医院电子信息系统面临的安全问题分析

李　青

（郓城县黄泥冈镇卫生院，山东　菏泽　274702）

摘　要：随着信息技术的快速发展，医院电子信息系统在提升医疗服务效率方面发挥了重要作用，同时为患者管理、病历存储和资源分配等领域提供了有力支持。然而，这些便利的背后也暴露出诸多安全隐患，例如患者隐私泄露、数据完整性威胁以及系统运行不稳定可能导致关键服务中断等问题。这些安全挑战不仅影响医护人员的日常工作，也直接危及患者的就医体验与生命安全。基于此，本研究围绕医院电子信息系统展开深入探讨，以其核心特点为切入点，详细分析当前主要安全风险，并结合实际案例提出针对性的解决方案。通过总结经验与教训，本研究旨在为未来医院的信息化建设提供科学支持与实践指导。

关键词：医院；电子信息系统；安全问题

中图分类号：TP309; R197.3　　**文献标志码：**A

Hospital Electronic Information System Security Issues Analysis

LI Qing

（*Huangni Gang Town Health Center*, *Yuncheng County*, *Heze* 274702, *China*）

Abstract: With the rapid development of information technology, hospital electronic information systems have played a crucial role in improving medical service efficiency, providing strong support for patient management, medical record storage, and resource allocation. However, behind these conveniences, numerous security risks have emerged, such as patient privacy breaches, threats to data integrity, and system instability that may lead to critical service disruptions. These security challenges not only affect the daily work of medical staff but also directly jeopardize patients' care experience and even their lives. Based on this, this study conducts an in-depth investigation into hospital electronic information systems, analyzing the major current security risks from the perspective of system characteristics, and proposes targeted solutions supported by real-world cases. By summarizing experiences and lessons, this research aims to provide scientific support and practical guidance for future hospital information system construction.

Keywords: hospital; electronic information system; security issues

0　引言

医疗行业的信息化正在以惊人的速度席卷全球。这一趋势不仅深刻改变了医院的日常运作模式，还为患者享受优质医疗服务提供了强有力的技术支持。在现代医院中，电子信息系统有效整合了患者管理、诊疗记录和药物分发等核心功能，大幅提升了工作效率，同时使医务人员能够将更多精力投入病患护理中。

然而，随着医院对电子信息系统依赖程度的持续加深，其所承载的数据价值也随之显著增加。与此同时，黑客攻击频率不断上升，内部数据泄漏事件屡见不鲜，而数据丢失或遭篡改的问题更是给许多医院带来极大的安全隐忧。因此，尽管数字化转型为医疗行业注入了新的活力，但由此引发的挑战亦不容忽视。

收稿日期：2025-12-04

作者简介：李青（1977.11—），女，汉族，山东郓城人，大专，助理工程师，主要研究方向为电子信息工程。

1　医院电子信息系统的特点

1.1　高集成性

在现代医疗体系中，高效的信息流转已成为提升诊疗质量的重要保障，而医院电子信息系统正是这一过程的坚实支撑。其中，“高集成性”是其最显著且最具价值的特征。该系统由多个子模块协同构建，包括门诊挂号、住院管理、药品供应链、实验室信息管理（LIMS）以及影像存储与通信（PACS）等。这种高度整合不仅实现了数据在各环节间的共享，还提高了整体运行效率。可以说，高集成性的医院电子信息系统既是现代医疗发展的重要成果，也是推动健康服务持续进步的关键力量[1]。

1.2　数据敏感性

电子信息系统处理的数据在医疗行业具有极高的敏感性。这些数据不仅涉及患者隐私，还关乎其健康状况等脆弱信息。从姓名、身份证号码到联系方式，这些基础数据常与详细的健康资料紧密相关，如病史记录、诊断结论、生物样本检测报告等。一旦这些数据泄露，患者可能面临难以估量的困

扰，甚至陷入舆论攻击或财产安全威胁。对医院而言，这不仅会损害声誉，还可能引发法律责任。因此，加强数据保护是医院运营中的核心任务之一。

1.3 实时性要求

相较于传统企业 IT 应用，医院电子信息系统对实时性的要求更加严苛。这并非仅出于效率提升的考量，更因为它直接关系到患者生命安全。在急救中心，每一次突发事件都可能带来大量伤员，这需要信息系统迅速接收并处理分流指令；在手术室，高效调配器械资源常常决定紧急手术是否顺利；而在重症监护室（ICU），生理参数监控必须保持精准稳定，以便医护人员及时应对病情变化[2]。此外，为确保系统始终处于最佳状态，不间断地进行更新和修补成为必要工作。然而，如果更新过程中出现疏漏，潜在风险可能被进一步放大。

2 医院电子信息系统面临的安全问题

2.1 外部攻击威胁

近年来，医院信息系统正面临前所未有的挑战。一系列外部网络攻击不仅显著改变了医疗行业的运行轨迹，还将患者和医务工作者暴露在潜在风险中。勒索软件、分布式拒绝服务攻击（DDoS）以及数据窃取等威胁，严重干扰了医院业务的正常运转，并直接危及患者的生命与健康。

以 DDoS 攻击为例，这类破坏手段通过大量消耗网络资源，使线上挂号、远程问诊等现代医疗服务瞬间瘫痪。依赖在线平台接受治疗或进行特殊预约的患者可能因此遭遇延误，甚至错失最佳诊疗时机。此外，针对敏感医疗数据的窃取行为则更加隐蔽且复杂。一些黑客组织利用先进技术非法获取患者隐私，用于敲诈勒索或牟取不法利益[3]。

2.2 内部威胁因素

许多医务人员由于缺乏足够的信息安全意识，在日常操作中容易产生风险。例如，一封错发的邮件可能泄露患者隐私；随手点击恶意链接可能引发网络攻击；轻信同事并泄露账户密码，则进一步放大了安全隐患。同时，共享账号虽然带来便利，但使责任追溯变得十分困难。

更复杂的问题还包括一些内部人员出于经济利益或个人矛盾而实施恶意行为。例如，有员工利用职务之便出售患者数据获利，也有人因离职纠纷采取报复性措施，通过破坏系统功能影响医院正常运行。当权限管理机制存在漏洞，高权限用户滥用职权访问敏感数据，则会加剧数据泄漏与安全失控的问题。

2.3 设备漏洞与更新滞后

医院电子信息系统由大量软硬件设备组成，这些设施共同支撑着现代医疗服务。然而，复杂设备中潜藏的安全隐患不容忽视，其中漏洞管理是最突出的问题。无论是操作系统、医学影像服务器，还是专用应用程序，每一环节都可能存在潜在威胁。

一些关键设备由于需要全天候运转以保障日常诊疗，很难腾出时间进行补丁更新。这种情况使它们长期暴露在已知漏洞之下，为网络攻击提供了可乘之机。此外，那些已停止厂商支持的老旧设备风险更高，因为无法获取必要的安全补丁，只能继续带着缺陷运行[4]。

2.4 第三方供应链风险

随着数字化生态体系愈发复杂，医院的信息安全正面临严峻挑战，其中尤以第三方供应链风险为甚。云服务提供商、IT 维护公司和软件开发商等外部合作伙伴虽然是医院数字化运转的重要组成部分，却也可能成为潜在的安全隐患。一旦第三方遭到网络攻击，其维护的接口或工具可能被植入恶意代码，从而波及整个医院信息系统。

此外，那些未经严格审查的小型供应商，其产品质量参差不齐，不仅容易引发兼容性问题，还可能隐藏无法察觉的安全漏洞，例如导致系统崩溃或数据泄漏。这些问题在高负荷运行环境下尤其容易爆发，不但会拖延医院日常工作效率，还可能直接影响患者诊疗。同时，多供应商协作模式虽然提高了运营效率，但也因沟通协调上的复杂性显著增加了管理成本。

3 医院电子信息系统安全问题的解决措施

3.1 提升外部防御水平

首先，在面对外部网络威胁时，应构建坚固且灵活的防御体系。部署高性能防火墙与入侵检测 / 预防系统（IDS/IPS），结合深度包检测（DPI）技术，能够有效识别并拦截潜在的恶意流量。这些技术不仅是冷冰冰的软件工具，更是保护患者隐私和诊疗数据的重要屏障。此外，为应对 DNS 劫持等复杂攻击，引入 DNS 安全扩展协议（DNSSEC）能够进一步提高域名解析过程中的安全性，为整个网络通信提供额外一层保障[5]。

其次，加强数据保护。在传输和存储阶段，全程加密是确保敏感信息不被非法窃取的关键手段。在传输环节，通过引入超文本传输协议安全版（HTTPS）或虚拟专用网（VPN），可以有效避免黑客利用数据包截获漏洞进行攻击。而在存储端，采用强密码学算法加密数据库并定期更换密钥，不仅能降低破解风险，还能显著增强系统整体抗风险能力。

最后，针对日益严峻的勒索软件威胁，制定完善的数据备份策略尤为重要。一旦核心系统瘫痪，将严重影响医院正常运作，甚至危及患者救治。因此，通过定期生成离线备份副本，并结合冗余存储设计，即使主系统遭受损害，医院也能迅速恢复业务连续性。

3.2 应对内部威胁

安全计算环境防护需考虑整个医院业务网络的安全架构和策略部署。例如，最基础的内部网络区域划分及 IP 地址分配，应根据医院业务网络规模较大、内部业务系统繁多等情况，在网络架构及规划时根据重要性等因素进行合理的构建，并前瞻性地将后期网络扩建等纳入考量范围，这将在安全防护策略制定上带来极大的便利性，可能节约很多网络安全建设开支。

首先，采用基于角色的访问控制模型（Role-Based Access Control, RBAC），通过精准划分权限，让每位用户仅访问与其工作相关的信息资源。这种方法不仅降低了因权限滥用导致的潜在风险，还为数据管理搭建了更合理的规则框架。在此

基础上，引入零信任架构尤为关键。零信任理念强调“不盲信任何用户或设备”，即使是来自内部的访问请求，也需经过身份验证和授权审核等多重步骤，以确保每次操作都得到严格把控[6]。

其次，定期组织员工培训有助于全面提升医护人员的数据安全意识。例如，通过模拟钓鱼邮件测试，提高其识别可疑链接或附件的能力；同时普及社会工程学知识，从心理层面帮助员工了解网络攻击者常用手段。

最后，引入行为监测工具是一项高效策略。通过记录和分析用户操作日志，一旦发现异常登录或未经授权的数据导出等可疑行为，可以实时触发警报并迅速采取阻断措施。此外，借助机器学习算法预测违规行为可能性，为管理层制定更加全面、主动的应对计划提供支持。

3.3 及时更新并修补漏洞

首先，需要制定一套全面、可靠的漏洞管理政策。在网络安全防护设计方面，针对现有的网络架构，采用防入侵、控流量、阻攻击、限访问、扩冗余的网络安全防护措施，构建多层次的网络防护机制，保障信息平台的网络安全以及数据交互业务的稳定性。在数据安全防护设计方面，根据该平台的特点，在数据传输、数据存储、日志审计三个方面进行数据安全防护方案设计。在系统安全防护设计方面，每年至少进行 1 次与平台数据交互的业务系统的安全基线核查、主机漏洞扫描、应用漏洞扫描以及渗透测试等安全扫描，并出具对应的整改报告。可以借助自动化扫描工具（例如 Nessus 或 OpenVAS），对所有联网设备及应用程序进行定期检测，并生成详细报告以便后续分析。同时，与厂商保持密切合作也不可忽视。通过追踪官方补丁发布动态并及时评估其影响范围，可以最大限度地降低潜在风险。

在完成初步评估后，还需对补丁安装过程进行充分测试，以避免升级引发新的兼容性问题。例如，可以搭建一个独立测试环境，用于模拟生产场景并验证新版本运行效果；或者采用蓝绿部署方式，让新旧版本同时运行，直至确认无误再完全替换。对于短期内无法彻底修复的问题，可采取临时缓解措施以争取解决时间。例如，如果某功能模块存在已知漏洞且暂时无法更新，可选择关闭该模块，或调整默认配置参数以规避危险区域。此外，为防止延误造成进一步损失，应尽快启动替代方案开发工作，并加速完成迁移流程，从根本上消除隐患。

最后，在应对紧急情况时，必须制定完善的事件响应计划。当严重漏洞被黑客利用而尚无正式修复手段时，与行业伙伴共享情报尤为关键。这种合作不仅能缩小攻击的影响范围，还能够帮助快速恢复正常服务水平。

3.4 重视第三方供应链风险处理

在选择合作伙伴时，医院应进行全面而详尽的背景调查，以构建坚实的第一道防线。例如，评估合作方是否具备丰富的项目经验，以及其在应对突发安全事件时的反应能力是否迅速可靠。

此外，与第三方签订详细的数据保密协议和明确责任范围的服务等级协议，是保障数据安全和规范双方合作的一项必要措施[7]。然而，仅在初期完成筛选是不够的。在长期合作中，对第三方系统和服务进行持续监督。比如，医院可以定期开展渗透测试，以识别外部组件引入后可能出现的潜在漏洞；要求供应商提交软件开发生命周期相关报告，包括代码审核结果和安全测试记录，从源头提升系统整体安全性。

当然，即便事先采取了充分准备工作，也无法完全规避所有意外情况。因此，为降低供应链中断可能引发的业务冲击，制定完善的灾备计划至关重要。例如，当核心设备或关键服务因故障停运时，应具备迅速切换至备用方案的能力。减少医疗流程受到的不良影响，还能确保患者获得连续且高质量的医疗服务。

4 结 语

综上所述，医院电子信息系统在为医疗行业注入活力、提升效率的同时，也不可避免地暴露出多种安全隐患。这些问题不仅涉及患者数据的保密性，还直接影响医疗机构的正常运转，甚至关乎社会公共安全。为了建立稳固可靠的信息体系，医院需从以下几个方面采取措施：首先，应加强外部防御，例如优化网络防火墙和升级反病毒软件；其次，要完善内部管理制度，通过精细化权限分配和规范操作流程等手段减少人为失误；还需定期开展漏洞排查，并对供应链环节进行严格监控，以最大限度降低风险。

参考文献：

[1] 林涛 . 电子信息工程系统在医院管理中的应用探析 [J]. 工程建设与设计 ,2024,(14):92-94.

[2] 霍学勇 , 丁军 . 数字化医院电子信息系统的设计要点与优化路径探析 [J]. 中国战略新兴产业 ,2024,(11):63-65.

[3] 徐扬凯 . 电子信息技术在医院信息化系统中的运用 [J]. 集成电路应用 ,2023,40(01):309-311.

[4] 郑树军 , 周波 . 医院管理信息系统中电子信息技术的应用 [J]. 长江信息通信 ,2022,35(03):176-178.

[5] 张广文 . 电子信息技术在医院管理信息系统中的应用探究 [J]. 网络安全技术与应用 ,2022,(03):108-109.

[6] 陈云 . 数据技术在医院信息管理系统中的运用分析 [J]. 软件 ,2021,42(12):86-88.

[7] 仲宇 . 电子信息工程系统在医院管理中的应用探析 [J]. 中国设备工程 ,2021,(18):49-50.