 DOI: https://doi.org/10.12349/iser.v6i3.5189

Research on Medical information security Risk Assessment and protection system construction—from the perspective of hospital information Department

Yabin Yuan

Department of Information, the Third People's Hospital of Fuyang City, Fuyang, Anhui, 236015, China

Abstract

With the rapid development of information technology, medical informatization plays an important role in improving the quality, efficiency and management level of medical services. However, the security of medical information has increasingly become the focus of the industry. As the core department of medical information management, hospital information department faces huge security risks. Based on the information security problem of hospital information department, this paper discusses the evaluation method of medical information security risk and the strategy of protection system construction. Firstly, this paper analyzes the characteristics and risks of medical information security, then puts forward an effective risk assessment model, and discusses the key points of information security protection system based on the actual situation of hospital information department. The research shows that the hospital information department should combine the innovation of information technology, establish a sound security protection mechanism, strengthen information security awareness education, improve the overall level of information security management, ensure the security of patient data, and protect the continuity and reliability of medical services.

Keywords

medical information security; risk assessment; protection system; hospital information department; information security management

医疗信息安全风险评估与防护体系建设研究——以医院信息科为视角

苑亚彬

阜阳市第三人民医院信息科，中国 · 安徽 阜阳 236015

摘　要

随着信息技术的快速发展，医疗信息化在提高医疗服务质量、效率和管理水平方面发挥着重要作用。然而，医疗信息的安全性问题也日益成为行业关注的焦点，医院信息科作为医疗信息管理的核心部门，面临着巨大的安全风险。本文围绕医院信息科的信息安全问题，深入探讨了医疗信息安全风险的评估方法与防护体系建设的策略。首先分析了医疗信息安全的特点与风险，随后提出了有效的风险评估模型，结合医院信息科的实际情况，探讨了信息安全防护体系的构建要点。研究表明，医院信息科应当结合信息技术的创新，建立健全的安全防护机制，加强信息安全意识教育，提升信息安全管理的整体水平，确保患者数据的安全，保护医疗服务的持续性和可靠性。

关键词

医疗信息安全；风险评估；防护体系；医院信息科；信息安全管理

1 引言

在现代医疗行业中，信息技术的应用日益普及，医院信息化建设成为提升医疗服务质量的重要手段。医疗信息系统通过电子化的方式存储、管理和共享患者的个人健康信息、诊疗记录及医院运营数据，不仅提高了医疗效率，也促进了医疗资源的优化配置。[1]然而，随着信息化进程的加速，医疗信息的安全问题逐渐凸显，医院信息科作为医院信息系统的核心管理部门，承担着信息安全保障的重要责任。

医疗信息安全的核心在于保护患者个人信息的隐私性和安全性，防止医疗数据遭到泄露、篡改或丢失。医疗信息系统通常涉及多个部门、人员及设备的协同工作，这使得其面临的安全风险复杂多样，涵盖了系统漏洞、数据泄露、网络攻击、恶意软件等多个方面。医院信息科需要不断提升安全防护能力，加强对信息安全风险的评估和管理，确保医疗信息系统的正常运行和患者信息的安全。

本文旨在从医院信息科的视角出发，分析医疗信息安

【作者简介】苑亚彬（1979–），男，中国安徽界首人，本科，工程师，从事医院信息安全研究。

全的风险评估方法，提出相应的防护体系建设策略，旨在为医院信息安全管理提供理论指导和实践参考，推动医疗信息安全工作的进一步落实。

2 医疗信息安全风险评估的背景与意义

2.1 医疗信息安全的背景

随着信息技术的不断进步，医疗行业的数字化、网络化进程加速，电子病历、医疗影像数据、药品管理系统等重要信息已实现全面电子化。在这种背景下，医院信息科肩负着管理和保护海量医疗数据的重任，然而，随着信息系统的广泛应用，信息安全问题也日益严重。医疗信息一旦泄露或遭到篡改，可能对患者的健康和医院的声誉造成不可估量的损失。

医疗信息系统的安全性不仅关系到患者个人信息保护，还与医疗服务的可靠性和医院的运营效率密切相关。为了保障信息系统的正常运行和数据的安全，医院信息科必须建立起完善的安全管理体系，并进行定期的风险评估，以提前识别潜在的安全隐患，防止信息安全事件的发生。[2]

2.2 医疗信息安全风险评估的意义

信息安全风险评估是指通过对医院信息系统的安全状态进行全面、系统地评估，识别潜在的安全风险，分析可能带来的后果，并采取相应的防护措施。进行风险评估的核心目的是通过科学的方法识别信息系统中的脆弱环节，进而制定合理的安全防护策略，确保医院信息系统的安全性和稳定性。对于医院信息科来说，进行信息安全风险评估具有深远的现实意义。

首先，风险评估能够有效识别医院信息系统中存在的安全漏洞和潜在威胁。随着医院信息系统的日益复杂，涉及的数据种类和数量也不断增加，包括患者的个人信息、病历、检查结果、诊疗记录等敏感数据，任何一次数据泄露或篡改都可能给患者和医院带来严重的后果。因此，医院信息科必须定期进行安全风险评估，发现系统中可能存在的薄弱环节，如系统漏洞、不完善的权限管理、数据加密缺陷等问题。[3] 通过提前识别这些潜在的安全威胁，医院能够采取有效的预防措施，减少安全事件的发生概率，避免重大安全事件的发生。

其次，风险评估帮助医院制定符合实际情况的信息安全防护策略。通过全面的风险评估，医院能够清晰地了解其信息系统的安全状况，明确哪些领域的安全防护措施不够到位，哪些环节可能存在更高的风险。例如，评估可能揭示出网络安全、数据备份、访问控制等方面的薄弱环节。基于这些评估结果，医院能够制定出更加科学、合理的信息安全防护策略，针对性地加强弱点，确保医院信息系统的整体安全性。同时，风险评估还为医院提供了应对突发安全事件的依据和方案，提升了医院信息安全管理的有效性。

最后，风险评估能够提升医院管理层对信息安全的重视程度，增强全体员工的信息安全意识。信息安全不仅仅是技术层面的问题，管理层的重视和全体员工的共同参与同样重要。通过定期开展信息安全风险评估，医院能够及时向管理层反馈信息安全状况，帮助管理层认识到信息安全的紧迫性和重要性，促进其为信息安全建设提供更多支持。同时，风险评估结果也可以作为信息安全培训的依据，帮助医院员工更好地理解信息安全管理的重要性，增强他们的安全意识和防护能力。通过全员参与，医院可以构建起良好的信息安全文化，推动医院信息安全管理体系的完善与发展。

总之，信息安全风险评估在医院信息科的安全管理工作中具有不可忽视的重要意义。通过风险评估，医院不仅可以识别和解决潜在的安全问题，还能提升信息安全管理水平，为医院的信息系统提供全面、持续的保护，确保患者数据的安全和医院服务的连续性与可靠性。

2.3 医疗信息安全风险的特点

医疗信息安全的风险具有独特的特点，这些特点使得医疗信息系统的安全管理比其他行业更加复杂和重要。首先，医疗信息系统涉及大量复杂且敏感的数据，包括患者的个人身份信息、病历数据、诊疗记录、药物使用情况、检验结果等，这些信息的安全性直接关系到患者的隐私权 [4]。如果这些敏感信息泄露或被篡改，不仅会严重侵犯患者的隐私，还会影响患者对医院的信任，甚至造成无法挽回的法律和社会后果。同时，医院的声誉也可能因此受到极大损害，患者流失、法律诉讼以及监管部门的处罚等后果可能会给医院带来沉重的财务和运营压力。

其次，医疗信息系统的安全风险具有多样性和复杂性。除去网络攻击、病毒、木马等技术性风险之外，医院信息系统还面临着来自人为操作失误、设备故障、数据备份不足等非技术性因素的威胁。

最后，医疗信息系统的安全风险具有动态性。随着信息技术的不断进步和新技术的应用，新的安全威胁不断涌现。为了应对这些不断变化的安全威胁，医院信息科必须不断监控和调整安全防护措施，持续更新技术手段，强化风险预警机制，以确保信息安全体系的有效性和可持续性。

3 医疗信息安全风险评估的实施方法

3.1 风险评估的基本步骤

医疗信息安全风险评估的基本步骤包括识别风险、分析风险、评估风险、制定防护对策和实施防护措施。首先，医院信息科需要对医疗信息系统的各个组成部分进行详细的风险识别，全面了解系统的结构、功能和应用范围，识别可能的安全风险。其次，通过对风险的定量分析和定性分析，评估各类风险的严重性和可能带来的后果，并对其进行优先级排序。接下来，医院信息科根据评估结果，制定针对性的防护对策，并通过技术手段和管理措施来降低风险的发生概率。最后，在实施防护措施后，医院信息科应定期进行风险

复评，确保信息安全防护体系的持续有效性。

3.2 风险评估模型的选择与应用

在进行医疗信息安全风险评估时，医院信息科可以选择适合自身信息系统特点的风险评估模型。常见的风险评估模型包括定量模型、定性模型和混合模型等。定量模型通过对安全风险的概率和影响进行量化评估，能够为决策提供科学依据。定性模型则通过专家评审、问卷调查等方式，结合主观判断对风险进行评估，适用于无法量化的风险评估。混合模型结合了定量和定性评估的优点，能够提供更加全面的风险评估结果。医院信息科应根据具体情况选择合适的评估模型，并结合实际开展评估工作。

3.3 风险评估的实施技术

为了提高风险评估的准确性和科学性，医院信息科可以采用多种技术手段进行支持。例如，数据挖掘技术可以帮助识别信息系统中的潜在安全威胁，自动化监控工具可以实时监测系统的安全状态，发现异常行为。安全漏洞扫描工具可以帮助检查信息系统中的安全漏洞，及时修补系统的薄弱环节。此外，医院信息科还可以借助专业的风险评估软件，帮助分析和预测信息安全风险，提供更加全面和系统的风险评估报告。[5]

4 医疗信息安全防护体系的建设

4.1 信息安全管理体系的建立

医疗信息安全防护体系的建设首先需要建立完善的信息安全管理体系。医院信息科应根据 ISO/IEC 27001 等国际标准，结合医院实际情况，制定信息安全管理制度。管理制度应包括信息安全政策、安全管理目标、信息安全职责、信息安全培训等内容，确保信息安全管理工作有序开展。此外，医院信息科还需要建立信息安全监控机制，定期进行安全检查，评估信息安全管理体系的有效性，及时发现并纠正管理中的漏洞。

4.2 技术防护措施的完善

信息技术手段是信息安全防护的核心，医院信息科应根据风险评估结果，采取针对性的技术防护措施。首先，医院信息科应加强对医院信息系统的访问控制，确保只有授权人员能够访问敏感数据。其次，应定期进行系统漏洞扫描和安全修复，确保系统不会因漏洞而受到攻击。同时，医院信息科应部署防火墙、入侵监测系统、数据加密技术等安全技术，防止恶意攻击和数据泄露。

4.3 人员培训与意识提升

信息安全不仅仅依赖于技术防护措施，人员的安全意识同样重要。医院信息科应定期组织信息安全培训，提高全体员工的安全意识，特别是对医护人员、行政人员等可能接触到患者敏感信息的人员进行专门的培训。通过培训，员工能够了解信息安全的重要性，掌握基本的安全操作规范，避免因人为失误导致信息泄露或系统故障。

5 医疗信息安全防护体系的实施效果与评价

5.1 实施效果的评估

医疗信息安全防护体系的实施效果应定期进行评估，医院信息科可以通过信息安全漏洞检查、系统安全性测试、员工安全行为评估等方式，检测防护措施的有效性。通过评估，医院可以及时发现防护体系中的不足之处，调整和完善安全措施。同时，医院信息科还可以通过与同行业的对比，了解自身防护体系的先进性和差距，不断提升安全防护水平。

5.2 持续优化的策略

随着信息技术的不断发展，新的安全威胁和漏洞不断出现，医疗信息安全防护体系的建设不能一蹴而就。医院信息科应定期对信息安全防护体系进行优化，及时引入新的安全技术和管理措施，以应对不断变化的安全风险。同时，应加强与外部安全机构的合作，获取最新的安全信息和技术支持，确保医院信息安全防护体系始终处于领先水平。

6 结语

医疗信息安全是保障医院正常运行和患者隐私的重要基石，医院信息科作为信息系统管理的核心部门，必须高度重视信息安全工作。通过有效的风险评估和科学的防护体系建设，医院能够识别潜在的安全隐患，采取针对性措施，确保医疗信息的安全性和完整性。随着信息技术的不断进步，医院信息科需要不断更新和优化安全管理体系，提升信息安全防护能力，为医疗服务的可持续发展提供坚实的保障。

参考文献

[1] 张新芳.病历档案研究成果的定量与定性分析——以《档案管理》载文为例[J].档案管理,2025,(01):119-124.

[2] 蒋百林.公立医院内部控制建设现状及完善措施研究[J].环渤海经济瞭望,2024,(12):19-22.

[3] 王淑,魏明月.数字化转型助力儿童友好型医院建设研究[J].中国数字医学,2025,20(01):1-7.

[4] 孟晓微,李岩,田霞,等.数据生命周期视角下健康医疗数据资产化研究[J].卫生经济研究,2025,42(02):28-31+36.

[5] 王云枫.浅探新医改制度下加强现代医院财务信息化建设的对策[J].乡镇企业导报,2024,(21):134-136.