医院信息系统中的网络安全与管理

王子洋
天津市职业病防治院　天津　300171

摘　要：医院信息系统网络安全与管理至关重要，关乎医疗业务运转与患者隐私安全。其涵盖基础架构、数据类型、拓扑结构等基础理论，涉及边界安全、数据加密、身份认证等技术体系。同时，需构建完善的组织架构与职责分工，制定严格政策流程，开展合规审计。当前面临物联网设备、云医疗等挑战，未来应探索安全即服务模式、前瞻研究量子加密技术、建立跨机构安全信息共享机制，以提升整体防护能力。

关键词：医院信息系统；网络安全；管理

引言：在数字化浪潮席卷下，医院信息系统已成为医疗行业高效运转的核心支撑，涵盖挂号、诊疗、影像存储等关键业务。然而，随着网络攻击手段日益复杂，医疗数据因其高价值性成为黑客觊觎的目标，数据泄露、系统瘫痪等安全事件频发，不仅威胁患者隐私与生命安全，也影响医院正常运营。因此，构建全方位、多层次的医院信息系统网络安全管理体系，已成为保障医疗行业稳定发展、维护公众健康权益的迫切需求。

1 医院信息系统中的网络安全基础理论

1.1 医疗信息系统架构解析

（1）核心系统：HIS（医院信息系统）支撑挂号、收费等日常运营；LIS（检验信息系统）管理检验流程与结果；PACS（影像归档和通信系统）存储传输CT、MRI等影像数据三者协同保障医疗业务运转。（2）数据类型：患者隐私数据含身份证号、病历等敏感信息；临床决策数据包括诊断记录、用药方案，直接影响诊疗；财务数据涉及收费明细、医保结算，关联医院资金安全。（3）网络拓扑结构：内网承载核心业务，与专网（如医保专线）、互联网交互时存在风险，互联网接入易引入外部攻击，专网数据交互可能因协议漏洞导致信息泄露。

1.2 网络安全威胁分析

（1）攻击面：系统漏洞多源于软件未及时更新；移动介质（如个人U盘、手机）接入内网，易携带恶意程序；第三方服务（如运维、云存储）若防护不足，可能成为攻击跳板。（2）典型攻击手段：勒索软件（如WannaCry）加密医疗数据索要赎金，致系统瘫痪；APT攻击长期潜伏，窃取核心医疗数据；内部人员因疏忽或恶意泄露数据，风险更难防范。（3）医疗数据特殊性：高价值性使其成为黑客目标，可用于诈骗等；不可恢复性若丢失，影响患者后续诊疗；法律敏感性违反《个人信息保护法》等，医院将面临严惩[1]。

1.3 安全需求与目标

（1）CIA三原则延伸：保密性要求患者隐私数据仅授权人员可访问，如通过权限分级限制病历查看；完整性需确保临床决策数据不被篡改，如采用区块链技术记录用药方案修改痕迹；可用性要求系统在突发故障时快速恢复，如影像系统需保障急诊医生随时调阅检查结果。（2）业务连续性要求：业务系统需7×24小时可用，通过双机热备、异地灾备实现故障无缝切换；门诊挂号、缴费系统需抵御流量攻击，避免就诊高峰时系统崩溃，保障患者就医流程顺畅。

2 医院信息系统中的网络安全技术体系

2.1 基础防护技术

（1）边界安全：防火墙作为网络边界第一道防线，通过预设规则过滤进出流量，阻断非法访问，例如限制外部IP直接访问HIS数据库；入侵防御系统（IPS）则实时监测网络异常行为，对SQL注入、端口扫描等攻击进行主动拦截，弥补防火墙仅被动过滤的不足，二者协同构建边界安全屏障。（2）数据加密：传输层采用SSL/TLS协议，在医生调取PACS影像、患者查询电子病历等数据传输过程中，对数据进行加密处理，防止中途被窃取或篡改；存储层运用AES加密算法，对数据库中的患者隐私数据、临床决策数据进行加密存储，即使数据库被非法入侵，攻击者也无法解读加密数据，保障数据存储安全[2]。（3）身份认证：多因素认证（MFA）结合密码、动态验证码（如手机短信验证码）、USBKey等多种认证方式，避免单一密码泄露导致账号被盗，例如医生登录系统时，需同时输入密码和手机接收的动态验证码；生物特征识别则利用指纹、人脸、虹膜等唯一生物信息进行身份验证，应用于重要操作授权，如修改患者核心病历数据需进行指纹验证，提升身份认证安全性。

2.2 高级防御技术

（1）零信任架构（ZTA）在医疗场景的应用：遵循“永不信任，始终验证”原则，打破传统内网“可信”的认知，对每一次访问请求（无论来自内网还是外网）都进行严格身份认证和权限校验，防止越权操作，有效应对内网横向渗透风险。（2）人工智能驱动的威胁检测：通过AI算法学习医疗系统正常操作模式，如医生日常调取病历的时间、频次、数据范围，设备正常通信流量等，当出现异常行为（如某账号短时间内批量下载患者数据、设备通信流量骤增）时，系统自动发出预警并触发干预措施，相比传统人工监测，能更快速、精准识别未知威胁，如APT攻击的早期痕迹。（3）区块链技术在电子病历防篡改中的实践：将电子病历关键信息（如诊断结论、用药记录）以区块形式存储在分布式节点上，每个区块包含前一区块的哈希值，形成不可篡改的链式结构。一旦有人试图修改某条病历数据，所有节点存储的哈希值都会发生变化，系统可立即发现篡改行为并追溯责任人，同时区块链的透明性也便于监管部门核查，保障电子病历的真实性和完整性，为医疗纠纷处理、医保审核提供可靠依据[3]。

2.3 应急响应与恢复

（1）灾难恢复计划（DRP）设计：明确灾难（如服务器宕机、勒索软件攻击、自然灾害）发生后的应急组织架构、职责分工，制定详细恢复流程，包括应急启动条件、数据恢复步骤、系统重启顺序等。例如当急诊系统因勒索软件瘫痪时，按照DRP，运维团队需在30分钟内启动应急响应，技术组负责隔离受感染设备，数据组负责恢复备份数据，保障急诊系统尽快恢复运行。（2）数据备份策略：采用异地容灾方案，在不同地理区域建立备份中心，主数据中心数据实时同步至备份中心，当主中心遭遇地震、火灾等灾难时，可快速切换至备份中心，避免数据丢失；同时实施冷热备份结合，热备份（如实时同步备份）用于快速恢复高频访问数据（如急诊患者病历），冷备份（如定期离线硬盘备份）用于存储历史数据（如往年归档病历），兼顾恢复速度与数据长期安全[4]。（3）攻防演练与红蓝对抗机制：定期组织攻防演练，将团队分为“红队”（模拟攻击者）和“蓝队”（负责防御），红队采用真实攻击手段（如模拟勒索软件攻击、内部人员泄露数据）对医疗系统发起攻击，蓝队则进行防御和应急处置。通过演练检验安全防护体系有效性，发现防护漏洞并及时修复，同时提升团队应急响应能力，确保在真实威胁发生时能高效应对。

3 医院信息系统中的网络安全管理体系

3.1 组织架构与职责

（1）网络安全委员会构成：由信息科、医务部、法务部协同组成核心决策层。信息科负责技术落地，如安全设备运维、漏洞修复；医务部结合临床场景制定安全规则，例如规范电子病历访问流程，避免影响诊疗效率；法务部对接法律法规，审核安全制度合规性，如确保数据处理符合《数据安全法》，同时在安全事件发生时提供法律支持，三者形成“技术+业务+法律”协同闭环，覆盖安全管理全流程。（2）网络安全管理员作为医院网络安全第一责任人，统筹安全战略规划，如制定年度安全预算、推动零信任架构落地；协调跨部门资源，当出现系统漏洞时，快速联动信息科修复、医务部调整临时诊疗流程；定期向院领导汇报安全态势，提供风险预警与应对建议，同时代表医院对接外部监管机构，确保安全管理与行业要求同步。

3.2 政策与流程设计

（1）访问控制策略：严格遵循最小权限原则，根据岗位需求分配系统权限。例如门诊医生仅可访问接诊患者的病历数据，无法查看其他科室患者信息；护士仅拥有病人信息录入、生命体征上传权限，无修改诊断结论权限，同时设置权限定期复核机制，避免离职员工权限未回收引发安全风险。（2）供应商安全管理：在第三方服务合作中，将安全要求纳入SLA条款。例如要求云存储供应商提供AES-256加密证明、每年开展安全审计；对运维服务商实施准入审核，核查其人员背景、安全资质，明确数据泄露后的赔偿责任，降低第三方服务引入的安全隐患。（3）员工安全意识培训体系：建立分层培训机制，对技术人员开展深度攻防培训，对临床医护人员侧重数据保护规范讲解；定期组织钓鱼模拟测试，通过发送伪装成“医保通知”的钓鱼邮件，检验员工识别能力，对测试不合格者进行二次培训，从人员层面减少安全漏洞[5]。

3.3 合规与审计

（1）等保2.0三级要求落地路径：分阶段推进合规建设，第一阶段完成差距评估，对照等保2.0三级标准梳理现有系统不足，如是否满足“重要数据异地备份”要求；第二阶段实施整改，部署符合标准的安全设备、完善管理制度；第三阶段申请测评，通过第三方机构检测后，定期开展合规复查，确保持续满足等保要求。（2）内部审计流程：每月进行日志分析，调取系统访问日志、数据操作日志，排查异常行为，如非工作时间批量下载数据；每季度开展渗透测试，由内部安全团队模拟黑客攻击，寻找系统漏洞；每年进行全面审计，覆盖技术防护、制度执行、人员培训等维度，形成审计报告并

督促问题整改。（3）监管机构对接：指定专人负责与卫健委、网信办对接，按时报送安全自查报告、数据安全事件；在监管机构开展检查时，提供系统架构图、安全制度文件等资料，积极配合检查工作；及时传达监管新规，如数据分类分级管理要求，确保医院安全管理与监管政策保持一致。

4 医院信息系统网络安全的挑战与对策

4.1 当前面临的主要挑战

（1）物联网设备安全：可穿戴设备、智能药柜等物联网设备接入医院网络后，部分设备因硬件资源有限，缺乏完善的安全防护功能，易成为网络攻击突破口；且设备数量多、分布广，难以实现统一管理，增加了漏洞排查与风险管控难度，可能导致设备数据被窃取或设备被非法操控。（2）云医疗安全：采用SaaS模式的云医疗服务中，医院数据存储于第三方云平台，数据主权界定模糊，医院对数据的直接管控能力减弱；云平台若存在安全漏洞，可能引发数据泄露，同时跨地域数据传输也面临更多安全风险，对数据安全保障提出更高要求。（3）人工智能医疗应用伦理风险：人工智能医疗应用依赖大量医疗数据训练，数据采集与使用过程中可能侵犯患者隐私；AI决策的黑箱特性，使其诊疗建议缺乏透明解释，若因算法偏差导致诊疗失误，责任界定困难，引发伦理争议。

4.2 未来发展方向

（1）安全即服务（SECaaS）模式探索：将网络安全服务外包给专业服务商，医院无需投入大量资源建设和维护安全系统，可通过按需订阅的方式获取边界防护、威胁检测等服务，提升安全防护的专业性与灵活性，降低安全管理成本。（2）量子加密技术前瞻研究：量子加密技术基于量子力学原理，具有不可破解的特性，可应用于医疗数据传输与存储，从根本上解决传统加密技术可能被破解的问题，为医疗数据安全提供更强有力的技术保障，目前需进一步突破技术落地的成本与兼容性难题。（3）跨机构安全信息共享机制：建立医院间、医院与监管机构间的安全信息共享平台，实时共享网络攻击情报、漏洞信息等，使各机构能及时了解最新安全威胁动态，提前做好防御准备，形成协同防御体系，提升整体网络安全防护能力。

结束语

医院信息系统网络安全与管理是保障医疗行业稳健发展的基石。面对日益复杂的网络威胁，需持续强化技术防护，完善管理体系，紧跟安全技术发展趋势，积极应对物联网、云医疗等新兴领域带来的挑战。唯有如此，才能为患者隐私筑牢防线，确保医疗业务连续稳定运行。未来，各方应携手共进，推动安全信息共享与协同防御，构建更加安全可靠的医疗网络环境，为公众健康事业提供坚实保障。

参考文献

[1]齐丽,娄中鑫.医院信息化建设中的网络安全与防护探讨[J].电脑校园,2023(7):72-73.

[2]许顺生.医院信息系统的管理与网络安全[J].科学与信息化,2023(6):159-161.

[3]周扬.医院信息系统的网络安全与威胁应对[J].电子乐园,2023(3):34-36.

[4]张敬国.医院信息系统的网络安全维护措施[J].集成电路应用,2023,40(2):156-157.

[5]时亚松.医院信息化建设中的网络安全管理与维护[J].中国信息界,2024(2):84-85.