医院电子信息化建设中的信息安全研究

陈明华
凤庆县人民医院　云南　临沧　675900

摘　要：医院电子信息化建设在提升诊疗效率与管理水平的同时，面临复杂的信息安全挑战。其核心问题包括：网络攻击频发、数据泄露风险突出、系统漏洞及物联网设备安全隐患；管理层面存在权限混乱、人员安全意识薄弱及第三方风险；法律层面涉及跨境数据传输合规性不足及患者知情权保障缺失。研究聚焦于构建动态风险评估模型，融合ISO27001与NIST框架，量化技术、管理及行业特有风险，并提出技术防护、管理机制优化及法律合规保障三位一体的安全体系，以保障医疗数据全生命周期安全。

关键词：医院；电子信息化建设；信息安全

引言：在医疗行业数字化转型浪潮下，医院电子信息化建设高速推进，HIS、LIS、PACS等系统深度集成，海量医疗数据应运而生。这些数据涵盖患者个人健康信息、基因数据等高价值内容，在提升医疗效率与质量的同时，也沦为黑客觊觎的目标。网络攻击、数据泄露、系统漏洞等安全威胁频发，不仅损害患者权益，更可能危及生命安全。此外，管理疏漏与法律合规问题也加剧了安全风险。因此，深入研究医院电子信息化建设中的信息安全问题，构建有效的防护体系，已成为当务之急。

1 医院电子信息化安全现状与问题分析

1.1 医院信息化架构特征

（1）分布式系统（HIS、LIS、PACS等异构系统集成）：医院核心业务依赖多系统协同，HIS（医院信息系统）、LIS（检验信息系统）、PACS（影像归档和通信系统）等异构系统深度集成。此类架构虽提升诊疗效率，但系统间数据流转频繁，运维需跨平台协同，如盛京医院数据库倒换需耗时两天两夜，且易因接口差异埋下安全隐患。（2）高价值数据集中（个人健康信息PHI、基因数据等）：医疗数据呈现规模化聚集特征，盛京医院存储电子病历达50T、影像数据500T，包含姓名、病情、基因等敏感信息。这些高价值数据成为黑客主要目标，在黑市可高价倒卖，甚至被用于敲诈勒索[1]。

1.2 主要安全风险

（1）技术层面：网络攻击频发，2018年南漳县人民医院、湖南省儿童医院均遭GlobeImposter家族勒索病毒攻击，导致HIS服务器加密、系统瘫痪；数据泄露隐患突出，某医疗企业650余万条患者信息未加密存储，遭境外IP窃取；系统漏洞普遍存在，部分机构高危漏洞达3个，且IoT医疗设备因安全标准不足成为新攻击入口。（2）管理层面：权限管理混乱，外包人员共用数据库账号，可随意访问导出数据；员工安全意识薄弱，华盛顿大学医学院员工因钓鱼邮件泄露8万份病历，7周后才被发现；第三方风险显著，HIS等系统运维商若防护不足，易引发连锁安全事件。（3）法律层面：跨境数据传输合规性不足，部分机构未按规定开展安全测评，存在数据非法流出风险；患者知情权保障缺失，病历流转、第三方调用中常出现信息泄露未及时告知的情况，违反《个人信息保护法》要求。

2 医院电子信息化建设中的信息安全风险评估模型构建

2.1 风险评估框架设计

（1）基于ISO27001与NIST网络安全框架的适配性分析：ISO27001聚焦信息安全管理体系的通用性要求，涵盖风险评估、控制措施等核心模块，可作为医院安全管理的基础框架；NIST网络安全框架则以“识别-保护-检测-响应-恢复”五阶段模型为核心，更侧重动态风险防控。在医疗场景中，需将两者适配融合：以ISO27001为基础搭建管理体系，明确医院信息安全的组织架构、制度规范及人员职责；结合NIST框架的动态特性，针对医疗业务连续性需求，强化“检测-响应-恢复”环节设计，例如在检测阶段增加医疗系统异常流量监控指标，响应阶段制定急救系统优先恢复预案，确保框架既符合通用安全标准，又适配医疗行业特殊性。（2）医疗行业特有风险指标：除通用安全指标外，需补充医疗场景专属指标。一是急救系统可用性，急救系统（如急诊挂号、生命体征监测系统）中断将直接威胁患者生命安全，需将其平均无故障时间（MTBF）、故障恢复时间（MTTR）纳入核心指标，要求MTTR不超过30分钟；二是数据篡改影响，医疗数据（如检验报告、手术记录）篡改可能导致误诊、误治，需评估数据篡改后的诊疗风险等级，按

影响程度划分为“致命-严重-一般-轻微”四级，例如手术记录关键数据篡改判定为“致命”风险[2]。

2.2 关键风险识别

（1）数据生命周期安全：覆盖数据采集、传输、存储、销毁全流程。采集阶段风险为数据源头造假（如虚假患者信息录入）、非授权采集（如擅自收集患者隐私数据）；传输阶段风险为数据截获（如未加密的病历数据在传输中被窃取）、传输中断（如网络故障导致数据传输失败）；存储阶段风险为存储介质损坏（如服务器硬盘故障导致数据丢失）、非法访问（如未授权人员访问数据库）；销毁阶段风险为数据残留（如报废硬盘未彻底清除数据，导致信息泄露）、销毁不及时（如过期医疗数据未按规定时限销毁）。（2）物联网设备安全：针对医院常用IoT设备，识别多维度风险。可穿戴设备（如远程心电监测设备）风险为数据传输不加密、设备被劫持（如篡改监测数据）；医疗机器人（如手术机器人、送药机器人）风险为系统漏洞（如机器人控制系统存在漏洞被恶意操控）、物理安全（如机器人碰撞患者或医护人员）；智能医疗设备（如智能输液泵、心电监护仪）风险为固件老化（如未及时更新固件导致安全漏洞）、接口不安全（如设备与HIS系统对接接口未做安全防护）。

2.3 量化评估方法

（1）层次分析法（AHP）确定风险权重：构建三级指标体系，一级指标为“技术风险、管理风险、行业特有风险”，二级指标包含“数据安全、设备安全、权限管理、急救系统安全”等，三级指标为具体风险点（如数据泄露、机器人系统漏洞）。通过邀请医疗信息化专家、网络安全工程师、临床医护人员组成评审组，采用1-9标度法对各指标进行两两比较，构建判断矩阵，计算权重值。例如，在一级指标中，“行业特有风险”因直接关联患者生命安全，权重设定高于通用技术风险、管理风险，通常分配35%-40%的权重；三级指标中，急救系统中断风险权重高于普通数据泄露风险[3]。（2）模糊综合评价法评估安全等级：结合医疗风险的模糊性特征，采用模糊综合评价法。首先确定评价因素集（如数据生命周期风险、IoT设备风险）和评价等级集（“高风险-中风险-低风险”）；其次构建模糊关系矩阵，通过专家打分确定各风险点隶属于不同评价等级的隶属度，例如某医院数据存储风险中，“高风险”隶属度为0.6，“中风险”为0.3，“低风险”为0.1；最后结合AHP确定的权重，进行模糊矩阵合成运算，得出综合评价结果，若最终结果隶属“高风险”等级，需启动紧急整改预案，隶属“中风险”等级则制定阶段性改进计划。

3 医院电子信息化建设中的信息安全保障体系设计

3.1 技术防护体系

（1）数据加密：同态加密、区块链存证技术应用：针对医疗数据全生命周期安全，采用分层加密策略。在数据计算环节应用同态加密技术，支持在加密状态下对病历数据进行统计分析、AI辅助诊断，避免数据解密过程中的泄露风险，例如在肿瘤患者基因数据研究中，可实现多医院数据“可用不可见”；在数据存证环节引入区块链技术，对电子病历、检验报告等关键数据的生成时间、修改记录进行上链存证，利用区块链不可篡改特性，防止数据被恶意篡改，同时满足医疗纠纷中的数据溯源需求，确保每一次数据操作都可追溯、可验证。（2）零信任架构（ZTA）在医疗网络中的部署：打破传统“内网可信、外网不可信”的边界思维，构建“永不信任、始终验证”的医疗网络防护体系。针对医疗场景设计分级验证机制：对核心业务系统（如HIS、急救系统）采用“多因素认证+最小权限”访问控制，医护人员需通过人脸、工牌、动态密码三重验证，且仅能访问其职责范围内的数据；对IoT设备（如医疗机器人、监护仪）进行身份标识与行为基线设定，实时验证设备接入合法性，一旦发现设备异常访问（如机器人试图连接非授权服务器），立即阻断并告警，防止设备成为网络攻击入口。（3）入侵检测与响应系统（IDS/IPS）优化：结合医疗业务特性优化IDS/IPS功能，建立医疗专属攻击特征库，涵盖勒索病毒、医疗数据窃取等典型攻击行为特征。在检测策略上，针对急救系统、影像传输系统等关键业务，设置“业务优先”检测模式，优先监控影响诊疗的异常流量；在响应环节制定分级处置预案，若检测到针对急救系统的DDoS攻击，立即启动流量清洗与备用链路切换，确保急救业务不中断；若发现数据窃取行为，同步触发数据冻结与溯源追踪，最大限度降低泄露影响。

3.2 管理机制优化

（1）安全运营中心（SOC）建设与威胁情报共享：搭建医院专属SOC，整合网络日志、设备状态、业务数据等多维度信息，通过AI算法实现安全风险的实时监测与预警，例如自动识别异常数据导出行为、设备固件漏洞。同时，加入区域医疗安全联盟，与其他医院、疾控中心、网络安全厂商共享威胁情报，及时获取医疗行业最新攻击手段（如针对疫苗管理系统的恶意软件），提前更新防护策略，形成“协同防御”格局。（2）人员安全培训体系（模拟攻击演练、权限分级管理）：建立

分层分类培训机制，对医护人员开展常态化安全意识培训，内容涵盖钓鱼邮件识别、隐私数据保护规范；对IT运维人员强化技术培训，重点提升漏洞修复、应急处置能力。每季度组织模拟攻击演练，通过发送仿真钓鱼邮件、模拟系统入侵等场景，检验人员安全防护能力，并将演练结果纳入绩效考核。同时，优化权限分级管理，依据“岗位需求”划分数据访问权限，例如门诊医生仅能查看本人接诊患者的病历，且无法导出完整数据，从源头减少人为操作风险。（3）第三方供应商安全审计与合同约束：制定第三方供应商安全准入标准，要求HIS系统运维商、IoT设备供应商具备等保2.0三级以上认证，提供安全防护方案与应急响应预案。在合作合同中明确安全责任条款，规定供应商需定期配合医院开展安全审计，若因供应商防护不足导致数据泄露或系统故障，需承担赔偿责任与法律后果。建立供应商动态评估机制，每半年对供应商的安全履约情况进行评估，对存在安全隐患的供应商，责令限期整改，整改不合格则终止合作[4]。

3.3 法律与合规保障

（1）等保2.0三级以上认证实施路径：制定分阶段认证计划，第一阶段（1-3个月）完成医院信息系统资产梳理与风险评估，针对等保2.0三级要求的物理环境安全、网络安全、数据安全等10个层面，排查整改薄弱环节（如补充机房门禁系统、优化数据备份策略）；第二阶段（4-6个月）搭建符合认证标准的安全技术体系与管理制度，邀请第三方测评机构开展预评估，整改发现的问题；第三阶段（7-9个月）正式提交认证申请，配合测评机构完成现场测评，确保顺利通过等保2.0三级认证，对涉及国家秘密、重要民生数据的系统，推进等保2.0四级认证。（2）跨境数据传输的本地化存储与脱敏方案：严格遵循《数据安全法》《个人信息保护法》要求，对含患者隐私的医疗数据实行本地化存储，在境内搭建数据中心，禁止未经审批将数据传输至境外。确需跨境传输的（如国际医疗合作中的病例数据），先对数据进行脱敏处理，删除姓名、身份证号、住址等可识别个人身份的信息，仅保留病情描述、诊疗方案等非敏感内容；同时向监管部门申请跨境数据传输许可，提交数据传输方案与安全保障措施，经审批通过后方可传输，确保跨境数据传输全程合规。

结束语

医院电子信息化建设中的信息安全研究意义重大，关乎患者权益、医疗秩序与社会稳定。本研究剖析了医院信息化安全现状，指出技术、管理与法律层面的多重风险，构建了适配医疗场景的风险评估模型，并提出涵盖技术防护、管理优化及法律合规保障的体系化方案。未来，随着技术的迭代与医疗模式的创新，信息安全挑战将持续演变。因此，需持续完善安全机制，强化多方协作，推动医疗行业信息安全标准与技术的升级，为医院电子信息化建设的稳健发展筑牢安全基石。

参考文献

[1]罗昊.医院电子信息化建设中的信息安全管理分析[J].无线互联科技,2022,19(2):27-28.

[2]王志宇,刘昊.探究医院电子信息化建设中的信息安全管理[J].中国科技投资,2019,18(29):229.

[3]王庆明.医院电子信息化建设中的信息安全管理策略[J].全体育,2021,19(16):279-280.

[4]江润平.对医院信息化建设中网络安全防护的对策研讨[J].信息与电脑,2019,31(14):206-207.