据快速发展的同时，数据防护系统不完善、数据安全意识薄弱、数据保护能力欠缺、数据泄露侵害隐私权、数据共

享安全危机等问题凸显。通过对医疗数据存在的现实问题理性分析研究，坚持数据安全与产业发展并重，完善医疗数据立法，以法治理念引领医疗大数据维护与共享。具体而言，在数据收集层面，严守知情同意原则，在获取明确授权后收集患者数据；在数据利用与管理阶段，培育相关主体风险责任意识，建立医疗数据安全内外部协同监管体制；在数据共享阶段，严格把控数据集质量建设，考虑建立统一共享平台，加快数据要素流动与资源配置，实现医疗数据价值最大化。医疗数据内容复杂且专业性极强，对该领域的风险法治因应研究需要具备扎实法学功底及实践经验，囿于笔者研究水平制约，本文不能做到面面俱到，研究仍可能存在不足之处，有待日后进一步补足改进。

参考文献

[1] 关于印发国家健康医疗大数据标准、安全和服务管理办法(试行)的通知[EB/OL]. http://www.nhc.gov.cn/guihuaxxs/gongwen12/201809/758ec2f510c74683b9c4ab4ffbe46557.shtml, 2023-12-01.

[2] 陈怡. 健康医疗数据共享与个人信息保护问题研究[J]. 情报杂志, 2023, 42(5): 192-199.

[3] 王叶, 何隽. 医疗数据监管的国外经验与国内对策研究[J]. 医学与法学, 2021, 13(1): 33-36.

[4] 叶涛. 论警务数据安全[J]. 中国人民公安大学学报(社会科学版), 2022, 38(4): 139-147.

[5] 刘恺. 美国病人隐私权法探析——兼论对我国立法的启示[J]. 重庆师范大学学报(哲学社会科学版), 2012(5): 123-128.

[6] 郑智航. 数据安全与数据利用平衡的法治保障[J]. 人民论坛·学术前沿, 2023(6): 79-87.

[7] 安全牛. DBIR: 四分之一的数据泄露都是公司内部人员所致[EB/OL]. https://www.sohu.com/a/228771444_490113, 2023-12-01.

[8] 关于构建数据基础制度更好发挥数据要素作用的意见[EB/OL]. http://m.news.cn/2022-12/19/c_1129220019.htm, 2023-12-01.