

# 医院信息化建设中网络安全的维护策略研究

葛 奇

山东菏泽 274000

**摘 要：**随着电子信息技术的快速发展，医院信息化建设已成为医疗行业的重要趋势。同时，分析了电子信息技术在医疗服务流程优化中的作用，如远程医疗、移动医疗和医疗物联网等。此外，还讨论了医疗数据分析与决策支持系统中的电子信息技术，以及远程医疗服务中的电子信息技术。最后，强调了电子信息技术在医院信息化系统中的安全与隐私保护的重要性，并提出了相应的维护策略。

**关键词：**网络安全；医院信息；档案管理维护；系统

## 引言

电子信息技术在医疗领域的应用已经越来越广泛，它不仅改变了医疗服务的提供方式，也提高了医疗服务的效率和质量。本文将探讨电子信息技术在医院信息化系统中的应用，包括基础应用、医疗服务流程优化、医疗数据分析与决策支持系统、远程医疗服务以及安全与隐私保护等方面。电子信息技术在医院信息化建设中发挥着重要的作用，它可以优化医疗服务流程、提高医疗质量和效率、降低医疗成本。然而，电子信息技术在医院信息化建设中 also 面临着一些挑战，如网络安全威胁、数据隐私保护等。为了保障电子信息技术在医院信息化建设中的安全与有效应用，需要采取相应的安全策略和措施，同时加强法律法规和标准的制定和实施。

## 一、医院信息化建设中的网络安全挑战

### （一）医疗数据的敏感性和隐私保护需求

1. 医疗数据包含患者的个人信息、诊断记录等敏感信息，一旦泄露，将对患者的隐私造成严重侵犯。

2. 保护医疗数据的隐私和安全是医院信息化建设中的首要任务。

### （二）网络攻击手段的多样化与智能化趋势

1. 黑客攻击、恶意软件、网络钓鱼等网络攻击手段不断更新和演进，给医院网络安全带来巨大威胁。

2. 智能化的攻击手段，如人工智能驱动的网络攻击，增加了医院防范网络安全风险的难度。

## （三）医院网络系统的复杂性和设备多样性的安全隐患

1. 医院网络系统通常包含多个子系统，如 HIS、LIS、RIS 等，这些系统之间的交互和数据传输增加了网络安全风险。

2. 医院使用的各种医疗设备也可能存在安全漏洞，如移动医疗设备、医疗物联网设备等，需要加强安全管理。

## （四）医院信息化建设中的网络安全策略概述

### 1. 建立全面的网络安全管理体系

（1）制定完善的网络安全策略和管理制度，明确责任和流程。

（2）建立网络安全监控和预警机制，及时发现和处理安全事件。

### 2. 强化医疗数据的加密和访问控制机制

（1）对医疗数据进行加密处理，确保数据在传输和存储过程中的安全性。

（2）实施严格的访问控制策略，限制对医疗数据的访问权限。

### 3. 定期进行网络安全风险评估和漏洞扫描

（1）定期进行网络安全风险评估，发现潜在的安全隐患。

（2）及时修复漏洞，避免被黑客利用。

## （五）案例分析

医院信息化建设已成为医疗服务升级的重要手段。其中，网络安全维护策略的应用显得尤为重要。某大型综合性医院在信息化建设项目中，成功实施了一系列有效的网络安全措施，不仅保障了医疗数据的安全，还提升了医疗服务的质量和效率。

该医院信息化建设项目的核心目标是通过建立一个

**作者简介：**葛奇（1988.01——），男，汉族，山东省聊城人，本科学历，助理工程师，主要从事电子信息工程的研究工作。

全面、集成的电子健康记录系统（EHR），实现患者信息、诊断记录、药物管理等关键数据的即时访问和共享。为确保数据安全，项目团队特别成立了网络安全小组，专门负责规划和执行网络安全策略。小组与国内外网络安全专家合作，通过威胁建模、风险评估和漏洞扫描等手段，确定了可能的安全隐患。随后，他们采取了多层次防护措施，例如实施端到端加密技术、部署防火墙和入侵检测系统，并对所有医务人员进行了网络安全意识的培训。

在网络安全策略实施后，医院系统遭受网络攻击的次数显著减少，数据泄露事件几乎绝迹。通过实时监控和安全日志的分析，安全小组能够迅速响应潜在的安全威胁，并有效隔离和修复问题。此策略不仅提高了患者信息的保密性，还赢得了病患和医务人员的信任。信息化建设项目的成功，也使得医院在同行中树立了良好的口碑，吸引更多的患者前来就诊。

然而，该项目的实施并非一帆风顺。在项目早期，因医务人员对网络安全措施的不适应，一度出现了操作效率下降的情况。为此，医院加大了对医务人员的培训力度，优化了安全工具的用户界面，并在系统中引入了安全智能助手，简化了操作流程，提高了医务人员的接受度和操作的便捷性。

通过这个案例，其他医院可得到以下启示：首先，网络安全是信息化建设不可或缺的一部分，必须从项目初期就开始规划和实施；其次，结合专业力量和采用先进的技术手段，能有效提升网络安全防护能力；再次，医务人员的参与和适应是确保网络安全措施得以有效执行的关键；最后，应当持续关注网络安全技术的发展动态，及时更新和升级安全策略，以应对日益复杂的网络安全威胁。成功实施网络安全维护策略的医院信息化建设项目，不仅对医院自身的长期发展至关重要，也为整个医疗行业的安全信息化提供了宝贵的经验。

## 二、电子信息技术在医院信息化系统中的基础应用

电子信息技术在医院信息化系统中的基础应用主要包括电子病历系统、医疗设备管理系统、药品管理系统等。这些系统通过电子化的方式，实现了医疗服务的数字化、网络化和智能化，大大提高了医疗服务的效率和质量。

### （一）电子病历

电子病历是医院信息化建设的核心，它将患者的医疗信息数字化存储，便于医生查阅和管理。电子病历系统不仅提高了医疗效率，还减少了医疗错误的发生。

### （二）医疗设备管理

医疗设备管理是医院信息化建设的重要组成部分。

通过电子信息技术，可以实现医疗设备的远程监控、故障预警和维护管理，提高设备的使用率和安全性。

### （三）医疗物联网

医疗物联网是将医疗设备、传感器和通信技术相结合，实现医疗信息的互联互通。医疗物联网可以提高医疗服务的质量和效率，例如，通过智能输液系统可以实时监测患者的输液情况，避免输液过快或过慢。

### 三、电子信息技术在医疗服务流程优化中的应用

电子信息技术在医疗服务流程优化中的应用主要体现在预约挂号、诊疗流程、费用结算等环节。通过电子信息技术，可以实现预约挂号的在线化，诊疗流程的标准化，费用结算的自动化，从而大大简化了医疗服务的流程，提高了医疗服务的效率。<sup>[1]</sup>

#### （一）远程医疗

远程医疗是通过电子信息技术实现医疗服务的远程化。它可以让患者在家中就能接受专家的诊断和治疗，提高了医疗效率，降低了医疗成本。

#### （二）移动医疗

移动医疗是指通过移动设备如手机、平板电脑等提供医疗服务。移动医疗可以让患者随时随地进行医疗咨询和健康管理，提高了患者的就医体验。

#### （三）医疗物联网

医疗物联网是将医疗设备、传感器和通信技术相结合，实现医疗信息的互联互通。医疗物联网可以提高医疗服务的质量和效率，例如，通过智能输液系统可以实时监测患者的输液情况，避免输液过快或过慢。

## 四、医疗数据分析与决策支持系统中的电子信息技术

电子信息技术在医疗数据分析与决策支持系统中的应用主要体现在医疗数据的收集、处理和分析。通过电子信息技术，可以实时收集和大量的医疗数据，然后通过数据分析，为医生提供科学的决策支持，从而提高医疗服务的质量。

### （一）数据挖掘与分析

数据挖掘与分析技术可以从海量的医疗数据中提取有价值的信息，为医疗决策提供支持。例如，通过对患者病历数据的分析，可以发现疾病的潜在规律，为疾病的预防和治疗提供依据。

### （二）人工智能与机器学习

人工智能和机器学习技术可以帮助医院实现自动化诊断和治疗，提高医疗效率和准确性。例如，通过对医学影像数据的分析，可以实现疾病的自动诊断。

### （三）大数据与云计算

大数据和云计算技术可以存储和处理海量的医疗数据，为医疗决策提供支持。例如，通过云计算技术，可以实现医疗数据的共享和备份，提高数据的安全性和可靠性。

### 五、远程医疗服务中的电子信息技术

电子信息技术在远程医疗服务中的应用主要体现在远程诊断、远程会诊、远程教育等环节。通过电子信息技术，可以实现医生与患者之间的远程交流，医生之间的远程会诊，医生与医学生之间的远程教育，从而扩大了医疗服务的范围，提高了医疗服务的效率。

#### （一）远程医疗系统的架构

远程医疗系统包括医疗设备、通信网络、数据存储和处理中心等组成部分。医疗设备通过通信网络将患者的生理数据传输到数据存储和处理中心，医生可以通过远程终端对患者进行诊断和治疗。

#### （二）远程医疗的应用场景

远程医疗可以应用于多种场景，如远程诊断、远程手术、远程监护等。例如，对于偏远地区的患者，可以通过远程医疗系统接受专家的诊断和治疗；对于危重症患者，可以通过远程医疗系统实现远程手术。

#### （三）远程医疗的优势

远程医疗具有提高医疗效率、降低医疗成本、提高医疗质量等优势。例如，通过远程医疗系统，可以避免患者因为长途跋涉而耽误病情；通过远程手术系统，可以让专家在远程指导下进行手术，提高手术的成功率。

### 六、电子信息技术在医院信息化系统中的安全与隐私保护

电子信息技术在医院信息化系统中的安全与隐私保护主要包括数据安全、网络安全、隐私保护等方面。通过电子信息技术，可以实现数据的安全存储和传输，网络的安全防护，隐私的有效保护，从而确保医疗服务的安全可靠。<sup>[2]</sup>

#### （一）网络安全威胁与挑战

网络安全威胁主要包括黑客攻击、病毒感染、数据泄露等。这些威胁可能导致医疗信息泄露、系统瘫痪等严重后果。

#### （二）安全与隐私保护策略

为了保障电子信息技术在医院信息化系统中的安全与隐私保护，可以采取以下策略：加强网络安全管理、数据加密、访问控制、安全审计等。

#### （三）法律法规与标准

为了保障电子信息技术在医院信息化系统中的安全与隐私保护，还需要制定相关的法律法规和标准。例如，

我国已经出台了《网络安全法》等相关法律法规，对网络安全进行了规范和保障。

在医院信息化建设中，网络安全至关重要。为了确保医院信息系统的安全性和稳定性，以下是一些关键的网络安全管理措施：

1. 制定详细的信息安全政策和规范：医院应制定一套全面的信息安全政策和规范，明确员工在使用医院网络和信息系统时的责任和行为准则。这些政策应包括访问控制、数据保护、安全漏洞管理、密码管理等方面的规定。

2. 加强员工安全意识培训和应急演练：定期对员工进行安全意识培训，提高他们对网络安全威胁的认识和防范意识。<sup>[3]</sup>培训内容可以包括密码安全、避免点击可疑链接、保护个人信息等。此外，还应定期进行应急演练，以检验医院在面对网络安全事件时的应对能力。

3. 与专业网络安全团队合作，提供技术支持与服务：医院可以与专业的网络安全团队合作，获取他们的技术支持和服务。这些团队可以提供实时的安全监测、漏洞扫描、入侵检测和响应等服务，帮助医院及时发现和处理安全威胁。

### 结论

电子信息技术在医院信息化系统中的应用，不仅提高了医疗服务的效率和质量，也为医疗服务的未来发展提供了新的可能。然而，电子信息技术在医院信息化系统中的应用也面临着一些挑战，如数据安全、网络安全、隐私保护等问题。因此，我们需要进一步加强电子信息技术在医院信息化系统中的应用研究，以解决这些问题，推动医疗服务的持续发展。

总的来说，电子信息技术在医院信息化系统中的应用，是医疗服务发展的重要趋势，也是医疗服务改革的重要手段。我们应该充分认识到电子信息技术在医院信息化系统中的应用的重要性，积极推动电子信息技术在医院信息化系统中的应用，以提高医疗服务的效率和质量，满足人民群众日益增长的医疗健康需求。

### 参考文献

- [1] 徐奎公, 徐奎公, 郭百艳. 电力变电站运行设备发热原因及预防对策[J].《电力设备》2019年第3期
- [2] 黄理民. 医院信息化建设中计算机网络安全管理与维护[J].《科技风》2020年36期
- [3] 嵇采茵. 激励理论在企业思想政治工作中的运用研究[J].《思想政治工作研究》2017-9-2