医院数据安全综合防护体系构建与应用*

——张倩倩 彭 远 刘 云 寇建秋 朱振国

【摘 要】 随着信息技术的发展，医院数据量快速增长，数据安全已成为医院管理的关键要素之一。通过结合人工智能、机器学习等技术搭建数据安全管理平台，对数据进行分类分级、风险评估等数据安全治理，以及脱敏、网关应用等数据安全防护，形成了多层次的数据安全综合防护体系。通过应用，有效防范了潜在的安全威胁，保障了敏感数据的安全性和业务的连续性。

【关键词】 安全风险；数据安全；数据安全防护；医院
中图分类号：R197.32；R197.5 文献标识码：B

Construction and Application of a Comprehensive Data Security Protection System in Hospitals/ZHANG Qianqian, PENG Yuan, LIU Yun, et al.//Chinese Health Quality Management, 2025, 32(12): 23－26

Abstract With the development of information technology, the volume of hospital data has grown rapidly, making data security one of the critical elements in hospital management. By integrating technologies such as artificial intelligence and machine learning to establish a data security management platform, comprehensive data security governance measures including data classification and tiering, risk assessment, as well as data security protection strategies such as data desensitization and gateway applications have been implemented, forming a multi－layered integrated data security protection system. Through practical application, this system effectively mitigates potential security threats, ensuring the security of sensitive data and the continuity of business.

Key words Security Risks; Data Security; Data Security Protection; Hospital

First-author's address Jiangsu Provincial Hospital of Chinese Medicine / Affiliated Hospital of Nanjing University of Chinese Medicine, Nanjing, Jiangsu, 210029, China

随着信息技术的快速发展，医院的数据量和数据类型急剧增长，数据安全问题日益凸显[1]。2021年，《中华人民共和国数据安全法》强调了健康医疗数据保护的重要性[2]；2022年，国家卫生健康委联合国家中医药局、国家疾控局颁布的《关于印发医疗卫生机构网络安全管理办法的通知》[3]，要求各医疗卫生机构加强数据全生命周期安全管理，采取数据脱敏、数据加密、链路加密等防控措施防止数据泄漏。医疗数据的机密性直接关系到患者隐私的安全性和医院运营的稳定性。然而，面对复杂多变的网络攻击及内部安全威胁，传统的安全措施难以满足当前安全需求。目前，医疗数据安全领域的研究热点主要聚焦于电子病历数据的隐私保护和数据共享等[4]，而缺乏对医院整体数据安全体系的研究。医院数据安全管理主要存在以下问题：一是数据安全意识不足[5]；二是敏感数据安全防护薄弱[6]；三是缺乏针对医疗领域数据安全体系的方案[7]。因此，亟需构建一个数据安全综合防护体系[8]。江苏省中医院通过信息化赋能，设计并实施了覆盖网络安全、数据安全、应用安全和系统安全等的综合防护体系，旨在提升医院数据整体安全水平。

1 数据安全综合防护体系建设

1.1 搭建数据安全管理平台

结合人工智能、机器学习等新技术，搭建数据安全管理平台。通过集成多种数据安全防护组件，设

DOI：10.13912/j.cnki.chqm.2025.32.12.05
* 基金项目：江苏省中医院院级课题(编号：Y24089)
江苏省中医院/南京中医药大学附属医院 江苏 南京 210029

计各类功能模块，包括数据资产梳理、身份治理、风险评估与治理、可视化等，为安全服务提供基础支撑。平台围绕敏感数据管理、数据风险评估及动态访问控制，对数据进行综合管理，联动人员管控、数据防泄漏、数据加密、数据脱敏、数据水印等多种数据安全工具进行统一运营监测。同时，平台通过运用业务化标签提升可读性，帮助用户简化数据安全状态评估及数据活动管控流程，让数据安全管理从数据安全单点建设转向体系化建设。医院数据安全管理平台架构见图 1。

1.2　建立数据安全运营管理体系

数据安全运营管理体系的建设重点为数据安全管理技术的落地和转换，从识别、防护、感知、运营四个维度进行数据安全防控。针对前期梳理出的数据资产、分类分级及风险评估结果，使用数据加密、脱敏、API 接口应用、防火墙、应急演练等方法实现安全运维管控，形成数据流通监管的安全运营体系。通过建立数据安全运营管理体系，可以支撑数据安全工作的持续进行，以及数据安全事件快速、有效响应[9]。

1.2.1 基础设施建设

基础设施建设是医院数据安全综合防护体系构建的关键环节，旨在构建高效、安全、可靠的网络环境。通过部署网络安全管理与态势感知平台，集成入侵防御系统及关键安全设备，结合大数据、多层次防火墙、虚拟专用网络等技术，使用自动化日志收集并实时分析，平台能够快速识别潜在安全威胁并及时生成警告，通知安全团队进行安全事件应急处理。这一过程中采用了动态加密技术和安全协议，以确保数据在传输过程中的保密性和完整性；配置了严格的访问控制策略，基于角色和权限管理，防止未经授权的访问与操作；建立了完善的日志监控和审计系统，实时监控网络活动，及时发现并响应潜在威胁。此外，平台针对中医诊疗数据和处方数据，采用了专门的加密策略和传输协议。结合安全漏洞扫描和定期渗透测试，持续评估和提升网络防护能力，确保医院数据的持续安全。

1.2.2 建立数据安全管理架构

在信息化赋能下，医院数据安全防护体系的运营需要高效的数据安全管理架构支持，涵盖数据安全治理和数据安全防护两个部分，如图 2 所示。数据安全治理负责全院范围内的数据资产管理、策略管理、风险评估、流转管控、分类分级、生命周期管理、泄露建模分析和溯源管理。数据安全防护负责具体的安全技术实施，包括数据外防、数据监测、数据管控和数据使用四个方面。通过建立上述数据安全管理架构，医院能够系统性地提升数据安全能力，确保数据在采集、传输、存储和使用过程中的安全性和合规性。

图 2　医院数据安全管理架构

1.2.3 数据分类分级

根据《卫生健康行业数据分类分级指南(试行)》要求，数据按照重要程度分为核心数据、重要数据和一般数据。结合该院数据特点，采用 4 级标准进行分级(表 1)，以确保各类数据资产在不同使用场景下得到相应保护，实现数据的全面治理和安全管理。

针对临床数据中心的 2 287 张源业务表、26 247 个字段梳理出核心、重要数据，使用数据集分类分级管理规范，对敏感数据进行分类分

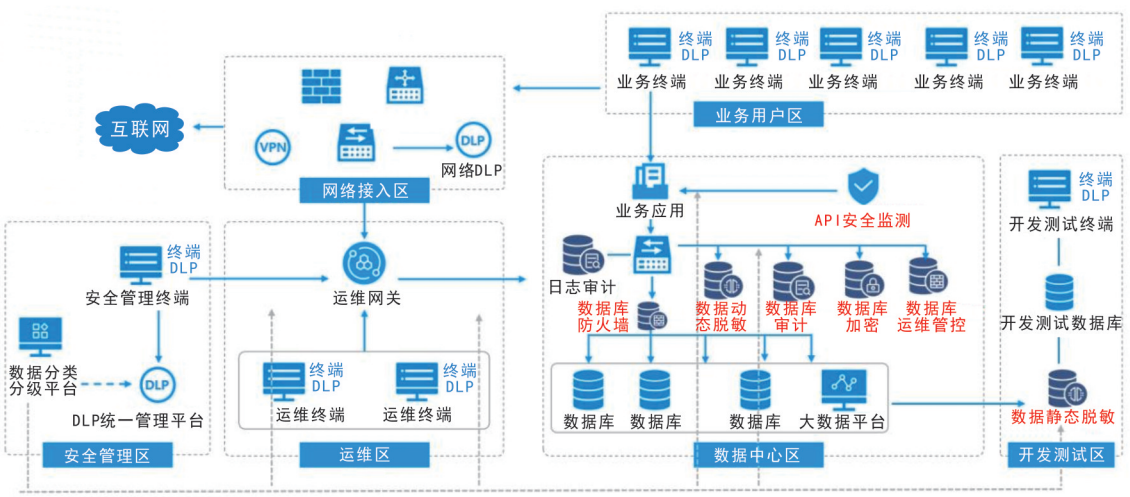

图 1　医院数据安全管理平台架构

表 1　江苏省中医院医疗数据级别划分标准

数据级别	敏感程度	指南标准	定义	示例	管理要求
一级	最低敏感度	一般数据	涉及公开信息或低敏感度数据	公告通知、新闻报道等	常规访问控制，定期备份
二级	一般敏感度	重要数据/一般数据	涉及日常运营数据，敏感度一般	患者流量、服务质量、运营指标等	常规访问控制，定期备份，数据保护
三级	较高敏感度	重要数据	涉及重要业务数据，但敏感度较低	财务报表、员工档案、药品库存等	访问控制，定期备份，数据加密
四级	最高敏感度	核心数据	涉及个人隐私、高度敏感的医疗信息等	患者病历、基因信息、个人隐私数据等	严格访问控制，加密存储，定期审计

级，包括患者基本信息、处方数据等。制定的分类分级策略可以针对性防护及数据监控，提高整体数据安全防护体系质量和稳定性。需注意，对其进行管理时，应严格控制访问，加密存储，定期审计。

1.2.4 数据安全风险评估

《数据安全法》《个人信息保护法》等对数据安全风险评估提出了明确要求，主要涉及评估准备、评估实施、风险分析与评价、编制风险评估报告等[7]。作为数据合规性的重要组成部分，数据安全风险评估不仅能推动标准法规的落地，提升数据安全体系的标准化程度，而且有利于医院及时掌握医疗数据的安全风险，合理制定安全规范，以防止数据安全类事件的发生[10]。

数据风险评估通过围绕 HIS、EMR、CDR、影像中心的数据和数据处理活动，综合运用数据安全风险分析与评价模型，对已识别的数据安全威胁、脆弱性、安全措施给出定性与定量相结合的风险分析与评价结果，并明确风险接受程度以及风险处置措施。结合该院实际，风险评估分为技术措施、管理措施等多个维度，通过调研访谈、工具检测、系统演示等方式，基于数据安全能力现状，分析得出其与数据安全目标之间可量化的差距，并输出风险评估报告。

1.2.5 数据脱敏

医院核心业务系统（如 HIS、LIS、EMR 等）存放了大量患者隐私数据，不同业务系统由不同厂商研发，数据量多且类型复杂。结合数据分类分级结果，对于核心敏感数据（如患者个人信息）需加密存储。如需进行数据传输和使用，应对敏感信息进行脱敏处理[11]。针对科研用途的数据申请，利用敏感数据识别工具，自动扫描、自动化脱敏处理；针对第三方数据接口中的敏感信息，利用静态脱敏系统，自动对数据进行变形、脱敏处理，以提高业务系统间的数据一致性。

此外，还需定期开展数据全生命周期风险评估工作，并动态感知数据安全风险，以数据敏感性为维度进行类别划分，保障数据流转过程的可视化；提供大数据访问可信验证机制[12]，对数据传输及使用进行可信验证、风险分析，尽早阻断数据风险。

1.2.6 API 网关应用管理

API 网关作为服务请求的统一入口，简化了客户端与服务端之间的交互，可以提供集中的身份验证和授权机制，实施速率限制和配额管理，防止过载影响系统稳定。在 API 共享数据时，通过使用数据安全相关插件来确保敏感数据在传输过程中被加密，并记录所有 API 调用日志，以确保操作可追溯。由于移动端与 Web 应用暴露在互联网上容易受到各种网络攻击，API 网关需集成 Web 应用防火墙，阻止 SQL 注入、XSS 等常见攻击，同时实时监控用户行为，检测异常活动，以便及时采取措施。API 网关还支持多因素认证机制，可以进一步提高访问的安全性，防止未授权访问，这不仅确保了数据的安全性和隐私保护，还促进了高效、合规的数据交换。

2　应用成效

本研究数据安全防护体系于 2023 年底投入使用。日常防护过程中，当数据安全管理平台实时检测到异常登录或异常加密等行为时会触发警报，数据安全防护体系随即启动处理程序，封锁被入侵账户，并对受影响的系统进行隔离，由数据库管理员检查数据完整性，确保无数据泄露。日志分析工具随即查找入侵路径，清理系统中的恶意代码，并修复安全漏洞。此外，安全管理团队会定期对数据进行全面评估，分析各环节表现及存在问题，并制订改进措施，优化处置程序，以确保数据在传输、存储和使用过程中的安全性和机密性。

以一次安全事件应急演练为例。该院在演练中使用网络模拟工具模拟钓鱼邮件攻击，黑客通过钓鱼邮件获取医院系统的管理员权限，企图窃取患者数据。数据安全管理平台检测到异常加密行为后，防护系统立即启动应急响应流程。首先，权限控制系统在 30 s 内锁定受影响终端；其次，态势感知平台通过 AI 分析确认了攻击特征；最后，安全团队在 77 s 内完成了应急处置。整个响应过程仅用时 107 s，避免了潜在的数据加密和勒索事件。

通过对 2023 年 1 月至 2024 年 12 月期间系统运行数据的分析，防护措施的具体效果见表 2。从具体指标来看，安全响应方面，通过部署

表2　数据安全防护体系实施前后效果对比分析

评估指标	实施前(2023年)	实施后(2024年)	改善程度
安全事件响应时间	平均15 min	平均2 min	降低86.7%
系统可用性	95.2%	99.8%	提升4.6%
安全事件处置时间	48 h	6 h	降低87.5%
数据备份恢复成功率	96%	99.9%	提升3.9%
异常行为检测准确率	85%	98%	提升13%
合规性审计通过率	92%	100%	提升8%

新一代防火墙和安全管理平台，安全事件响应时间从平均15 min降低至2 min，应急处置效率提升明显。数据安全方面，通过采用混合加密方案和数据脱敏，敏感数据一律经过脱敏或者漂白后进行传输使用，避免了隐私信息泄露。

3　讨论

近年来，国家层面陆续出台了《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规以规范数据安全，特别是对卫生机构的数据安全提出了合规性要求[13]。然而有研究[14]显示，已开展数据安全建设的医院仅占32.64%，说明医院在数据安全建设方面还存在不足。传统的数据安全防护模式往往聚焦于单点防御，数据安全防护体系仍处于碎片化状态，缺乏完整的实践参考[15-16]。本研究通过构建一套集基础设施建设、管理体系、分类分级、风险评估和API网关应用于一体的医院数据安全综合防护体系，确保了数据的真实性、安全性和完整性，可为医疗行业数据安全保护以及数据安全防护体系行业标准构建提供参考。

医院数据安全防护是一个复杂且重要的任务，尽管本研究在数据安全体系建设方面取得了一定成效，但仍存在一定的局限性：一是数据源的复杂性和多样性。近年来，医院外部的数据应用和合作增多，会导致数据安全管理措施难以及时覆盖所有潜在数据风险场景[17]。二是数据安全应用场景急需落地，数据分类分级结果需更有效地和数据应用相结合[18]。三是人工智能、区块链等新技术的快速发展，应与医疗数据的高度敏感和高价值相结合，平衡数据安全与隐私保护，确保在提升数据价值的同时保障数据安全。未来，将进一步探讨基于人工智能和机器学习的安全防护技术，以提升威胁检测和响应的智能化水平。

参考文献

[1]　王　恒，赵　禹. 智慧医院数据安全管理的基础建设与应对策略探讨[J]. 中国医院管理，2024，44(12)：96－98.

[2]　全国人民代表大会常务委员会. 中华人民共和国数据安全法[EB/OL]. (2021－06－10)[2024－11－15]. https://flk.npc.gov.cn/detail2.html?ZmY4MDgxODE3OWY1ZTA4MDAxNzlmODg1YzdlNzAzOTI.

[3]　国家卫生健康委，国家中医药局，国家疾控局. 关于印发医疗卫生机构网络安全管理办法的通知[EB/OL]. (2022－08－29)[2024－11－15]. http://www.nhc.gov.cn/guihuaxxs/s10743/202208/50e2ef41b7554ae894053bcac32b79f0.shtml.

[4]　郭鑫鑫，任　皓，刘敏超. 基于CiteSpace的医疗数据安全领域研究热点分析[J]. 中国病案，2023，24(7)：42－45.

[5]　郑　攀，刘　华，琚文胜，等. 我国医院数据安全现状调查分析[J]. 医学信息学杂志，2024，45(5)：71－75.

[6]　胡　斌. 大数据时代下医院信息管理系统的安全体系研究[J]. 信息与电脑(理论版)，2024，36(15)：115－117.

[7]　王天罡，李晓亮，卫　荣，等. 医院数据安全综合防护体系建设十年实践[J]. 中国数字医学，2022，17(8)：1－8.

[8]　罗　松，熊　冰. 智慧医院建设促进公立中医医院高质量发展的实践[J]. 中医药管理杂志，2023，31(19)：175－177.

[9]　贾玉来. 医疗健康数据安全运营能力建设与实践[J]. 大数据时代，2024(11)：23－27.

[10]　曾令平，刘　宇，路正鹏，等. 数据安全风险评估方法研究与实践探索[J]. 金融科技时代，2023，31(4)：11－16.

[11]　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.

[12]　王凤英，张　方，张　伟. 基于医疗健康大数据的安全起源模型与可信性验证算法[J]. 山东理工大学学报(自然科学版)，2017，31(6)：6－11.

[13]　杨　正，李　鹏，周　睿，等. 利用医疗卫生数据分类分级的研究推进数据要素探索[J]. 中国数字医学，2025，20(4)：28－34.

[14]　郑　攀，刘　华，琚文胜，等. 我国医院数据安全现状调查分析[J]. 医学信息学杂志，2024，45(5)：71－75.

[15]　吴震天，夏逸舜，莫远明，等. 医院数据资产安全治理体系的建设研究[J]. 中国数字医学，2025，20(4)：21－28.

[16]　迟吉凤. 基于数据全生命周期的安全防护体系探究[J]. 网络安全和信息化，2025(4)：13－14.

[17]　巫朝霞，唐靖蕾，苗志伟. 云环境下支持多授权机构的医疗数据安全共享方案[J]. 计算机应用研究，2023，40(12)：3800－3804.

[18]　陈继何. 医院大数据中心建设及应用[J]. 数字通信世界，2023(12)：123－125，128.

通信作者：
朱振国：江苏省中医院/南京中医药大学附属医院信息数据中心高级工程师
E－mail：182901222@qq.com

收稿日期：2024－12－19
修回日期：2025－05－20
本文编辑：黄海凤、刘斯妤