智慧医院信息安全建设与管理策略

杨　静
上海市浦东新区周浦医院　上海　201418

摘　要：随着信息技术的不断发展，智慧医院已经成为了医疗行业的新趋势。然而，智慧医院的信息安全问题也日益凸显，如何保障智慧医院信息系统的安全运行成为了亟待解决的问题。本文从智慧医院信息安全建设与管理的角度出发，对智慧医院信息安全建设的策略进行了探讨，并提出了相应的管理措施。

关键词：智慧医院；信息安全；建设策略；管理措施

引言

随着互联网技术的飞速发展，信息化已经成为了各行各业发展的重要驱动力。在医疗行业，智慧医院作为一种新型的医疗服务模式，通过信息化手段实现了医疗资源的优化配置和高效利用，为患者提供了便捷、高效的医疗服务。然而，智慧医院的信息安全问题也日益凸显，如何保障智慧医院信息系统的安全运行成为了亟待解决的问题。本文从智慧医院信息安全建设与管理的角度出发，对智慧医院信息安全建设的策略进行了探讨，并提出了相应的管理措施。

1 智慧医院信息安全建设策略

1.1 制定全面的信息安全政策

智慧医院信息安全建设的首要任务是制定全面、科学的信息安全政策。这一政策的制定需要充分考虑智慧医院的实际情况，结合国家相关法律法规和标准，确保信息安全政策既符合法律法规要求，又能适应智慧医院的信息化发展需求。具体来说，智慧医院信息安全政策应包括以下几个方面的内容：智慧医院信息安全政策应明确信息安全的总体目标，即确保智慧医院的信息系统安全稳定运行，保障患者信息的安全和隐私，维护智慧医院的正常运营秩序。同时，还应明确各业务部门在信息安全工作中的职责和任务，确保信息安全工作的落实。智慧医院信息安全政策应明确信息安全的基本原则，包括合法性原则、全员参与原则、预防为主原则、综合治理原则等。这些原则为智慧医院信息安全工作提供了基本遵循，有助于确保信息安全工作的有效性和可持续性。智慧医院信息安全政策应设定具体的信息安全要求，包括技术层面的安全防护措施、管理层面的安全管理制度、人员层面的安全培训和意识等。这些要求为智慧医院信息安全工作提供了具体指导，有助于提高信息安全工作的实际效果。为了适应信息化发展的需要，智慧医院信息安全政策应定期进行评估和修订。评估内容包括政策的执行情况、信息安全状况的变化等，修订内容包括政策的不适应情况、新的法律法规和标准等。通过评估和修订，智慧医院可以不断优化和完善信息安全政策，提高信息安全工作的针对性和实效性[1]。

1.2 建立完善的安全防护体系

智慧医院在信息安全建设中，首要任务是建立一套全面的安全防护体系。这个体系应该包括物理安全、网络安全、数据安全和管理安全四个方面。每一个方面都是保护信息资源的重要环节，缺一不可。首先，物理安全是信息安全的基础。智慧医院应当确保其设施和设备的安全，防止未经授权的人员进入，防止设备被盗、损坏或者破坏。这可能涉及到门禁系统、监控系统、报警系统等设备的安装和维护。同时，对于重要的设备和数据，还应该有专门的存储区域和访问控制。其次，网络安全是保护信息资源不受网络攻击的关键。智慧医院应当采用防火墙、入侵检测系统等技术手段，防范外部攻击。防火墙可以阻止未经授权的访问，入侵检测系统可以在攻击发生时立即发出警报。此外，还应当定期进行网络安全审计，检查网络设备的安全性能，发现并修复潜在的安全漏洞。再次，数据安全是保障信息资源不被非法获取和利用的重要手段。智慧医院应当采用加密、备份等技术手段，防止数据泄露、篡改和丢失。对于敏感的数据，还应当进行加密处理，只有拥有相应密钥的人才能访问。同时，定期的数据备份也是必不可少的，以防数据丢失或损坏。最后，管理安全是确保信息安全事件得到有效管理的关键。智慧医院应当建立一套完善的信息安全管理制度，包括信息安全政策、操作规程、应急预案等。此外，还应当定期进行信息安全培训，提高员工的信息安全意识和技能。同时，应当建立一套有效的信息安全审计制度，定期对信息安全状况进行检查和评估。

1.3 强化安全意识培训和教育

信息安全不仅仅是技术问题，更是一种文化。智慧医院应当认识到，员工的安全意识是保障信息安全的第一道防线[2]。因此，加强员工的安全意识培训和教育，提高员工的信息安全素质，是智慧医院信息安全建设策略中的重要一环。首先，智慧医院应当定期组织员工参加信息安全培训。这些培训可以涵盖国家相关法律法规、行业标准和最佳实践等内容，以确保员工了解并遵守相关的法律法规，掌握行业标准和技术要求，以及学习并实践最佳的信息安全实践。通过这种方式，可以提高员工的信息安全意识和技能，使他们在日常工作中能够更好地保护医院的信息安全。其次，智慧医院可以通过开展信息安全知识竞赛等活动，激发员工的学习兴趣。这些竞赛可以是团队竞赛，也可以是个人竞赛，内容可以包括信息安全的基本知识、最新的信息安全威胁和防护技术等。通过竞赛，可以让员工在轻松愉快的氛围中学习信息安全知识，提高他们的信息安全素养。最后，智慧医院应当加强对员工的安全考核和激励。可以将信息安全纳入员工绩效考核体系，对员工的信息安全行为进行考核，并根据考核结果给予相应的奖励或惩罚。这样，不仅可以让员工明白保护信息安全的重要性，也可以激励他们更加积极地参与到信息安全的工作中来。

1.4 建立应急响应机制

智慧医院信息安全建设策略的第四点是建立应急响应机制。智慧医院应当建立完善的应急响应机制，确保在信息安全事件发生时能够迅速、有效地进行处置。具体来说，智慧医院应当制定应急预案，明确应急响应流程和责任分工；建立应急响应小组，负责应急处置工作；定期组织应急演练，检验应急预案的有效性和完善性；加强与政府、行业组织和其他医疗机构的合作，共享信息安全信息和资源。应急响应机制是智慧医院信息安全建设的重要组成部分。通过制定应急预案，明确应急响应流程和责任分工，智慧医院可以迅速、有效地应对各种信息安全事件，避免或减少事件造成的损失。建立应急响应小组可以保证在信息安全事件发生时，有专业的人员负责应急处置工作，针对不同等级的安全事件进行分类处理，确保问题得到及时解决。为了确保应急预案的有效性，智慧医院需要定期组织应急演练。通过模拟信息安全事件的发生和处理过程，可以发现应急预案中存在的问题和不足，并及时进行完善和改进[3]。同时，加强与政府、行业组织和其他医疗机构的合作，可以共享信息安全信息和资源，提高应急响应能力。

2 智慧医院信息安全管理措施

2.1 制定合理的权限分配策略

智慧医院应当制定合理的权限分配策略，确保员工在完成工作任务的同时，不会滥用权限导致信息安全事故。具体来说，智慧医院应当根据员工的职责和工作内容，合理分配系统访问权限；对于敏感数据和关键业务系统，应当实行严格的权限控制和审计机制；对于临时访问需求，应当实行审批制度，确保权限使用的合规性。首先，智慧医院应当根据员工的职责和工作内容，合理分配系统访问权限。这意味着，不同部门的员工应当拥有不同的访问权限，以确保他们只能访问与自己职责相关的系统和数据。例如，医生和护士只应当能够访问患者的基本信息和病历记录，而不应该能够访问患者的诊断结果和其他敏感信息。此外，不同级别的员工也应当拥有不同的访问权限，以确保他们不能访问到自己无权访问的信息。其次，对于敏感数据和关键业务系统，智慧医院应当实行严格的权限控制和审计机制。这意味着，只有经过授权的员工才能够访问这些系统和数据，同时，智慧医院还应当对这些系统的使用情况进行实时监控和审计，以便及时发现并阻止任何不当行为。此外，智慧医院还应当定期对员工的权限进行审查和调整，以确保他们的权限始终与自己的职责和工作内容保持一致。最后，对于临时访问需求，智慧医院应当实行审批制度，确保权限使用的合规性。这意味着，员工在需要临时访问某些系统或数据时，应当向上级领导提交书面申请，说明访问的原因、时间和目的。只有在得到批准后，员工才能够访问这些系统和数据[4]。这样既可以避免员工滥用权限，也可以确保敏感信息的安全。

2.2 加强网络安全监控

智慧医院信息安全管理措施中的加强网络安全监控是其中的重要环节。随着信息技术的发展，医疗行业对信息化的需求越来越高，网络安全问题也日益突出。因此，智慧医院必须采取有效的措施，加强网络安全监控，确保医院信息系统的安全稳定运行。首先，智慧医院应当部署网络安全监控系统。这个系统可以实时监测网络流量、设备状态等信息，及时发现网络异常情况。例如，如果发现某个服务器的CPU使用率突然升高，可能就意味着有黑客正在进行攻击；如果发现某个网络设备的连接状态异常，可能就意味着有设备被病毒感染或者被非法访问。这些异常情况都需要及时处理，以防止网络安全事件的发生。其次，智慧医院应当建立网络安全事件报告机制。当网络安全事件发生时，需要立即向相关部门报告，以便尽快采取措施进行处理。这个机制可以包括电话报警、邮件报警、短信报警等多种方式，确保信息能够及时、准确地传达到相关人员。再次，智

慧医院应当加强对网络安全事件的分析和处理。这包括对网络安全事件的起因进行深入分析，找出问题的根源；对网络安全事件的影响进行评估，确定应对策略；对网络安全事件的处理过程进行记录，总结经验教训。通过这样的分析和处理，可以有效地防止类似事件的再次发生。此外，智慧医院还应当加强员工的网络安全意识培训。许多网络安全问题的产生，都是由于员工的操作不当或者缺乏必要的安全知识导致的。因此，定期进行网络安全知识的培训，提高员工的网络安全意识，是防止网络安全事件的有效手段。

2.3 落实数据备份和恢复措施

智慧医院信息安全管理措施智慧医院作为现代医疗行业的重要组成部分，其信息安全管理工作是确保医院正常运行和患者信息安全的基础[5]。为了保障智慧医院的信息安全，我们需要采取一系列有效的措施。以下将详细阐述智慧医院的信息安全管理措施：智慧医院应当制定详细的数据备份计划，对关键数据和系统进行定期备份。备份数据的频率和周期应与数据的敏感性和重要性相匹配。例如，对于一些涉及到患者隐私和医疗关键数据的信息系统，应采取更为频繁的备份策略。除了备份数据之外，智慧医院还需要建立高效的数据恢复机制。当数据因各种原因丢失或损坏时，能够通过备份数据快速恢复正常运行。这需要定期测试备份数据的恢复能力，确保在需要时可以有效地恢复数据。备份数据是智慧医院的重要资产，需要对其进行严格管理和保护。要确保备份数据的安全性，防止备份数据泄露或被破坏。同时，还要对备份数据进行定期检查和维护，保证其可用性和完整性。综上所述，通过科学合理地制定数据备份计划、建立完善的数据恢复机制以及对备份数据进行严格管理和保护，可以大大提高智慧医院信息系统的可靠性和稳定性，保障医院正常运行和患者信息安全。

2.4 加强供应商管理

智慧医院信息安全管理措施是一个复杂的系统工程，其中，加强供应商管理是一个重要的环节。供应商提供的产品和服务直接关系到医院的信息安全，因此，对供应商的管理必须严格把关。首先，智慧医院应当对供应商进行资质审查。这包括对供应商的营业执照、税务登记证、组织机构代码证等相关证件进行审核，确保供应商具有合法的经营资格。同时，还应对供应商的技术能力、管理水平、信誉度等进行评估，以确保其有能力提供符合医院需求的产品和服务。其次，智慧医院在与供应商签订合同时，应明确安全要求和服务承诺。合同中应包含对供应商的信息安全责任要求，如数据保密、非泄露、备份和恢复等；服务承诺则应包括供应商应提供的技术支持、售后服务等内容。通过这种方式，可以确保供应商在提供服务的过程中，严格遵守医院的信息安全规定。再次，智慧医院应定期对供应商进行考核和评价。考核内容包括供应商的产品质量、服务水平、响应速度等；评价则应根据考核结果，对供应商的表现进行综合评价，优秀者予以奖励，不合格者则应予以整改或更换。通过这种机制，可以促使供应商持续提高服务质量，满足医院的信息安全需求。

结语

智慧医院的信息安全建设与管理是保障信息系统安全运行的重要基础。本文从智慧医院信息安全建设与管理的角度出发，对智慧医院信息安全建设的策略进行了探讨，并提出了相应的管理措施。希望通过本文的研究，为智慧医院的信息安全建设提供有益的参考和借鉴。

参考文献

[1]王海峰，李晓东.(2023).智慧医院信息安全建设与管理策略研究[J].计算机工程与应用，(6)，1-5.

[2]李明，张华.(2022).基于区块链技术的智慧医院信息安全管理策略研究[J].信息网络安全，(4)，1-4.

[3]刘洋，王丽.(2023).智慧医院信息安全管理体系构建及实施策略研究[J].中国卫生政策研究，(3)，1-7.

[4]陈杰，杨洪波.(2022).基于云计算的智慧医院信息安全管理策略研究[J].计算机应用研究，(2)，1-6.

[5]赵云，李娟.(2023).智慧医院信息安全风险评估与管理策略研究[J].电子技术应用，(1)，1-5.