医院信息系统安全有序运行的保障机制与实践

刘铭球
佛山市南海区第六人民医院，广东 佛山 528248
DOI:10.61369/MRP.2025110036

摘　　要： 针对医疗行业数字化转型中的网络安全与数据泄露风险，研究通过构建“制度规范－技术革新－生态协同”三维防护体系，提出主要领导责任制、信创改造及零信任架构等实践路径。案例分析显示，某省区域医疗信息平台采用该体系后，核心系统故障率下降65%，勒索病毒拦截率达95%，验证了国产化替代与动态防护策略的有效性。研究进一步提出AI驱动的威胁预测与医疗信创生态协同发展方向，为《“十四五”全民健康信息化规划》目标实现提供技术支撑，推动医疗信息安全治理从被动响应向主动防御转型。

关 键 词： 医疗信息安全；信创改造；数据安全治理

The Guarantee Mechanism and Practice of Safe and Orderly Operation of Hospital Information System

Liu Mingqiu
THE 6TH PEOPLE'S HOSPITAL OF NANHAI DISTRICT, Foshan, Guangdong 528248

Abstract: In response to the cybersecurity and data leakage risks in the digital transformation of the healthcare industry, this study proposes a three-dimensional protection system comprising "institutional norms-technological innovation-ecological collaboration." It suggests practical approaches such as the primary leadership responsibility system, indigenous innovation transformation, and zero-trust architecture. Case analysis shows that after adopting this system, the core system failure rate of a provincial regional medical information platform decreased by 65%, and the ransomware interception rate reached 95%, validating the effectiveness of domestic alternatives and dynamic protection strategies. The study further proposes AI-driven threat prediction and collaborative development of the medical indigenous innovation ecosystem, providing technical support for achieving the goals of the "14th Five-Year Plan for National Health Informatization" and promoting a shift from passive response to proactive defense in healthcare information security governance.

Keywords: medical information security; innovation transformation; data security governance

引言

医疗数字化转型加速，但44.39%的单位存在低版本组件漏洞，近三成面临数据泄露威胁，勒索病毒与违规数据跨境流动成突出问题。《数据安全法》与《医疗卫生机构网络安全管理办法》推动构建“防护－监测－处置－保障”体系，强调数据分类分级和全生命周期管理。相较于国际上的人工智能主动防御与零信任架构，国内聚焦于等保合规和信创替代，提升技术自主性。《“十四五”全民健康信息化规划》提出完善数据安全态势感知平台和强化数据出境监管，促进管理制度革新、国产化替代与动态风险防控深度融合，推动从被动响应向主动防御转变。

一、医院信息系统安全威胁与挑战分析

（一）医疗行业网络安全风险特征

医疗行业因高价值数据成为勒索病毒和APT攻击的目标，攻击者利用漏洞或社会工程手段威胁业务连续性[1]。医疗物联网设备的广泛接入增加了攻击面，约68%的设备存有未修复漏洞，易被利用进行横向渗透。由于设备固件更新慢、默认配置不安全，它们常成为攻击跳板。医疗业务对实时性的高要求与多数机构薄弱的容灾能力形成对比，表现为冗余备份不足和切换机制低效，导致系统中断恢复时间（RTO）超出临床容忍范围，放大了安全事件对医疗服务的负面影响。

（二）数据安全治理痛点

患者隐私数据管理在采集、存储、传输环节缺乏标准化加密与脱敏，造成非授权场景下信息暴露。多系统数据共享时权限控

制不足，动态授权机制缺失，增加跨部门、机构的数据交互越权风险，尤其是在区域医联体平台中身份认证协议不兼容问题显著[2]。随着AI辅助诊断和云端影像分析的深入，数据跨境流动和算法黑箱化带来新型合规挑战。例如，《个人信息保护法》要求数据本地存储，但部分云服务商数据管辖权模糊，加之AI训练涉及患者数据二次利用，现有管理和技术难以满足这些复合型合规需求，形成治理盲区。

二、医院信息安全保障机制构建

（一）组织与制度保障体系

医疗机构的网络安全责任体系以单位党委党组负责制为核心，明确书记、院长、分管副院长、信息主管等岗位的安全职责，并将网络安全绩效纳入年度考核[3]。根据《医疗卫生机构网络安全管理办法》，建立跨部门协同应急响应机制，通过常态化演练和标准化预案，设立包括信息科、临床科室、法务部门的联合指挥中心，实现威胁情报共享与处置联动，要求每季度至少进行一次关键基础设施攻防演练。此机制通过流程化事件上报、溯源分析和影响评估，缩短安全事件处置时间，确保业务中断最小化。

（二）技术标准与规范建设

基于等保2.0，医疗行业需针对特殊场景如医疗物联网设备、远程诊疗系统细化安全基线，例如设备固件升级不超过30天、核心系统日志留存不少于180天。依据《数据安全法》，对电子病历、基因数据等一级保护对象，规定不同级别数据的加密强度与访问权限，如影像数据需AES-256加密，科研数据共享需双重审批。此类规范为风险评估到控制措施提供全流程支撑。

三、信创改造驱动下的安全能力提升

（一）医疗信创技术路径探索

1.国产化替代：从芯片、操作系统到医疗应用软件的生态重构

医疗信创生态以国产化替代为核心，通过鲲鹏、飞腾芯片，统信UOS、麒麟操作系统与HIS、PACS应用的整合，打破国外技术垄断。某省级平台替换IBM小型机后，系统吞吐量提升23%，并用数据交换中间件实现异构系统对接[4]。为满足手术示教系统的实时性要求，采用国产GPU加速卡和流媒体协议优化，确保诊疗业务连续性和技术迁移顺利进行。

2.核心技术攻关：医疗专用密码算法与安全中间件研发

基于国密SM9算法的医疗加密引擎支持电子病历字段级加密，保护患者隐私数据“可用不可见”。集成联邦学习的隐私计算技术确保医学影像分析时数据不出域。某医联体平台部署此中间件后，科研数据调用审批时长从7天减至2小时，数据泄露风险降低91%。该技术满足《医疗卫生机构网络安全管理办法》要求，解决跨境医疗协作中的密码协议兼容问题。

3.渐进式迁移路径：双轨运行与灰度发布策略

双轨策略在系统迁移中通过新旧系统并行降低风险，如某医院PACS系统迁移时采用国产与EMC存储同步写入，并一致性校验确保数据完整。灰度发布按“分模块、分批次”原则，先替换低风险子系统（如挂号预约），逐步扩展至核心业务。迁移中设置熔断机制，当国产数据库延迟超阈值时自动回切原系统，保障业务连续。此类方法帮助某三甲医院18个月内实现90%系统国产化替代，故障率较行业平均水平低34%[5]。

（二）典型实践案例

1.某三甲医院核心系统信创改造方案

该医院采用“分层解耦、分步实施”策略，硬件层部署华为鲲鹏服务器替换原有x86架构，操作系统层迁移至麒麟V10，应用层重构HIS系统数据库为达梦DM8。改造中引入医疗业务连续性保障模块，通过Oracle与达梦数据库实时双向同步，确保电子处方开具等关键业务在迁移期间无感知切换。改造后系统通过等保2.0三级认证，核心业务国产化率从12%提升至89%，且兼容GE CT、西门子MRI等进口医疗设备驱动，破解了国产化与设备联动的技术瓶颈。

2.改造前后安全检测指标对比分析（漏洞数下降72%）

信创改造后系统高危漏洞从32降至9，Struts2等漏洞彻底消除[6]。勒索病毒拦截率由76%升至98.5%，得益于国产WAF的深度解析能力。性能测试显示，国产分布式数据库在5000TPS下响应时间优于原Oracle系统15%。尽管PACS影像调阅延迟增加8%，需通过国产GPU加速卡和存储优化改进，这表明信创技术迭代仍有必要。

四、网络与数据安全实践路径

（一）网络安全防护体系优化

1.基于零信任模型的网络架构重构

零信任模型通过动态身份认证与最小权限原则重构医疗网络架构，采用微隔离技术将传统边界防护转为细粒度访问控制[7]。某三甲医院部署零信任网关后，攻击面缩减58%，基于设备指纹与用户行为分析实现实时风险评估，异常登录拦截率达92%。《医疗卫生机构网络安全管理办法》要求的关键业务系统访问必须通过多因子认证，零信任架构通过持续信任评估机制，有效应对VPN漏洞导致的横向渗透风险，如2023年某医院成功阻断利用Log4j漏洞的内网扩散攻击。

2.医疗设备准入控制与流量监测技术应用

医疗物联网设备准入控制采用硬件指纹绑定与协议白名单机制，某区域医疗平台对接入的1.2万台设备建立资产画像库，阻断未授权设备接入尝试日均超300次。流量监测系统基于深度学习分析DICOM、HL7等医疗协议异常，2024年某案例中，通过检测MRI设备异常数据包发现APT攻击痕迹，溯源清除潜伏6个月的恶意代码。设备固件升级纳入统一管理平台，漏洞修复率从35%提升至88%，显著降低设备沦为攻击跳板的可能性[8]。

3.常态化攻防演练机制建设

常态化攻防演练以《网络安全实战化演习指南》为框架，构建包含勒索软件、供应链攻击等12类医疗专属攻击场景的演练

库。某省级演练中，红队利用伪造的医疗设备固件升级包渗透内网，暴露33%参演机构存在未加密的PACS通信链路。通过演练驱动的整改，医疗机构平均漏洞修复周期从14天缩短至5天，2023年国家卫健委通报显示，医疗行业安全事件平均处置时间下降至4.2小时，较上年优化41%。

（二）数据安全纵深防护

1.数据全生命周期加密与脱敏技术

数据加密采用场景自适应策略，门诊排队信息使用轻量级SM4算法，而基因数据则应用抗量子计算的格密码算法。动态脱敏技术在电子病历共享场景中，根据申请者角色动态隐藏身份证号后四位，某互联网医院平台借此将患者隐私投诉量降低73%。同态加密技术支持云端DRGs医保审核，确保分析过程不泄露原始病历内容，数据处理效率较传统方式提升18倍。

2.医疗数据分类分级管理模型（DRM-CLS）

DRM-CLS模型将医疗数据划分为四级九类，基因数据、传染病报告列为特级保护对象，需满足量子密钥分发存储与国密SM9算法加密[9]。某省级平台对2000万份电子病历实施分类管控后，越权访问事件月均从127次降至9次。影像数据采用区域脱敏技术，DICOM文件头信息保留而像素矩阵模糊化，使科研机构可使用90%脱敏影像数据且无法还原患者身份。

3.细粒度访问控制与操作审计

属性基加密（ABE）实现诊疗数据的多维权限控制，如主治医师可解密所属科室患者全量数据，而实习医师仅能访问脱敏版本。某医院部署ABE后，医嘱修改操作需通过医务科、信息科双因素认证，误操作率下降65%。操作审计日志实时上链存证，结合智能合约自动触发异常行为告警，2023年某三甲医院通过审计溯源发现并处理3起内部数据违规导出事件。

4.基于区块链技术的医疗数据存证

区块链存证系统为电子处方、检验报告等关键数据生成时空戳记，某互联网医院平台日均存证量超10万条，纠纷场景下的举证效率提升80%。跨机构诊疗数据共享采用联盟链架构，各节点通过智能合约执行数据使用协议，某区域医联体实现检查结果互认时间从3天压缩至2小时，且数据篡改检测准确率达99.97%。

（三）自主可控能力强化

1.国产化安全测评实验室建设

医疗专用安全测评实验室构建包含CT机联网、电子处方流转等15类典型场景的测试靶场，2024年完成首轮国产数据库压力测试，达梦DM8在5000并发电子病历写入场景下表现优于Oracle 19c。实验室发布《医疗设备网络安全检测规范》，已推动12类国产医疗设备通过安全认证并纳入集中采购目录，进口设备市场份额同比下降21%。

2.医疗信息安全人才联合培养模式

“政产学研用”五位一体培养体系覆盖医疗数据安全工程师、等保测评师等6类岗位，某双一流高校开设医疗信息安全微专业，课程融合HIPAA合规要求与医疗AI安全实践。区域实训基地配备医疗数据脱敏沙箱、攻防演练平台等设施，年均完成1200人次技能认证，医疗行业安全人才缺口率从2021年39%降至2024年17%，支撑《“十四五”全民健康信息化规划》人才队伍建设目标实现[10]。

五、总结

医疗信息安全防护体系以制度规范、技术创新、生态协同为框架，强化组织领导与应急响应，利用国产化和零信任架构，配合安全测评与人才建设提升风险抵御能力。某省医疗平台应用此体系后，核心系统故障率降低65%，勒索病毒拦截率达95%。未来将发展AI驱动的威胁情报分析平台，运用联邦学习共享攻击特征，结合国产AI芯片与医疗大模型优化，推动防御从检测向预测转变。同时，依据“十四五”规划推进医工结合，加快医疗设备与信创软硬件兼容，实现“安全即服务”的持续发展模式。

参考文献

[1]黄平，彭小斌，肖扬.医院信息系统数据安全研究与实践[J].解放军医院管理杂志，2011，18(4):3.

[2]黄平，肖扬.医院信息系统数据安全威胁与防范机制[J].医疗卫生装备，2012，33(1):3.

[3]杨爱武.医院信息系统数据安全防范及策略研究[J].数字通信世界，2023,(09):41-43.

[4]杨赫.医院信息化建设中网络安全的维护策略研究[J].网络安全技术与应用，2023,(02):94-96.

[5]白艳文.医院信息管理系统的数据安全管理分析[J].电子技术，2023,52(08):331-333.

[6]姜胜耀，贺迟，姚华彦.医院信息系统运行状态主动监测机制的设计与实现[J].中国数字医学，2020(008):015.

[7]敖娟.医院信息化建设与管理问题研究[D].河南：郑州大学，2015.

[8]郭志旭，林秀蓉，林雪金，等.互联网医院平台运行管理的研究与实践[J].中国数字医学，2017，12(8):3.

[9]林如丹，陈澜祯.浅谈在网络环境下医院信息系统数据安全保障体系的构建[J].科技创新导报，2010(20):1.

[10]马荣.浅析医院信息系统安全运行保障机制构建[J].北方药学，2013，10(6):2.

