数字化医院信息安全建设与管理策略

张　中
卫宁健康科技集团股份有限公司　上海　200072

摘　要：数字化医院信息安全建设与管理策略是确保医疗数据完整、可用与患者隐私保护的关键。通过制定明确的信息安全策略与政策，建立信息安全管理体系，强化网络安全防护、数据加密与备份、账号与权限管理，以及完备应急管理措施，数字化医院能够有效应对内外部信息安全威胁。同时，加强安全服务管理与职工信息安全知识培训，提升整体信息安全防护能力，确保医院信息系统稳定运行，为医疗服务提供坚实保障。

关键词：数字化医院；信息安全建设；管理策略

引言：随着信息技术的飞速发展，数字化医院已成为现代医疗服务的重要模式。然而，信息安全问题也随之凸显，对医院运营和患者隐私构成严重威胁。为确保数字化医院的安全运行，构建一套完善的信息安全建设与管理体系显得尤为重要。本策略旨在通过深入分析信息安全理论基础，明确数字化医院的信息安全需求，提出切实可行的信息安全建设与管理策略，为数字化医院的可持续发展提供坚实保障。

1 数字化医院信息安全建设与管理的理论基础

1.1 信息安全的概念与范畴

（1）信息安全的定义。信息安全是指保护信息免受未经授权的访问、使用、披露、中断、修改或销毁的过程。它涵盖了确保信息的机密性、完整性和可用性的所有措施。机密性要求信息只能被授权人员访问，完整性保证信息在传输和存储过程中不被篡改，而可用性则确保信息在需要时能够被访问和使用。这些原则共同构成了信息安全的核心，为数字化医院的信息系统提供了必要的保护。（2）信息安全的组成要素。信息安全的组成要素包括保密性、完整性、可用性、真实性、不可抵赖性、可审计性和可恢复性。保密性通过加密和访问控制等手段确保信息不被未授权人员获取。完整性使用校验机制和哈希算法等手段保护信息在传输和存储过程中不被篡改。可用性则通过冗余系统和故障转移机制确保信息在需要时能够可靠地被访问。真实性通过身份认证和数字签名等手段验证信息的来源和内容。不可抵赖性通过日志记录和数字签名等手段确保信息发送方无法否认其发送的事实。可审计性通过日志记录和审计跟踪等手段记录相关操作和事件，便于后续审计和调查。可恢复性则通过备份和灾难恢复计划确保在信息安全事件发生后能够快速恢复系统的功能和数据。

1.2 数字化医院信息安全的特点与需求

（1）数字化医院的信息系统结构。数字化医院的信息系统结构复杂，包括医院信息系统（HIS）、医学影像存档与通信系统（PACS）、实验室信息系统（LIS）、临床信息系统（CIS）等多个子系统。这些系统相互连接，共同支持医院的日常运营和医疗活动。然而，这种复杂的系统结构也带来了信息安全方面的挑战，需要采取有效的措施来确保整个系统的安全性和稳定性。（2）数字化医院的信息安全需求与挑战。数字化医院面临着来自内外部的多种信息安全威胁，如黑客攻击、恶意软件、数据泄露等。这些威胁不仅可能导致医院运营中断，还可能危及患者的隐私和生命安全。因此，数字化医院需要建立完善的信息安全体系，包括加强网络安全防护、实施数据加密和备份、强化账号和权限管理等措施，以应对这些挑战并确保医院信息系统的正常运行。

2 数字化医院信息安全建设的主要内容

2.1 制定信息安全策略和政策

（1）明确信息安全的目标、原则和要求。信息安全策略是数字化医院信息安全建设的基石。医院应明确信息安全的目标，即保护患者隐私、确保医院数据的完整性和可用性，以及防范和应对信息安全事件。同时，医院应确立信息安全的原则，如最小权限原则、责任明确原则、持续改进原则等，这些原则将指导信息安全工作的全过程[1]。此外，医院还应制定详细的信息安全要求，包括数据加密标准、访问控制策略、备份和恢复策略等，以确保信息安全工作的具体执行。（2）将信息安全纳入医院管理体系。信息安全不仅仅是信息技术部门的责任，而是整个医院管理体系的重要组成部分。医院应将信息安全纳入医院战略规划、业务流程、员工培训等多个环节，确保信息安全理念贯穿于医院的日常运营中。通过设立信息安全管理部门或委员会，协调各部门之间的信息安全工作，确保信息安全策略的顺利实施。

2.2 建立信息安全管理体系

（1）组建专门的信息安全团队。数字化医院应组建一支专业的信息安全团队，负责信息安全的整体规划、实施和维护。这支团队应具备丰富的信息安全知识和实践经验，能够应对各种信息安全挑战。团队成员应包括信息安全专家、网络管理员、数据备份与恢复专家等，以确保信息安全工作的全面性和专业性。（2）制定信息安全管理制度和流程。信息安全管理制度是指导信息安全工作的准则。数字化医院应制定一套完整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。这些制度应明确信息安全工作的职责、权限、流程和要求，确保信息安全工作的有序进行。同时，医院还应建立信息安全审核和评估机制，定期对信息安全工作进行检查和评估，以发现潜在的安全隐患并及时整改。（3）定期开展风险评估和安全审计。风险评估和安全审计是发现信息安全漏洞和潜在威胁的重要手段。数字化医院应定期开展风险评估工作，对医院的信息系统进行全面的安全漏洞扫描和渗透测试，以发现潜在的安全隐患。同时，医院还应定期进行安全审计，对信息安全工作的实施情况进行检查和评估，确保信息安全制度的有效执行。

2.3 强化网络安全防护

（1）采用防火墙、入侵检测与防御系统等技术手段。网络安全防护是数字化医院信息安全建设的重要环节。医院应采用先进的网络安全技术，如防火墙、入侵检测与防御系统等，以抵御来自外部的恶意攻击。防火墙可以阻止未经授权的访问和数据泄露，而入侵检测与防御系统则可以及时发现并应对潜在的网络威胁。（2）安装网络管理软件，实时监控服务器和各终端的运行情况。为了实时掌握网络系统的运行状态，数字化医院应安装网络管理软件。这些软件可以实时监控服务器和各终端的运行情况，包括网络流量、系统资源使用情况、异常登录行为等。通过及时发现和处理异常情况，医院可以迅速响应并应对潜在的信息安全事件[2]。

2.4 数据加密与备份

（1）对敏感数据进行加密处理。数据加密是保护患者隐私和数据安全的重要手段。数字化医院应对敏感数据进行加密处理，如患者姓名、住址、诊断结果等。通过采用先进的加密算法和密钥管理机制，医院可以确保敏感数据在传输和存储过程中的安全性。（2）实施定期的数据备份和恢复策略。数据备份是确保医院数据安全的关键措施。数字化医院应制定并实施定期的数据备份和恢复策略，包括全量备份、增量备份和差异备份等。同时，医院还应确保备份数据的可靠性和可用性，以便在需要时能够迅速恢复数据。为了应对紧急情况，医院还应建立灾难恢复计划，确保在数据丢失或系统瘫痪的情况下能够迅速恢复业务运行。

2.5 强化账号和权限管理

（1）建立科学的账号和权限管理机制。账号和权限管理是确保信息安全的重要环节。数字化医院应建立科学的账号和权限管理机制，包括账号的申请、审批、分配和注销等流程。同时，医院还应实施定期审查和更新账号的策略，确保账号的权限与其工作职责相匹配。通过实施细粒度的权限控制策略，医院可以限制用户对敏感数据的访问和操作权限，从而降低数据泄露的风险。（2）对用户进行身份认证和权限控制。身份认证和权限控制是确保用户合法访问系统资源的关键措施。数字化医院应采用多因素身份认证方法，如用户名和密码的组合、生物特征识别等，以提高身份认证的安全性和准确性。同时，医院还应实施细粒度的权限控制策略，根据用户的角色和职责分配不同的权限。这意味着用户只能访问与其工作相关的资源和数据，而不能访问其他不相关的资源和数据。通过实施严格的身份认证和权限控制策略，医院可以确保只有经过授权的用户才能访问和操作敏感数据。

3 数字化医院信息安全管理的策略

3.1 安装有效的防病毒软件

（1）周期性地对系统程序进行检查。防病毒软件是数字化医院信息安全的第一道防线。为了确保系统的安全性，医院应安装经过专业认证的高效防病毒软件，并周期性地对系统程序进行全面检查。这种检查可以及时发现并清除潜在的病毒和恶意软件，防止它们对系统进行破坏或窃取敏感数据[3]。（2）利用病毒防火墙进行系统实时监控。除了周期性检查外，医院还应利用病毒防火墙对系统进行实时监控。病毒防火墙能够实时拦截和阻止恶意软件的入侵，确保系统的稳定运行。同时，防火墙还能记录并分析可疑的网络活动，为医院提供实时的安全威胁情报。

3.2 桌面系统安全管理

（1）提出桌面系统的具体安全要求。桌面系统作为医护人员日常工作的主要平台，其安全性至关重要。医院应针对桌面系统提出具体的安全要求，如禁止安装未经授权的软件、限制对敏感数据的访问等。这些要求有助于规范医护人员的操作行为，降低因误操作或恶意行为导致的信息安全风险。（2）进行必要的安全保护。为了满足桌面系统的安全要求，医院应采取必要的安全保

护措施。这包括安装桌面安全软件、定期更新操作系统和应用程序补丁、使用强密码策略等。这些措施能够增强桌面系统的安全防护能力，防止病毒和黑客的攻击。

3.3 强化安全服务管理

（1）与专业的信息安全服务机构建立长期合作关系。数字化医院在信息安全方面面临诸多挑战，因此与专业的信息安全服务机构建立长期合作关系显得尤为重要。这些机构拥有丰富的信息安全经验和先进的技术手段，能够为医院提供全面的信息安全咨询、评估和解决方案。通过与这些机构合作，医院可以不断提升自身的信息安全防护能力。（2）定期进行系统全面检测和安全修复。为了确保系统的安全性，医院应定期邀请专业的信息安全服务机构对系统进行全面检测和安全修复。这些检测可以发现系统中存在的安全漏洞和薄弱环节，并提出相应的修复建议。通过及时修复这些漏洞，医院可以显著降低信息安全风险。

3.4 加强安全管理机制建设

（1）制订医院信息安全建设规划。为了指导医院信息安全工作的有序开展，医院应制订详细的信息安全建设规划。这个规划应明确信息安全的目标、原则、策略和措施，以及相关的责任人和时间表。通过实施这个规划，医院可以确保信息安全工作的连续性和有效性。（2）建立和完善医院信息安全组织与制度。为了加强信息安全管理，医院应建立和完善信息安全组织与制度。这包括成立信息安全管理部门或委员会、制定信息安全管理制度和流程、明确信息安全职责和权限等。这些组织和制度的建立有助于确保信息安全工作的规范性和有效性[4]。（3）加强职工信息安全知识宣传和培训。职工是医院信息安全的重要参与者。为了提升他们的信息安全意识和技能水平，医院应加强信息安全知识的宣传和培训。这可以通过组织定期的信息安全培训、发布信息安全简报、开展信息安全知识竞赛等方式实现。通过这些活动，医院可以增强职工对信息安全的重视程度和防范能力。

3.5 完备应急管理措施

（1）制订可靠实用的应急方案。为了应对可能发生的信息安全事件，医院应制订可靠实用的应急方案。这个方案应明确应急响应的流程、责任人和措施，以及相关的技术保障和物资储备。通过实施这个方案，医院可以在信息安全事件发生时迅速作出反应，降低损失和影响。（2）建立单机版的应急系统。为了确保在网络安全受到威胁时仍能保持业务的连续性，医院应建立单机版的应急系统。这个系统应包含医院的核心业务数据和关键应用程序的备份，以及相应的恢复工具和流程。当网络安全出现问题时，医院可以迅速切换到单机版应急系统，确保医疗服务的正常进行。

结束语

综上所述，数字化医院的信息安全建设与管理是一项系统工程，涉及技术、管理、人员等多个层面。通过实施上述策略，医院能够显著提升信息安全防护能力，确保医疗数据的完整性、可用性和患者的隐私安全。未来，随着技术的不断进步和威胁的不断变化，数字化医院需持续优化信息安全策略，加强技术创新与人才培养，以应对新的挑战，为医疗服务的高质量发展贡献力量。

参考文献

[1]夏彩凤,董慧星,朱宇喆.数字化智慧医院建设的方案与策略[J].中国新通信,2021,(10):89-91.

[2]陈子璇.智慧医院管理背景下的医院信息化建设研究[J].现代信息科技,2021,(11):124-127.

[3]刘爱军,王韬,刘盾.智慧医院相关技术在医院建设中的应用[J].中华医院管理杂志,2020,(09):75-76.

[4]罗紫瑜.智慧医院医疗服务价格信息化建设探讨[J].中国冶金工业医学杂志,2020,(04):43-44.