浅谈医院信息安全建设

王 博 吴思嘉 段张星*
宁夏医科大学总医院 宁夏 银川 750000

摘 要：医院信息安全建设对保障医疗行业稳定运行与患者权益意义重大。本文阐述了医院信息安全建设的核心内涵与目标，从信息系统、数据、网络三方面剖析核心内容，分析技术、管理、人员层面面临的核心挑战，并从技术保障、管理优化、人员培育三方面提出实施路径，为医院信息安全建设提供全面参考，提升医院信息安全水平，保障医疗业务顺利开展。

关键词：医院信息安全；建设挑战；实施路径；防护体系

引言：医疗信息化进程的加速使医院信息系统承载大量敏感医疗数据，其安全性关乎患者权益、医院声誉及医疗行业稳定。然而，医院信息安全建设面临诸多挑战，技术上系统复杂、新兴技术引入新风险；管理上制度不完善、监管不力；人员上意识与技能参差不齐。在此背景下，深入探讨医院信息安全建设，明确建设方向与路径，对提升医院信息安全防护能力具有重要意义。

1 医院信息安全建设的核心内涵与核心目标

1.1 医院信息安全建设的核心内涵

医院信息安全建设是保障医疗行业稳定运行与患者权益不受侵害的关键环节。从技术层面看，涵盖网络架构安全、数据存储安全、应用系统安全等多个维度[1]。网络架构安全要求构建稳固可靠的网络拓扑，防止外部非法入侵与内部信息泄漏，确保医疗数据在网络传输过程中的完整性与保密性。数据存储安全强调对海量医疗数据进行加密处理，采用先进的存储技术与管理机制，避免数据因硬件故障、自然灾害或人为失误而丢失损坏。应用系统安全聚焦于各类医疗业务系统，如电子病历系统、医院信息管理系统等，通过身份认证、访问控制等手段，保障系统仅被授权人员使用，防止恶意攻击与非法篡改。从管理层面讲，涉及信息安全制度建设、人员安全意识培养等方面。完善的信息安全制度为医院信息安全提供行为准则与规范指引，明确各部门与人员在信息安全保障中的职责与义务。人员安全意识培养则通过定期培训与教育，提升全体员工对信息安全重要性的认识，使其在日常工作中自觉遵守安全规定，减少因人为疏忽引发的安全风险。

1.2 医院信息安全建设的核心目标

医院信息安全建设的核心目标在于全方位保障医疗信息资产安全。确保医疗数据在生命周期内的保密性，防止敏感信息如患者个人隐私、疾病诊断结果等被非法获取与利用。这要求医院采用先进的加密技术对数据进行加密，同时加强对数据访问的管控，只有经过授权的人员才能访问相关数据。维护数据的完整性，保证数据在存储、传输与处理过程中不被篡改、破坏，为医疗决策提供准确可靠依据。医院要建立数据完整性校验机制，对数据进行定期的完整性检查，及时发现数据是否被篡改。保障数据的可用性，使医疗业务系统在任何时候都能正常运行，医护人员能够及时获取所需信息，为患者提供及时有效的医疗服务。医院需建立完善的系统监控与维护机制，实时监测系统的运行状态，及时处理系统故障，确保系统的可用性。通过信息安全建设，提升医院应对信息安全事件的能力，降低安全事件对医院正常运营的影响，维护医院的声誉与社会形象，促进医疗行业的健康有序发展。医院要制定完善的应急预案，定期进行应急演练，提高应对信息安全事件的能力，减少事件造成的损失。

2 医院信息安全建设的核心内容

2.1 信息系统安全建设

医院信息系统作为医疗业务运转的核心支撑，其安全建设至关重要，它犹如医院信息大厦的坚固框架，支撑着整个医疗流程的有序开展。一旦信息系统出现安全问题，将导致挂号、诊断、治疗等环节陷入混乱。该建设涵盖硬件、软件及系统运行环境等多个层面[2]。硬件方

作者简介：王博，男，1988年12月，本科，中级，研究方向：医院信息运维；邮箱：408859461@qq.com

作者简介：吴思嘉，男，1986年8月，本科，中级，研究方向：医院信息系统的管理和运维，邮箱：51289073@qq.com

通讯作者：段张星，男，1989年5月，本科，初级，研究方向：计算机，邮箱：112442904@qq.com

面，要确保服务器、存储设备等关键基础设施具备高可靠性与稳定性，采用冗余设计、定期维护等手段，降低硬件故障对系统运行的影响。软件层面，操作系统、数据库管理系统等基础软件需及时更新补丁，修复已知安全漏洞，防止恶意软件入侵。各类医疗业务应用软件，如电子病历系统、医院信息管理系统等，要严格遵循安全开发规范，进行安全测试与代码审查，避免软件存在安全缺陷。系统运行环境安全则涉及机房的物理安全，包括门禁系统、监控设备、消防设施等，保障机房环境符合安全标准，防止非法人员进入与自然灾害破坏。此外，信息系统安全建设还需建立完善的系统监控与审计机制，实时监测系统运行状态，记录用户操作行为，及时发现异常情况并采取应对措施，确保信息系统安全稳定运行，为医疗业务提供可靠保障。

2.2 数据安全建设

医疗数据包含患者个人隐私、疾病诊断、治疗方案等敏感信息，这些信息是患者的生命密码，数据安全建设不仅关乎患者的个人权益，更影响着医院的声誉和社会的稳定。一旦数据泄露，将给患者带来巨大的伤害。数据安全建设是医院信息安全建设的重中之重。数据保密性方面，采用加密技术对数据进行加密处理，无论是存储在数据库中还是传输在网络上，都确保数据以密文形式存在，防止数据被非法窃取与解读。数据完整性方面，运用数字签名、哈希算法等技术，对数据进行完整性校验，保证数据在传输与存储过程中不被篡改、破坏，维持数据的原始状态。数据可用性方面，建立数据备份与恢复机制，定期对重要数据进行备份，并将备份数据存储在安全可靠的位置，当数据遭受损坏或丢失时，能够迅速恢复数据，确保医疗业务的连续性。同时加强数据访问控制，根据用户角色与权限，严格限制对数据的访问，只有经过授权的用户才能访问相应数据，防止数据泄露与滥用。

2.3 网络安全建设

医院网络连接着内部各个部门与外部医疗机构、医保部门等，它是医院信息交互的神经脉络，网络安全建设是保障医院与外界信息畅通、协同合作的关键。若网络安全出现问题，将阻碍医疗资源的共享和患者的及时救治。网络安全建设关乎医院信息流通的安全与顺畅。构建安全可靠的网络架构，采用防火墙、入侵检测系统、虚拟专用网络等技术，对网络边界进行防护，阻止外部非法网络流量进入医院内部网络，防止网络攻击与恶意软件传播。加强无线网络安全管理，对无线网络进行加密认证，设置访问密码与访问权限，防止未经授权的设备接入无线网络，保障无线网络环境的安全。定期对网络设备进行安全检查与维护，更新设备固件，修复安全漏洞，确保网络设备正常运行。此外，开展网络安全培训与教育，提高医院全体员工的网络安全意识，使其了解常见的网络安全威胁与防范措施，在日常工作中自觉遵守网络安全规定，共同维护医院网络安全。

3 医院信息安全建设面临的核心挑战

3.1 技术层面的挑战

医院信息安全建设在技术层面遭遇诸多难题。随着医疗信息化进程加快，医院信息系统日益复杂，涵盖电子病历、医疗影像、远程医疗等多个子系统，各系统间数据交互频繁，这给安全防护带来巨大压力[3]。不同系统采用的技术架构、开发语言存在差异，安全标准难以统一，导致安全漏洞难以全面排查与修复。新兴技术如物联网、云计算在医疗领域的应用，虽提升了医疗服务效率，却也引入新的安全风险。物联网设备数量众多、分布广泛，部分设备安全防护能力弱，易成为攻击入口，引发数据泄露或系统瘫痪。云计算环境下，数据存储在云端，医院对数据的控制权减弱，数据隐私保护面临挑战，如何确保云服务提供商遵守安全规范、保障数据安全成为亟待解决的问题。此外，网络安全威胁不断演变，黑客攻击手段日益多样化、智能化，如分布式拒绝服务攻击、零日漏洞攻击等，传统安全防护技术难以有效应对，需要不断更新升级安全设备与技术，以跟上安全威胁的发展步伐。

3.2 管理层面的挑战

医院信息安全管理体系的完善与执行存在一定困难。信息安全制度建设方面，部分医院虽制定了一系列安全制度，但制度内容不够细致全面，缺乏针对性和可操作性，无法有效指导实际工作。制度更新不及时，不能适应医疗信息化发展的新需求与新变化，导致制度形同虚设。在安全策略制定上，缺乏整体规划与统筹协调，各部门各自为政，安全策略存在冲突与漏洞，无法形成有效的安全防护合力。安全监管方面，医院内部安全监管机制不健全，监管力度不足，对信息安全违规行为的处罚力度不够，难以形成有效的威慑。同时，与外部监管机构的沟通协作不够顺畅，不能及时获取最新的安全监管要求与信息，导致医院信息安全管理工作滞后。

3.3 人员层面的挑战

医院工作人员信息安全意识与技能水平参差不齐，给信息安全建设带来阻碍。部分医护人员对信息安全重要性认识不足，在日常工作中随意泄露患者信息、使用弱密码、点击不明链接等，增加了信息泄露风险。技术人

员虽具备一定专业技能，但面对不断变化的安全威胁，知识更新速度跟不上，缺乏应对新型安全问题的能力。医院对员工的信息安全培训不够系统全面，培训内容缺乏针对性与实用性，培训方式单一，导致员工参与培训的积极性不高，培训效果不佳。此外，医院人员流动频繁，新入职员工对医院信息安全制度与流程不熟悉，需要花费大量时间与精力进行培训与适应，在这期间容易出现信息安全漏洞。

4 医院信息安全建设的实施路径

4.1 技术保障路径

技术保障是医院信息安全建设的核心支撑，需围绕信息系统与数据全生命周期防护构建多层次技术体系。搭建专业化数据安全管理平台，集成人工智能、机器学习等前沿技术，整合各类安全防护组件，实现对医院信息的全方位监测与管控[4]。部署网络安全管理与态势感知平台，配套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，通过自动化日志收集与实时分析，快速识别潜在安全威胁并生成预警，为安全事件应急处理提供支撑。采用动态加密技术与安全协议，保障数据传输过程中的保密性与完整性，配置基于角色和权限的访问控制策略，防范未经授权的访问与操作。建立完善的日志监控和审计系统，实时追踪网络活动，结合安全漏洞扫描和定期渗透测试，持续提升网络防护能力。对医院数据进行科学分类分级，依据相关行业指南标准划分数据级别，针对不同级别数据采取差异化防护策略，强化敏感数据脱敏处理，筑牢数据存储、传输、使用各环节的安全防线。

4.2 管理优化路径

管理优化是医院信息安全建设的重要保障，需立足全生命周期管理理念，构建系统化管理架构。完善医院信息安全顶层设计，明确数据管理部门、业务部门、信息化部门在安全管理中的权责，落实安全责任分工，形成权责清晰、协同高效的管理格局。建立健全信息安全管理制度与操作规程，结合医院业务模式变更及时修订完善，确保制度的有效性与协同性，将总体安全策略拆解为具体管理要求，融入日常运营各环节。构建融合管理、技术、运营三位一体的立体化网络安全管理模式，推动安全管理与业务工作深度融合，形成“实战化、体系化、常态化”的安全防护态势。建立防护、监测、处置、保障四个体系协同的综合防控格局，强化安全检查与监督管理，制定完善的应急预案，推动联防联控机制落地，确保安全事件得到快速有效处置，持续提升信息安全管理的规范化水平。

4.3 人员培育路径

人员培育是医院信息安全建设的基础环节，需围绕安全意识提升与专业能力培养构建全方位培育体系。将信息安全培训纳入医院常态化工作，覆盖全体工作人员，重点普及数据安全防护知识、网络安全风险常识及相关操作规范，提升工作人员的安全防范意识，引导工作人员自觉遵守安全管理制度。针对信息安全管理人员、技术运维人员开展专业化培训，聚焦数据安全管理、网络安全防护、安全事件处置等核心内容，提升专业技术能力与应急处置水平，满足医院信息安全建设的技术需求。建立健全人员考核机制，将信息安全工作表现纳入工作人员考核范围，强化考核结果运用，以此激励工作人员更加积极主动地重视并做好信息安全工作[5]。加强与行业内专业机构的交流合作，引进先进培育理念与技术经验，开展常态化学习交流活动，持续更新工作人员的知识体系，打造一支专业素养过硬、安全意识突出的信息安全队伍，为医院信息安全建设提供人力支撑。

结束语

医院信息安全建设是一项长期且复杂的系统工程，关乎医疗行业的健康发展。通过技术保障、管理优化和人员培育等多维度实施路径，能够有效应对当前面临的挑战，构建起全方位、多层次的信息安全防护体系。这不仅有助于保障医疗信息资产安全，还能提升医院应对信息安全事件的能力，维护医院的正常运营秩序，为患者提供更加安全可靠的医疗服务。

参考文献

[1]倪敏杰.数字化环境下医院信息安全建设分析[J].城市情报,2022(18):82-84.

[2]耿辉,于春霞.医院档案信息化建设中的信息安全管理现状及对策[J].中国卫生产业,2024,21(7):148-151.

[3]杨虹.医院档案信息化建设中信息安全管理分析[J].黑龙江档案,2024(1):237-239.

[4]黄娟,黄小明.医院信息化建设中的信息安全问题与应对分析[J].网络安全技术与应用,2025(2):123-125.

[5]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.