• 医学信息技术 •

医联体大数据安全管理体系建设与实施*

周大鸿 黄艺璠 王红迁 缪斯蔚 李 颖

（陆军军医大学第一附属医院医学大数据与人工智能中心 重庆 400038）

〔摘要〕 **目的/意义** 基于医联体大数据构建数据安全管理体系，以达到增强数据防护、减少安全隐患并提高数据安全性的目的。**方法/过程** 通过分析医联体业务场景，在采集、传输、存储、处理、共享、销毁全生命周期建立数据安全策略和应用安全技术，完善数据安全体系建设。**结果/结论** 数据安全管理体系是医联体业务的“安全带”，以清晰的安全制度和标准为大纲，为医院业务合法合规开展提供了有效路径并建立了反馈机制。

〔关键词〕 医联体；数据安全；管理体系；全生命周期；安全审计

〔中图分类号〕 R－058 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673－6036.2024.06.012

Construction and Implementation of the Big Data Security Management System for Medical Alliance

ZHOU Dahong, HUANG Yifan, WANG Hongqian, MIAO Siwei, LI Ying

Center for Medical Big Data and Artificial Intelligence, The First Hospital Affiliated Army Medical University, Chongqing 400038, China

〔**Abstract**〕 **Purpose/Significance** The data security management system is built based on the big data of medical alliance to achieve the purpose of enhancing data protection, reducing security risks and improving data security. **Method/Process** By analyzing the business scenario of medical alliance, data security policies and application security technologies are established in the full life cycle of collection, transmission, storage, processing, sharing and destruction, and the construction of data security system is improved. **Result/Conclusion** The data security management system is a “safety belt” for the business of medical alliance. With a clear security system and standards as the outline, it provides an effective path for the legal and compliant development of hospital business and establishes a feedback mechanism.

〔**Keywords**〕 medical alliance; data security; management system; full life cycle; security audit

1 引言

2020 年 7 月印发的《医疗联合体管理办法（试行）》[1]明确提出医联体应在确保数据安全的前提下加强数据信息资源共享和安全管理。2021 年 6 月通过的《数据安全法》[2]明确提出总体国家数据安全观，确立了数据分类分级管理，建立了数据安全风险评估、监测预警、应急处置、数据安全审查等基本制度，明确了相关主体的数据安全保护义务。陆军军医大学第一附属医院医学大数据与人工智能中心作为陆军军医大学的医学大数据中心，承担 4 家大学附属医院的数据管理和运营工作，在国家相关

〔修回日期〕 2024－02－26

〔作者简介〕 周大鸿，中级工程师，发表论文 1 篇；通信作者：黄艺璠。

〔基金项目〕 国家重点研发计划项目（项目编号：2016YFB1001404）。

政策和法规的要求下，为加强医疗机构业务的纵向合作，开始探索基于医联体的大数据安全体系建设策略和方法，以保障数据在全生命周期采集、传输、存储、处理、共享、销毁各节点的安全。

2 医联体数据安全管理体系建设必要性与挑战

2.1 医联体大数据安全体系建设的必要性

一是数据安全责任体层面，保障医疗数据的安全是医联体的重要责任。医疗数据泄漏或不当使用，会对患者的隐私权和医疗机构的声誉造成极大损害。因此，建立完善的数据安全体系，确保数据的保密性、完整性和可用性，是医联体义不容辞的责任。二是法律和政策层面，国家发布了一系列与数据安全相关的上位概括性法律和法规，但下位相关指南和文件存在一定程度的混乱。要真正落实法律法规的要求，亟需体系化的建设思维来完善数据安全的实施路径。三是信息化建设层面，医联体数据安全体系建设是信息化的必经过程。医联体业务的发展建立在数据互联互通的基础上，存在网络环境不安全、外部攻击高频、数据安全策略差异化等现象，医联体数据的安全性是必须面对的问题。

2.2 医联体大数据安全体系建设的挑战

医联体建设是优化医疗资源、推动分级诊疗的重要举措，应通过数据互联互通打破各机构之间的业务壁垒，建立良性互动的长效机制[3]。陆军军医大学 4 家附属医院先后与重庆市 3 个等级多家医院签约组建医联体，医联体业务开展过程中需要共享多种类型的大量数据，例如患者信息、医疗记录、检验检查结果、用药信息等[4]；又由于各级机构信息化建设的差异性、数据使用规范制度的完善性等因素，存在数据泄漏或不当使用的极大风险[5-6]；随着医联体各机构的数字化转型，数据的应用场景更加广泛和复杂，数据安全策略和管理规范的复杂度更高，给数据的可用性、完整性和安全性带来了新的挑战，也提出了更高的要求。

3 医联体数据安全管理体系建设目标与原则

医联体数据安全管理体系建设的核心目标包括确保医联体数据的安全性和完整性、提高医联体数据的使用效率和共享程度、完善数据安全管理制度和技术手段。建设过程应满足以下原则。一是整体规划、分步实施。医联体数据安全管理体系建设应有清晰、整体的规划，考虑各成员单位的业务需求和实际情况，分步实施并逐步完善。二是统一标准、规范管理。4 家大学附属医院需制定统一的数据安全管理标准和规范，各成员单位按照标准规范执行。三是保障安全、注重效率。在保障数据安全的前提下，注重提高数据的使用效率，确保医联体业务的顺利开展。四是权责明确、协同合作。明确各成员单位在数据安全管理体系中的权责，加强数据安全组织的协同合作，共同维护医联体数据的安全。

4 医联体数据安全管理体系建设的路径和方法

4.1 评估风险

4 家大学附属医院作为医联体的重要成员，数据规模大、业务类型多，导致数据安全的风险评估过程复杂。结合多方面因素对数据安全风险进行定性、定量评估：一是结合数据全生命周期各环节的安全防范点；二是结合数据的使用者和使用场景；三是结合业务的当前发展状况和后续发展计划；四是综合考虑数据的敏感性和重要性、数据的存储和处理方式、数据可能面临的威胁和攻击、数据风险管理的有效性等因素。数据安全风险管理，见表 1。

表 1 数据安全风险管理

序号	风险点	风险描述	L	S	R
1	数据泄漏风险	医疗机构涉及大量敏感数据，包括患者基本信息、健康状况、就诊记录等，这些数据的泄漏可能对患者和医疗机构带来不良影响	5	5	关键风险
2	数据篡改风险	不法分子可能篡改数据，从而造成数据失真，影响医疗质量和安全	4	4	重要风险
3	数据滥用风险	医疗机构内部人员可能超权限、超用途、超时间使用数据，甚至存在非法获取和滥用	4	3	中度风险
4	数据传输风险	数据未按照相关规定传输，存在违规使用传输介质，内、外网交叉传输等问题	4	3	中度风险
5	外部攻击风险	由于医疗行业的特殊性，医疗数据是黑客攻击的重点目标，存在较大的外部攻击风险	3	5	重要风险
6	内部管控风险	医疗机构内部人员权限管理不规范，可能随意访问隐私数据，造成数据泄漏	2	3	低度风险
7	制度不健全	医疗机构的安全管理制度尚需完善，存在数据安全管理和保护方面的漏洞和缺陷	2	4	中度风险
8	安全技术不足	医疗机构缺乏必要的、完善的安全技术措施，如加密、访问控制、监控等，可能导致数据的安全性和完整性受到威胁	3	4	中度风险
9	合规性风险	医疗机构需要遵守一系列法律法规和标准，如《医疗信息安全规范》《个人信息安全规范》等，若违反相关规定，可能会面临法律责任和罚款等风险	1	5	低度风险
10	流量异常风险	医疗机构的数据访问流量异常，通常由流量规模大、流量内容异常引起	2	2	低度风险
11	声誉风险	医疗机构数据的泄漏或滥用等安全事件可能对其声誉造成不良影响，降低患者的满意度和对医疗机构的信任度	2	3	低度风险
12	业务中断风险	医疗机构的业务系统和数据安全受到威胁，可能导致业务中断，给医疗机构带来经济损失和形象损失	2	5	中度风险

注：发生概率 L：5 极高，4 高，3 一般，2 低，1 极低。影响程度 S：5 极大，4 大，3 一般，2 小，1 极小。风险等级 R = L × S：17—25 关键风险，13—16 重要风险，8—12 中度风险，4—7 低度风险，1—3 轻微风险。

4.2 数据安全保障措施

4.2.1 建立数据安全策略 以建设原则为“总开关”，从技术、管理、法律、人员角度出发拟定和细化一系列安全策略[7]。例如网站公开数据需经过机构数据安全委员会审批；文件共享数据需采用加密技术、审计技术，对移动介质传输数据采用加密或访问控制的移动介质[8-9]；对应用程序接口（以下简称接口）接入采用口令、密码或生物技术鉴别身份，加强反攻击策略；对即席查询的数据采用校验技术保证其完整性，采用审计技术形成流量报告，及时监控异常和高频查询并预警；对数据分析平台加强访问和使用权限管理，对数据操作支持留痕和溯源。同时制定一系列数据安全应急响应计划，对不同紧急情况和事件设立应对措施，包括组织协调、通信联络、现场控制、技术方案等方面。

4.2.2 建立数据安全组织架构 建立数据安全管理的组织架构并明确责任和分工，将数据安全分层次落实到人，建立多层次、全方位的数据安全管理组织：成立数据安全委员会决策层，由各机构院（处）领导组成，作为审核数据使用安全的最终负责人；下设数据安全工作办作为管理层，负责制定数据安全策略、政策和标准，管理数据安全风险；设置安全管理员作为执行层，负责实施和执行数据安全计划，包括数据安全管理的培训、安全事件的响应和处置、安全漏洞的修复等；设置数据安全监督员作为监督层，定期评估安全工作并及时发现和纠正数据安全隐患和不规范行为。

4.2.3 建立数据库审计检测方案 根据《网络安全法》相关规定，运用审计检测技术记录数据库、服务器的全部操作日志[10]。严格结合医联体的数据使用场景，细化服务器、数据库的“允许”“禁止”“后台预警”等具体策略。服务器层面：监控文件的拷贝导出；监控文件的恶意批量删除和修改等风险操作；监控服务器异常远程连接、同一 IP 多次登录错误。数据库层面：对药品、处方等敏感表的查

询设置敏感对象告警；对 No Where 条件、No Limit 语句、高风险的 DDL、DML 等 SQL 语句进行风险操作告警；对 SQL 注入、漏洞攻击、非法提权等情况进行非法入侵告警；根据数据库表索引的有无、索引的数量设置阶梯级的 SQL 执行时限。建立数据流向图，完整记录数据在全生命周期各节点的形式和内容、进出库（服务器）时间、使用人和数据链路等信息。建立审计日志灾备机制，定期检查分析日志，定位异常事件并排查解决风险。

4.2.4 *建立数据脱敏方案* 为避免敏感数据信息泄漏问题，分析数据脱敏适用场景并结合数据安全策略制度，采用基于数据元的方法，对数据进行漂白、变形、遮盖等形式的静态、动态脱敏处理[11]。（1）识别安全级别。识别字段的安全级别，判断使用场景和角色权限。（2）设立差异化的脱敏规则。如对敏感的就诊信息、手机号码，用“*”“?”“XX”符号替换或遮蔽；对非必要信息如地址中的县、镇、街道信息截断处理；用生日、年龄替换身份证号等。（3）建立并定期更新脱敏字典。建立原始内容与脱敏后内容的等价替换关系。用术语代码替代诊断、手术、检查报告的详细描述，如用“CA”替换“癌症”，用“ITP”代替“免疫性血小板减少症”等；删除药品的厂商品牌名或使用通用的药名代替，如“盐酸曲美他嗪片”替换为“心可舒”，“思密达”替换为“蒙脱石散”等。（4）敏感数据调用限制。医联体各机构调用患者的处方、医嘱、手术等敏感数据时，以“唯一标识，一次一人”为原则，在患者短信授权后，可通过其身份标识信息查阅。（5）明细数据处理。数据分析场景中，对无需明细数据的情况，仅提供平均数、极值、和值等统计学分析值；对身份证号、年龄等范围化处理，避免数据失真，更防止数据滥用；对需要明细的数据分析，使用随机的唯一标识替换原有身份信息相关标识，确保无法追溯到具体患者。通过以上措施确保数据在各使用场景中满足准确性和可靠性、敏感度可控要求。

4.2.5 *建立数据接口检测方案* 医联体各机构之间数据互通应用场景最多的是接口访问，数据接口检测技术方案和访问控制技术是确保数据安全的重要手段，包括以下具体措施。（1）接口列表。将医联体各机构网络 IP 段纳入接口的访问控制列表，梳理并生成数据接口服务目录，设置各接口的访问令牌权限信息，严格控制数据在访问权限方面的安全[12]。（2）接口监控。运用 HTTP/HTTPS 协议解析技术监控网络流量、记录接口请求次数。（3）接口识别。运用接口内容识别技术，判断接口返回值与请求的一致性，判断接口返回字段与令牌权限的匹配度；运用敏感数据访问检测技术，判断脱敏规则有效性。（4）接口检测。启用接口检测任务，定期模拟接口请求，保证接口健壮性。（5）检测报告。按时间维度生成接口检测报告，内容包括接口请求总次数、IP 及归属地分布地图、低谷平段和高峰时间段的趋势图、平均响应时间、最大响应时间、请求错误代码和详情，实时记录接口升级、故障和异常情况等重要事件并同步短信告警通知科室成员，综合评估接口的负载情况和定位潜在问题，保障接口的内容安全性、敏感可控性和负载健壮性。

4.2.6 *基于医联体应用场景对数据分类并制定自动化分级策略* 数据分类作为数据分级的前置工作，以 GB/T38667—2020《信息技术 大数据 数据分类指南》为指导，提供更加清晰有序的定级条件。由于医联体数据的特征具有多元性，遵循“相互独立，完全穷尽”（mutually exclusive collectively exhaustive，MECE）原则[13]，从数据应用场景维度出发，考虑业务包容性和分类的拓展性，将医联体数据分为跨机构（科室）协同治疗、慢性病管理和监测、疾病预防和转诊、临床路径优化、远程健康教育等类别。数据分级作为数据分类的细化补充，结合相关法律法规，将医联体数据从低到高初始化为公开级、普通级、敏感级、重要级、控制级 5 个安全等级[14-15]。遵从数据分级“就高从严”原则的同时，适当赋予数据流通和共享的自由度，促进数据效能增益。根据数据不同形态、生命周期阶段、时空域下管控要求差异，设置对数据安全等级进行升级或降级的策略规则。例如脱敏后的医疗数据相较于原始数据的形态需要降低安全等级；数据使用或传输过程相较于数据存储保护的安全要求更

高；数据在各机构内部交互的安全性要求比在医联体之间流通宽松；定期评估数据安全风险的结果、数据安全相关法规的新颁或废除都可作为数据安全等级升降的参考指导等。数据分级不是终局性的，要灵活使用数据和管理数据安全，允许在满足一定条件时由职能部门调整等级，运用机器学习或自然语言处理技术自动调整。

4.3 检查和优化

要建立持续稳定的数据安全体系，必须建立数据安全的闭环流程，定期组织数据安全检查、完善数据安全制度和应急计划、组织安全培训活动。根据检查阶段的成果，及时更新和优化数据安全体系，不断适应医联体的变化需求。

5 医联体大数据安全体系建设效果

通过医联体数据安全体系建设，现已将 4 家大学附属医院的 16 378 张数据表，合计 254 亿条数据纳入安全管理体系，整体看来数据安全体系建设的运营效果良好，有效保护了患者就诊信息隐私，保障了数据互联互通的安全性和合法性，为医联体业务的开展扣上了“安全带”。

5.1 数据安全层面

数据汇聚平台作为对医联体其他机构提供数据服务的基础，遵循安全管理体系的总体策略并落地各项措施，汇总和治理 4 家大学附属医院的业务系统的数据。通过接口检测技术统计其他机构调用 4 家大学附属医院数据服务共 21 079 次，合计109 353 条，其中被调用的数据安全管控率总体达 87.54%。对全库各表 303 881 个字段设置访问权限和安全级别，新增 1 167 张数据表备份。通过令牌权限校验有效识别并拦截不符合调用者权限的接口服务 2 714 次，更新脱敏字典、调整脱敏规则 49 批次，统计接口调用频次及其日均高峰时间段，并提高对应接口的并发量。由此，为数据的安全性和可靠性提供支撑，对数据质量的提升发挥反馈作用。

5.2 合法合规层面

通过记录和审计数据库、服务器的操作，各机构能够及时发现和解决潜在的数据安全风险，为数据安全合规性报告提供数据依据，有效避免法律纠纷和经济罚款风险，提高数据安全紧急情况的响应能力。

5.3 医疗业务层面

数据安全管理体系建设有助于更好地使用、管理和分析医疗数据，通过在医生工作站、患者统一视图等应用系统中嵌入数据接口调用服务，保证数据脱敏规则生效前提下，提供安全、有价值的数据服务。各机构的医生和研究人员可更便捷地访问医联体内的患者就医情况、疾病模式、药物疗效等信息；患者也能更便捷地选择就诊机构，查看就诊记录、检验检查报告等；可减少数据泄漏造成的隐私受损事件，提高患者对医院的信任度和满意度。在提高医联体医疗业务开展效率和质量的同时，降低成本，助力解决医疗资源短缺和分布不均衡的问题。

6 结语

医联体数据安全体系以数据安全策略为抓手，在安全组织架构、数据库审计检测、数据脱敏技术、数据接口检测技术体系、数据分级分类等方面部署精细化的安全技术和措施，消除数据外部渗透、内部泄漏的风险，规范数据存储和使用制度，强化医疗健康数据保护，为后续业务的建设和发展奠定基础，数据安全不再是医联体业务发展的壁垒[16]。切实解决公众在不同医疗机构就诊要多次问诊和检查后才能治疗的难题，实现医疗资源的上下贯通，为医疗机构及患者提供更安全、可靠的服务。

《“数据要素 ×”三年行动计划（2024—2026 年）》[17]对医联体数据安全体系的建设提出相关指导要求和关键目标，是推动医疗行业数字化转型和智能化发展的重要方案。陆军军医大学第一附属医

院医学大数据与人工智能中心应依据数据隐私保护政策、数据质量标准政策、安全共享政策等数据要素相关政策进一步确保数据的合规性、安全性和高效性。医联体要落实《关于加强数据资产管理的指导意见》，需要各机构成立专门的数据资产管理团队，建立完整的、高适配性的数据管理框架，遵循“原始数据不出域、数据可用不可见”的数据共享原则，建立数据资产管理考核和激励机制，从而探索和激发数据要素潜能的方式和实践场景，增进高质量的数据要素供给[18]。医联体数据的管理和使用不是一蹴而就的，在医联体业务变化快和数据的复杂度、体量增大的背景下，须持续深入地优化数据安全体系的建设，进而体现医疗数据的作用效能。

作者贡献：周大鸿负责研究设计、相关政策梳理、论文撰写；黄艺璠负责数据分析；王红迁负责论文修订；缪斯蔚负责英文摘要撰写、论文校对；李颖负责现状调研、数据分析。

利益声明：所有作者均声明不存在利益冲突。

参考文献

1 关于印发医疗联合体管理办法（试行）的通知［EB/OL］.［2023 - 07 - 17］. http://www.nhc.gov.cn/xcs/zhengcwj/202007/62e9df95714741fa95f9074828848f05.shtml.

2 谢祎，何波. 中国数据法律制度体系研究［J］. 大数据，2024，10（1）：141 - 156.

3 汉业旭，张柠，姚峥，等. 北京某三甲医院开展医联体建设实践与思考［J］. 中国医院，2023，27（10）：94 - 96.

4 周暖青. 医疗行业数据安全监管体系的建设与实践［J］. 福建电脑，2023，39（9）：45 - 50.

5 涂兴锋，王琼，孙雪. 分级诊疗制度下区域医疗信息共享的现状研究——基于医方视角［J］. 行政事业资产与财务，2021（19）：54 - 55.

6 舒婷，徐帆，李红霞，等. 我国医联体内医疗机构信息化建设现状调研［J］. 中国卫生质量管理，2022，29（12）：1 - 5.

7 于柯实. 探讨大数据时代计算机网络信息安全及防护策略研究［J］. 信息系统工程，2023（9）：130 - 133.

8 诸天逸，李凤华，成林，等. 跨域访问控制技术研究［J］. 网络与信息安全学报，2021，7（1）：20 - 27.

9 王宇. 计算机信息技术数据的安全漏洞及加密技术［J］. 数字技术与应用，2023，41（9）：234 - 236.

10 王俊新，尚明伟，臧达菲. 数据库审计系统在医院管理中的应用［J］. 中华医学图书情报杂志，2019，28（3）：76 - 80.

11 刘荣管，王兆栋，邓兰华，等. 基于数据元的医疗数据脱敏方法研究［J］. 信息技术与信息化，2023（7）：4 - 7.

12 欧卫红，杨永琴. 计算机网络安全中数据加密技术的应用［J］. 科技创新与应用，2021，11（35）：106 - 109.

13 李子龙，谭钦文，郎流胜，等. 基于麦肯锡理论和系统思维技能模型的安全风险分析研究［J］. 工业安全与环保，2023，49（6）：44 - 48.

14 张琼丽，陈翼. 数据分级分类方法及实践研究［J］. 技术与市场，2022，29（8）：150 - 153.

15 张胜发，马玉环，张敬晨，等. 基于数据安全的健康医疗科学数据分级指南研究［J］. 医学信息学杂志，2023，44（8）：19 - 24.

16 刘谦，刘阳. 用信息化手段促进医联体的建设［J］. 中国数字医学，2020，15（1）：118 - 120.

17 “数据要素 ×”三年行动计划（2024—2026 年）.［EB/OL］.［2023 - 12 - 31］. http://www.cac.gov.cn/2024 - 01/05/c_1706119078060945.htm.

18 关于加强数据资产管理的指导意见.［EB/OL］.［2023 - 12 - 31］. https://www.gov.cn/zhengce/zhengceku/202401/content_6925470.htm.