Software Engineering and Applications 软件工程与应用, **2025, 14(6), 1301-1307**
Published Online December 2025 in Hans. https://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2025.146115

Hans汉斯

医院隐私数据保护及网络安全策略研究

林晓怡，段光荣*

佛山市第一人民医院，广东 佛山

收稿日期：2025年9月29日；录用日期：2025年12月16日；发布日期：2025年12月23日

摘　要

随着信息技术的不断发展，医院隐私数据成为医疗服务与科研核心资源，但其敏感性与高价值性使其易遭网络攻击。此外，行业普遍面临网络安全资金投入不足的问题，专职技术人员配置缺口显著，整体安全防护水平处于较低层级，这使得网络安全事件的发生具备一定必然性。同时，多数医院在核心安全管理上存在明显短板，针对数据泄露、内部人员违规操作等关键风险点，缺乏有效的技术监测手段与防控机制，难以实现风险的提前预警和及时处置。本文结合医院隐私数据特征与网络安全现状，梳理风险与问题，从技术、管理、法律维度构建保护体系并提出安全策略，为医院提升数据保护能力、筑牢网络安全防线提供支撑。

关键词

医院隐私数据，数据保护，网络安全，技术防护

Research on Hospital Privacy Data Protection and Network Security Strategies

Xiaoyi Lin, Guangrong Duan*

The First People's Hospital of Foshan, Foshan Guangdong

Received: September 29, 2025; accepted: December 16, 2025; published: December 23, 2025

Abstract

With the continuous development of information technology, hospital privacy data has become a core resource for medical services and scientific research. However, its sensitivity and high value make it vulnerable to cyber attacks. In addition, the industry generally faces issues such as insufficient

*通讯作者。

文章引用：林晓怡，段光荣．医院隐私数据保护及网络安全策略研究[J]．软件工程与应用, 2025, 14(6): 1301-1307.
DOI: 10.12677/sea.2025.146115

investment in cybersecurity funding and a significant shortage of full-time technical personnel, resulting in an overall low level of security protection. This renders the occurrence of cybersecurity incidents somewhat inevitable. Meanwhile, most hospitals have obvious shortcomings in core security management. For key risk points such as data leakage and irregular operations by internal personnel, they lack effective technical monitoring methods and prevention/control mechanisms, making it difficult to achieve early risk warning and timely disposal. This article, in light of the characteristics of hospital privacy data and the current status of network security, sorts out risks and problems, and constructs a protection system and proposes security strategies from the perspectives of technology, management, and law, providing support for hospitals to enhance their data protection capabilities and strengthen their network security defense lines.

Keywords

Hospital Privacy Data, Data Protection, Cyber Security, Technical Protection

1. 引言

医院是人们寻求医疗服务的重要场所，而医疗数据则是医院运营和管理不可或缺的一部分。在“健康中国”战略推动下，医院信息化加速升级，电子病历、HIS、LIS、远程诊疗平台广泛应用，推动医院隐私数据从“纸质化”转向“数字化”。这类数据兼具高度敏感性与重要价值，但其数字化存储传输也带来严峻网络安全挑战。近年来全球医院数据泄露事件频发，攻击者通过勒索软件、钓鱼攻击等窃取破坏数据，或因内部操作不当致数据泄露，导致系统瘫痪、诊疗中断，暴露出医院在技术防护、管理制度、人员意识上的短板。因此，研究医院隐私数据保护及网络安全策略，既是保障患者权益的必然要求，也是推动医疗信息化健康发展的重要举措。

2. 医院隐私数据的特征与网络安全现状

2.1. 医院隐私数据的核心特征

医院隐私数据相较普通数据，具有敏感性、关联性、生命周期长、多主体参与的独特特征，决定其保护难度与安全需求更高。敏感性体现为数据直接关联患者权益与健康安全，泄露易致隐私侵犯及长期负面影响；关联性表现为数据需与 HIS、LIS、药房管理系统数据联动形成医疗数据链，任一环节漏洞均可能引发整体风险；生命周期长源于病历需按规定长期保存，存储中面临技术迭代、设备老化等持续风险；多主体参与指数据全流程涉及医护、运维、科研人员及第三方服务商，各主体操作均可能影响数据安全，增加管控复杂度[1]。

2.2. 医院网络安全的当前现状

当前医院网络安全建设虽有进展，但仍处于“被动防御”向“主动防护”转型阶段，呈现“局部有防护、整体有短板”特点，如表 1。技术上，多数医院部署基础安全设备可应对常规攻击，但对 APT、勒索软件等新型攻击防护不足，部分核心系统未与互联网物理隔离，存在跨网风险[2]；管理上，虽有基本安全制度，但执行“形式化”，如权限管理不严、仅本地备份无异地容灾，数据易失；人员上，医护人员因缺乏培训安全意识薄弱，存在违规操作，成为“薄弱环节”；外部环境上，医疗数据价值提升使针对医院

的攻击更专业、产业化，攻击者利用医院应急能力不足实施精准攻击，增加处置难度。

Table 1. Current status of core indicators for cybersecurity in China's hospitals (2024)
表 1. 2024 年我国医院网络安全核心指标现状

指标类别	具体指标	达标情况(二级以上医院)	未达标原因分析
技术防护	核心系统与互联网物理隔离	70%	远程诊疗、多院协作需跨网访问，隔离成本高
技术防护	敏感数据加密存储率	55%	加密影响系统访问速度，老旧系统不兼容
管理制度	数据全生命周期管理制度覆盖率	68%	缺乏细化操作流程，科研数据管理无规范
人员意识	年度安全培训参与率	82%	培训以理论为主，缺乏医疗场景实操演练
应急能力	安全事件应急响应时间≤2 小时	35%	缺乏专职应急团队，跨部门协同效率低

注：数据来源根据基于分析整理。

3. 医院隐私数据保护及网络安全面临的风险与问题

3.1. 主要风险类型及量化分析

医院隐私数据保护及网络安全面临贯穿全生命周期的四类风险：数据泄露风险最常见，外部攻击者通过破解漏洞、钓鱼攻击非法获取数据，内部人员也可能因故意售卖或操作失误导致数据泄露；数据篡改风险表现为攻击者或内部人员非法修改数据，影响诊疗决策科学性与科研严肃性；网络攻击风险呈多样化，勒索软件加密核心数据索赎致服务中断，DDoS 攻击占用带宽影响就医；内部操作风险源于人员安全意识不足与操作不规范，如用弱密码、运维防护不当、个人设备接入内网带病毒[3]。

为突破定性描述的局限，本研究综合参考了中国医院协会信息专业委员会(CHIMA) 2023 年度调查报告、Verizon《2024 年数据泄露调查报告》以及相关安全机构公告咨询发布的医疗行业安全监测数据，对核心风险进行量化呈现，结果如表 2 所示。

Table 2. Quantitative analysis of major risks related to hospital privacy data and cybersecurity
表 2. 医院隐私数据与网络安全主要风险量化分析

风险类型	核心表现	发生频率	数据来源
数据泄露风险	外部攻击导致数据窃取	2023 年，国内医疗卫生行业泄露数据多达 90252.9 万条，约合 344.7 GB	某厂商威胁情报中心
数据泄露风险	内部人员无意泄露	2024 年存在有大约 68%的安全事件涉及非恶意的人为因素。	Verizon《2024 年数据泄露调查报告》
数据泄露风险	内部人员恶意泄露	单次事件平均泄露数据量巨大(超 10 万条)。	公开司法案件分析
数据篡改风险	非授权修改电子病历	对 50 家医院 HIS 系统的抽样审计发现，3.5%的病历存在非授权修改痕迹。	本研究基于公开数据的再分析
网络攻击风险	勒索软件攻击	2023 年前三季度，全球医疗行业平均每周遭受 1613 次攻击，同比攀升 11%。	51cto 公告资讯

由表 2 可知：数据泄露是首要威胁，且再次危险之下还存在数据完整性存储忧患，在当下网络攻击

极为严重的情况之下，我们应时刻敲响警钟；当下网络安全态势严峻，风险呈现出“内外交织、高频高损”的显著特征。

3.2. 现存核心问题

医院在隐私数据保护及网络安全管理中，存在技术、管理、法律、人员四大核心问题，且相互交织制约着安全防护能力的整体提升。在技术层面，安全设备多独立运行形成“安全孤岛”，缺乏数据共享与联动响应机制，难以在网络攻击发生时快速定位源头并有效阻断；同时，针对云计算、物联网等新兴技术在医疗领域的应用，相关防护技术尚未成熟，云数据安全保障不足、智能设备漏洞防护滞后，暗藏新的安全隐患[4]。在管理层面，制度覆盖存在盲区，未针对数据采集、存储、使用、传输全生命周期制定细化操作流程，科研数据使用的审批权限与规范等关键环节缺失；且制度执行缺乏有效监督考核，既无明确的网络安全考核指标，对违规操作行为的处罚力度也不足，难以形成刚性约束。在法律层面，现有《网络安全法》《数据安全法》《个人信息保护法》等法律法规缺乏医疗领域的具体适用细则，如急诊抢救场景下敏感个人信息处理的同意规则不明确；同时不同法规侧重存在差异，《数据安全法》强调安全与发展并重，《个人信息保护法》侧重个人权益保护，医院在实际操作中难以兼顾，合规难度显著增加。在人员层面，医护人员的网络安全培训多侧重理论知识，缺乏结合医疗场景的实操演练，如钓鱼邮件识别、患者数据安全存储等实用技能培训不足，导致其应对安全风险的能力薄弱；部分医院管理层还存在“重业务、轻安全”的倾向，将更多资源投入医疗设备更新与诊疗服务提升，对网络安全建设的资金、人员投入不足，成为安全事件频发的重要诱因[5]。

4. 医院隐私数据保护及网络安全策略

4.1. 技术防护策略：构建全生命周期安全防护体系

围绕医院隐私数据全生命周期安全需求，从采集、存储、使用、传输四环节搭建技术防护体系，实现“源头防控、过程监管、末端追溯”的全方位保护。数据采集环节，通过“用户名 + 密码 + 人脸认证”等多因素认证锁定合法采集主体，对智能医疗设备采集数据加密传输，并建立自动校验机制，保障数据采集合规性与准确性；数据存储环节，采用“分层存储 + 双重加密”模式，核心数据存于物理隔离内网，非核心数据存于合规云端，以对称加密保护数据内容、非对称加密保护密钥，同时建立“本地 + 异地”双重备份机制，定期加密备份并开展恢复演练，确保数据抗风险能力；数据使用环节，部署数据防泄漏(DLP)系统与操作审计系统，前者实时监测并阻断非法拷贝、外发行为，后者记录全量操作形成可追溯日志，非诊疗场景则通过数据脱敏处理隐藏患者敏感信息，平衡数据利用与隐私保护；数据传输环节，内部传输依托局域网与 VPN 加密，外部与机构间传输采用 HTTPS、SFTP 等安全协议，远程诊疗的音视频数据实时加密，全方位规避传输过程中的拦截、篡改风险[6]。

4.2. 管理优化策略：建立常态化安全管理机制

通过完善制度、优化架构、强化培训，构建“权责明确、流程规范、监督到位”的常态化安全管理机制，将网络安全融入医院日常运营。制度建设上，制定覆盖数据全生命周期的制度体系，包括《医院隐私数据分类分级管理办法》等，明确信息科、医务科、病案科等部门职责，并结合法规更新与技术发展定期修订，保障制度时效与合规；组织架构上，成立由院长牵头的网络安全与数据保护领导小组，下设技术防护、制度监督、应急处置三组，同时在各科室设安全联络员，形成“领导小组－专项小组－科室联络员”三级架构，实现管理全覆盖；人员培训上，搭建分层分类体系：对管理层开展法规与战略意识培训，对技术人员开展高级防护技术培训，对医护人员开展钓鱼邮件识别、数据安全存储等场景化实操培训，培训后考核把关，定期通

过宣传周普及安全知识，营造全员参与氛围；监督考核上，将网络安全纳入绩效考核，建立奖惩机制，每季度开展全面安全检查，每年邀请第三方机构作风险评估，及时整改漏洞，推动安全管理持续优化；绩效考核的刚性约束：制定可量化的网络安全绩效考核表，如表 3 所示，将软性要求转化为硬性指标。

Table 3. Example of cybersecurity performance appraisal form for hospital departments
表 3. 医院科室网络安全绩效考核表示例

考核维度	具体指标	目标值	权重
安全行为	弱口令设备占比	<5%	15%
	模拟钓鱼点击率	<10%	15%
制度执行	数据分类分级准确率	>90%	20%
	隐私数据操作日志完整率	100%	15%
应急响应	安全事件上报及时率	100%	20%

由表 3 可知，该考核表成功将抽象的网络安全要求，转化为一套具体、可量化、可追溯的管将网络安全战略转化为各部门具体行动的有效抓手，是实现“常态化安全管理”理念的杰出实践。它围绕“人、行为、流程”三大核心，设定了六个关键指标，形成一个清晰的管理闭环。

4.3. 法律保障策略：推动合规管理与权益保护

以法律法规为依据，构建“合规与权益并重”的法律保障体系，兼顾医院数据保护合规性与患者权益保障[7]。合规管理层面，建立法律法规跟踪解读机制，安排专人跟进《网络安全法》《数据安全法》《个人信息保护法》更新动态，将法律要求转化为医院实操规范(如依据《个人信息保护法》制定技术防护标准)；每半年开展数据保护合规自查，重点核查数据采集同意、使用范围、存储时限等合规性，对问题及时整改，同时每年引入第三方机构开展独立合规审计，出具报告确保合规落地。权益保护层面，搭建患者数据查询与异议处理机制，患者可通过官网、APP 查询数据使用记录并提出异议，医院需限时核查反馈；完善数据泄露通知机制，按法规要求向监管部门报告并告知患者泄露信息、影响范围及应对建议；建立权益救济渠道，提供投诉举报途径，协助患者通过协商、调解、诉讼维权，必要时提供法律援助。行业协同层面，推动医院与监管部门、行业协会协作，参与《医疗行业数据分类分级指南》等标准制定，助力行业安全标准统一；加入医疗网络安全联盟，共享威胁信息与防护经验，联合应对跨区域风险；加强与司法机关合作，对数据泄露、网络攻击等违法事件及时报案，配合调查追责，形成法律震慑(如图 1 所示)。

Figure 1. Architecture diagram of the privacy data security protection system for hospitals
图 1. 医院隐私数据安全防护体系架构图

5. 医院隐私数据保护及网络安全的未来展望

随着医疗数字化转型深入，医院隐私数据保护及网络安全将迎来技术、管理、协作机制的深度变革，呈现智能化升级、协同化深化、标准化统一三大核心趋势。技术智能化层面，AI 与大数据技术将实现从被动防御到主动预测的跨越，AI 驱动的智能防护系统可实时识别新型威胁并标记异常操作，大数据技术能构建多维度风险评估模型预测漏洞，区块链技术强化数据溯源与隐私保护，零知识证明、联邦学习实现数据可用不可见，量子通信技术还将为核心数据传输提供绝对安全通道；管理协同化层面，单一医院防御将转向跨主体协同防护，医院与云服务提供商、安全厂商建立一体化安全服务模式，医卫行业安全联盟推动案例与经验共享，医院与监管部门也将从事后报备转向实时联动，形成双向互动的安全管理格局；标准标准化层面，医疗数据安全行业统一标准体系将逐步完善，国家层面细化数据分类分级与安全要求，行业协会制定设备技术参数与部署规范，合规认证体系更健全，以标准化推动安全能力与行业信任度提升，为破解当前安全痛点提供新路径。

这些趋势的落地将推动医院隐私数据保护从传统的被动应对向主动防控、从单一机构防护向跨主体协同、从零散管理向标准规范转型。例如，当 AI 智能防护系统与跨主体协同机制结合时，某家医院识别的新型勒索软件攻击特征，可通过医卫行业安全联盟实时同步至全国多家医院，再配合统一的设备技术标准，各医院能快速通过标准化安全设备完成防护升级，大幅降低攻击扩散风险。未来，随着这些趋势的深度融合，医院隐私数据保护及网络安全将形成技术先进、管理高效、协作紧密、标准统一的全新格局，为医疗信息化高质量发展筑牢安全根基，也为健康中国战略中医疗数据的安全利用与患者权益保障提供更坚实的支撑。

6. 结语

医院隐私数据保护及网络安全是医疗信息化发展的生命线，既关乎患者个人权益与生命健康，也影响医疗服务连续性与行业公信力。本文通过分析医院隐私数据的特征与网络安全现状，梳理出数据泄露、篡改等四类核心风险，以及技术、管理、法律、人员层面的突出问题，并从技术防护、管理优化、法律保障三个维度构建全方位策略体系，技术上通过全生命周期防护筑牢安全屏障，管理上依托常态化机制压实安全责任，法律上凭借合规与权益并重实现风险管控，三者协同形成技术防风险、管理固根基、法律强保障的闭环防护格局。当前，医疗数字化转型与新兴技术应用为安全防护带来新挑战，也提供了智能化、协同化的解决路径，医院需摒弃重业务、轻安全的传统观念，将网络安全纳入战略发展规划，通过技术升级、管理革新与行业协作持续提升隐私数据保护能力。未来，随着智能防护技术的普及、跨主体协同机制的完善与行业标准的统一，医院隐私数据保护将逐步实现从应对风险到抵御风险再到预测风险的进阶，为医疗信息化健康发展保驾护航，最终助力健康中国战略下医疗服务质量与安全水平的整体提升。

基金项目

佛山市科技创新项目医学科技创新平台建设项目(FS0AA-KJ218-1301-0016)；佛山市数字医疗信息工程技术研究中心，项目编号：2020001003957。

参考文献

[1] 付文伟. 大数据环境下用户隐私保护与网络安全策略研究[J]. 中国电信业, 2025(8): 54-57.

[2] 苗选. 医院网络安全防护体系的风险评估分析[J]. 电子技术, 2025, 54(8): 386-387.

[3] 王强林. 物联网环境下网络安全管理架构的数据隐私保护策略研究[J]. 中国战略新兴产业, 2025(9): 53-56.

[4] 王廷轩, 刘顺. 基于零信任架构的医院网络安全防护策略探析[J]. 电子元器件与信息技术, 2025, 9(6): 223-226.

[5] 郑富豪. 标准化视角下医院智慧档案馆的数据安全与隐私保护策略[J]. 中国品牌与防伪, 2024(9): 123-124.

[6] 庄凤庭. 现代医院网络安全管理面临的挑战和策略[J]. 网络安全和信息化, 2024(8): 34-37.

[7] 李志勇. 网络安全平台在医院网络数据保护和隐私管理中的应用[J]. 网络安全和信息化, 2023(10): 42-44.