网络空间安全视角下医院信息化建设的挑战与应对

陈伟杰
广东 广州 510000

DOI: 10.61369/TACS.2025110009

摘　　要： 数字时代的医院信息化建设在提升效率的同时，也面临诸多网络空间安全挑战。这些挑战包括技术漏洞、隐私风险、老旧系统现代化改造的复杂性、人才短缺以及预算不合理等问题。本文提出了如一体化防御系统、智能合约和弹性投资模式等多维度解决方案，以增强安全性并推动其安全发展。

关 键 词： 医院信息化；网络空间安全；对策

Challenges and Responses to Hospital Informatization Construction from the Perspective of Cyberspace Security

Chen Weijie
Guangzhou, Guangdong 510000

Abstract: Hospital informatization construction in the digital age brings efficiency improvements but faces numerous cyberspace security challenges. These include technical vulnerabilities, privacy risks, legacy system modernization complexities, workforce gaps, and budget inefficiencies. Multidimensional solutions like integrated defense systems, smart contracts, and resilient investment models are proposed to enhance security and promote its secure development.

Keywords: hospital informatization; cyberspace security; countermeasures

引言

在数字时代，医院信息化建设已成为必然趋势，带来了提高医疗服务效率和优化管理等诸多益处。然而，它也面临重大的网络安全挑战，如数据泄露、系统中断和隐私侵犯[1]。现有的市级医疗信息化项目法规和技术管理标准，对医院网络安全实践起到了指导作用。但随着技术和网络威胁的快速演变，这些政策需要不断审视和更新。本文旨在探讨这些挑战，并从技术框架、漏洞、隐私风险和人才短缺等方面提出相应对策，以推动网络空间安全背景下医院信息化的安全发展。

一、医院信息化建设现状

（一）市政工程基础设施中的技术框架

在市政工程框架下，医院信息化系统中网络空间安全技术的整合已达到一定水平，但仍有提升空间。在网络架构设计方面，许多医院采用了相对先进的模式。例如，它们常使用多层网络结构来分离不同类型的数据和服务，比如将患者信息管理与行政运营分开[2]。这有助于通过减少未经授权访问的可能性来增强患者相关数据的安全性。

然而，在复杂的医院环境中，确保不同网段之间在保持安全的同时实现无缝通信仍是一项挑战。至于数据管理平台，医院越来越依赖数字系统来存储、管理和分析患者数据、病历及其他信息。一些医院已实施先进的数据加密技术，以在存储和传输过程中保护敏感数据。尽管如此，数据量的不断增长以及跨部门和跨机构数据共享的需求带来了新的威胁。例如，在共享过程中确保数据完整性和保密性并非总是易事。总体而言，虽然市政工程基础设施内的医院信息化建设技术框架取得了进展，但仍需持续努力应对新出现的网络空间安全挑战。

（二）技术管理的政策环境

当前医院信息化建设技术管理的政策环境，特别是在网络空间安全方面，主要依赖现有的市级医疗信息化项目法规和技术管理标准[3]。这些法规和标准在指导和规范医院信息化中的网络安全实践方面发挥着关键作用。它们界定了医院信息系统中数据安全、网络访问控制和系统运行管理的基本要求。例如，它们可能规定患者相关数据的加密方法，以防止未经授权的访问和数据泄露。关于网络访问，可能有规则明确谁可以在何种条件下访问不同级别的医院信息。技术管理标准还涵盖系统维护、备份和灾难恢复等方面。它们确保医院信息系统能够稳定、持续运行，将潜在网络攻击或系统故障的影响降至最低。然而，随着信息技术的快速发展以及网络威胁形势日益复杂，这些市级法规和标准可能

难以跟上步伐。新型网络威胁，如高级持续性威胁（APT），可能无法被现有政策环境完全应对。因此，持续审查和更新这些法规和标准对于适应医院信息化建设中不断变化的网络空间安全要求至关重要。

二、医院信息化系统中的安全威胁

（一）网络安全管理中的技术漏洞

从技术管理角度来看，医院信息化系统存在一些严重的漏洞。在医疗物联网设备方面，缺乏标准化的安全协议以及加密措施不足是突出问题。这些设备常常收集并传输患者的敏感数据，如生命体征和病史。如果没有适当的安全机制，它们很容易遭到黑客攻击，进而导致数据泄露或设备被非法控制[4]。例如，攻击者可能会操控输液泵的设置，危及患者生命。

云平台在医院信息化中越来越多地用于数据存储和处理，同样也存在风险。云系统中访问控制不完善，可能会让未经授权的人员获取患者记录、研究数据以及医院管理信息。此外，云基础设施的共享特性意味着一个租户出现安全漏洞可能会影响其他租户。

跨系统互操作性也是一个存在漏洞的领域。随着医院整合电子健康记录（EHR）、图像存档与通信系统（PACS）以及医院资源规划（HRP）等多个系统，这些系统之间的接口可能缺乏适当的安全验证。恶意行为者可能会利用这些薄弱接口注入虚假数据、扰乱系统运行或获取受限信息。为确保医疗信息的安全与可靠，医院信息化系统网络安全管理中的所有这些技术漏洞都亟待解决。

（二）城市公共卫生数据治理中的隐私风险

在城市公共卫生数据治理背景下，患者数据在城市医疗网络间共享的过程中存在重大隐私风险。城市中不同医院和医疗机构之间的数据整合与共享旨在提高医疗服务的整体效率。然而，这也使患者数据面临潜在威胁[5]。

一个主要问题是缺乏足够的隐私保护机制。当数据在多方之间传输和共享时，患者信息的安全无法得到有效保障。例如，薄弱的身份验证和授权流程可能会让未经授权的人员访问敏感的患者数据。恶意行为者可能会利用这些漏洞获取个人健康记录，其中可能包含疾病史、基因数据和治疗方案等高度机密信息。

此外，城市公共卫生系统数据共享环境的复杂性进一步加剧了隐私风险。不同机构的信息安全管理能力可能参差不齐。它们之间不兼容的数据格式和安全标准会给实施统一有效的隐私保护措施造成阻碍。这种情况使得在整个数据共享过程中难以确保对患者隐私进行持续可靠的保护。

另外，数据滥用的潜在风险也很大。即使出发点是好的，但在数据共享过程中对患者数据处理不当也会导致隐私侵犯。例如，数据可能被用于非最初预期的目的，比如在未经患者明确同意的情况下被用于商业营销。城市公共卫生数据治理中的这些隐私风险给医院信息化系统的安全带来了严峻挑战。

三、多维挑战分析

（一）技术管理制约因素

1. 遗留系统现代化的复杂性

在确保城市服务连续性的同时，对医院遗留信息系统进行现代化改造面临着众多挑战。遗留系统通常依赖过时的硬件和软件，很难整合新的安全功能与技术。由于缺乏这些系统的相关文档和专业知识，问题变得更加棘手，因为要弄清楚其内部运行机制并进行必要的升级困难重重[6]。

此外，遗留系统中存储的数据格式可能不兼容，阻碍了向新平台的无缝转移。数据迁移过程需要精心规划，以避免数据丢失或损坏，否则可能对患者护理和行政管理工作产生严重影响。另外，将遗留系统与新的网络安全措施相结合可能会打乱现有的工作流程，给医院工作人员带来不便，并可能影响服务的提供。

另一个复杂之处在于，遗留系统在设计时可能未考虑到当前的网络安全威胁。因此，它们更容易遭受数据泄露和勒索软件等攻击。加强这些系统的安全性需要全面了解其架构和潜在漏洞，但这并非易事。总体而言，在医院信息化建设中对遗留系统进行现代化改造并保持服务连续性是一项复杂的任务，需要仔细考虑多个因素。

2. 网络安全专业人才缺口

从网络空间安全角度来看医院信息化建设，网络安全专业领域存在明显的人才缺口。医疗行业需要精通实施先进网络安全协议的技术人员。然而，此类专业人才短缺[7]。

医院网络安全是一个高度专业化的领域。它要求从业人员不仅要了解一般网络安全的复杂细节，还需深入掌握医疗环境相关知识。例如，他们需要了解像患者病历这类特殊数据类型，这些数据极为敏感，受到严格法规的保护。针对医疗与网络安全交叉领域的专业培训项目匮乏，这使得问题更加严重。大多数普通网络安全课程并未涵盖医院信息学的独特方面，导致毕业生无法应对医院环境中的各种挑战。

此外，医疗和网络安全领域技术变化迅速，这进一步拉大了这一差距。新的威胁不断出现，医院需要能够快速适应并实施最新安全措施的员工。招聘经验丰富的网络安全专家也很困难，因为各行业对这类专业人才需求旺盛，与以技术为主的公司相比，医院可能无法提供有竞争力的薪资或工作条件。这种专业人才的整体短缺，对医院信息化建设中有效实施先进的网络安全措施构成了重大制约。

（二）市政工程局限性

1. 安全基础设施预算分配不合理

从网络空间安全角度看，医院信息化建设中安全基础设施预算分配不合理是一个重大障碍。市政资金投入机制往往与医疗 IT 项目中快速演变的网络安全需求不匹配[8]。传统的预算分配模式可能无法充分考虑网络威胁的动态特性。例如，它们可能每年为安全基础设施分配固定金额，却不考虑新出现的攻击类型，比如针对医院数据的复杂勒索软件，或者旨在窃取患者信息的高级网络钓鱼活动。

这种不合理性导致对关键安全组件的投资不足。可能没有足够资金用于升级安全软件、聘请熟练的网络安全人员或实施最先进的加密技术。结果，医院可能会因安全系统过时，无法保护敏感的患者记录、医学研究数据和运营信息而变得脆弱。

此外，预算分配的不合理还导致不同安全要素之间缺乏整合。安全基础设施的某些方面可能资金过剩，而其他方面却被忽视。这种不平衡影响了医院信息化中网络安全框架的整体有效性。很难建立一个全面协调的防御机制，使医院面临潜在的网络相关干扰风险，这可能对患者护理和医院声誉造成严重后果。

2. 跨部门协调障碍

从网络空间安全角度来看医院信息化建设，跨部门协调障碍带来了重大挑战。市政工程通常涉及多个部门，每个部门都有自己的目标、重点和工作方法。例如，规划部门可能专注于城市的整体布局和长期发展，而负责医院信息化实施的部门可能更关注医院当前的技术需求和安全要求[9]。

这些差异可能导致策略不一致。规划部门在设计大规模市级信息化框架时，可能没有充分考虑医院特定的网络安全漏洞和合规要求。另一方面，医院层面的实施部门可能难以将其以安全为重点的信息化计划融入更广泛的市政工程蓝图中。

此外，部门之间的沟通差距加剧了这一问题。缺乏定期有效的沟通渠道可能导致误解，一个部门可能不知道另一个部门的进展、需求变化或新出现的网络安全威胁。这种协调不足不仅会减缓医院信息化建设进程，还会增加忽视关键网络安全问题的风险，使医院在网络空间中容易受到攻击。

四、战略应对机制

（一）技术创新途径

1. 一体化防御系统架构

从网络空间安全角度来看，医院信息化建设中的一体化防御系统架构应是一个全面且多维度的结构。其核心如文献[10]所提议的，融合了人工智能驱动的威胁检测和基于区块链的数据完整性验证。

人工智能驱动的威胁检测在实时监控医院信息系统内的网络活动方面能发挥关键作用。通过分析网络流量中的模式、行为和异常情况，它可以迅速识别潜在的网络威胁，如恶意软件攻击、未经授权的访问尝试和数据泄露。人工智能算法能够不断从新出现的威胁中学习，随着时间推移调整并提高检测准确性。

另一方面，区块链为数据完整性验证提供了一种防篡改机制。在医院环境中，患者记录、医学研究数据和管理信息至关重要。区块链技术可确保这些数据以不可篡改且可验证的方式存储。每一个数据条目都经过加密，并与之前的条目相链接，形成一条信任链。这不仅保障了数据的真实性，还为所做的任何更改提供了审计追踪。

这两种技术在防御系统架构中的整合产生了协同效应。当人工智能检测到威胁时，区块链可确保即使威胁设法渗透系统，数据依然保持完整。它们共同构成了一个强大的一体化防御系统，能有效应对网络空间安全背景下医院信息化建设所面临的挑战。

2. 智能合约在健康数据治理中的应用

基于区块链技术的智能合约，在网络空间安全背景下的医院信息化建设中可发挥关键作用。在健康数据治理方面，它们提供了一种防篡改且透明的方式来管理数据共享和访问权限。

对于跨城市医疗网络的安全数据共享，智能合约可以自动化合规机制。可以对其进行编程，以执行关于谁能在何种情况下、出于何种目的访问特定健康数据的严格规则。例如，当患者数据需要在不同医院间共享以进行复杂诊断时，智能合约可以核实所有相关方是否满足数据访问的法律和道德要求[11]。这确保了数据不会被滥用或被未经授权的实体访问。

此外，智能合约可以记录与健康数据相关的每一笔交易。这创建了一个不可篡改的审计追踪，这对于跟踪数据使用情况和确保问责制至关重要。万一发生任何安全漏洞或数据滥用情况，审计追踪可用于确定问题来源并采取适当行动。通过将智能合约整合到健康数据治理中，医院能够提升其信息化系统的安全性和完整性，从而在数字时代更好地保护患者信息。

（二）城市政策强化措施

1. 医疗设备网络安全认证标准

在网络空间安全范畴内的医院信息化建设领域，为医疗设备建立健全的网络安全认证标准至关重要。应推荐市级医疗物联网设备网络安全认证技术规范。这些标准需要全面涵盖各个方面，从医疗设备软硬件的基本安全要求到数据传输中使用的通信协议。

例如，应严格定义设备内的认证机制，以确保只有授权用户能够访问和操作医疗设备，保障患者特定数据的完整性和保密性。必须明确规定在医院网络内部以及与外部系统通信时数据传输过程中的数据加密标准，以防止数据泄露或被截取。此外，医疗设备软件的更新机制也应成为认证标准的一部分，确保能够及时安装安全补丁以应对新出现的威胁[12]。通过为医疗设备制定如此详细且严格的网络安全认证标准，医院可以提升其信息化基础设施的安全性，确保数字时代医疗服务的安全与可靠。这不仅保护了患者隐私和医疗数据，还维持了医疗机构在复杂网络空间环境中的正常运转。

2. 弹性基础设施投资模式

设计弹性基础设施投资模式对于网络空间安全背景下的医院信息化建设至关重要。城市需要开发适应性融资模式，在医院信息技术升级过程中将网络安全弹性置于优先地位。例如，可以探索公私合营（PPP）模式。在这种模式下，在技术和创新方面具有专业知识的私营部门可以与市政府合作。私营实体可以为医院投资最先进的网络安全基础设施，如先进的加密系统和入侵检测软件。作为回报，市政府可以为这些系统的运营和维护提供长期合同，确保私营合作伙伴有稳定的收入来源。

此外，应采用基于风险的投资方法。城市应根据不同医院的规模、数据敏感性和信息技术系统的复杂程度，评估它们面临的潜在网络风险。风险较高的医院将获得更有针对性的基础设施升级投资。这种方法不仅优化了有限资金的使用，还有效提升了医

院网络整体的网络安全弹性。通过实施此类弹性基础设施投资模式，医院在信息化过程中能够更好地抵御网络威胁，保护患者数据和医疗服务的正常运行[13]。

（三）组织能力建设

1. 市企协作培训项目

市企协作培训项目在提升网络空间安全背景下医院信息化建设的组织能力方面发挥着关键作用。市政当局和医疗信息技术服务提供商建立联合技术培训举措。这些举措旨在应对医院信息化建设中的特定挑战。例如，它们专注于传授与医院信息系统相关的最新网络安全威胁的深入知识，如针对患者数据的勒索软件攻击。

培训项目将理论教学与实践操作相结合。市政当局可以引入监管知识和行业最佳实践，而医疗信息技术服务提供商则贡献其在系统开发、维护和安全增强方面的技术专长。通过这些共同努力，医院工作人员，包括信息技术管理员和医务人员，能够更好地应对信息化建设的各个方面。他们学习如何识别医院网络中的潜在安全漏洞、保护敏感医疗数据，并确保信息系统的平稳运行。此外，协作培训还可以在医院信息化生态系统的不同利益相关者之间培养合作意识和信息共享。这种综合培训方法不仅提高了参与者的个人技能，还增强了从网络空间安全角度应对医院信息化建设复杂挑战的整体组织能力。

2. 跨机构协调事件响应框架

跨机构协调事件响应框架在网络空间安全背景下的医院信息化建设中至关重要。当发生大规模医疗数据泄露事件时，不同机构需要有效协作。该框架首先应明确医院、当地卫生部门和相关网络安全机构之间的清晰沟通渠道。例如，建立安全且专用的通信平台以确保实时信息共享。它还需要明确职责划分。每个机构都应确切知道自己负责哪些任务，比如医院负责提供关于数据泄露范围和性质的准确数据，而网络安全机构则专注于分析攻击向量并实施应对措施。此外，该框架应纳入联合培训和演练项目。这些活动可以增强机构间的协调能力，使它们在实际事件发生时能够更顺畅地做出响应。通过定期模拟大规模医疗数据泄露事件，各机构可以加深对事件响应过程的理解，加强合作，最终提高医院信息化建设中跨机构事件响应的整体有效性，以更好地维护网络空间安全。

五、结论

总之，为实现医院信息化中的网络安全弹性，将技术管理进步与市政工程改革相结合至关重要。医疗领域的数字化转型在带来诸多益处的同时，也使医院面临各种网络威胁。通过将这两方面结合起来，医院能够更好地保护其信息系统和患者数据。

展望未来，量化公共卫生基础设施项目中网络安全方面的投资回报率（ROI）意义重大。了解网络安全措施的财务影响和收益，有助于决策者更有效地分配资源。这能让医院在实施安全解决方案的成本与网络攻击可能造成的损失之间找到平衡，确保网络安全投资既合理又有效。

此外，人工智能辅助的市政治理模式的发展是一个充满希望的未来方向。从市政层面来看，人工智能有潜力提高医院信息化管理的效率和准确性。它可以分析海量数据，提前预测网络威胁，并协助制定更具针对性和前瞻性的安全策略。这些未来的研究方向不仅有助于在网络空间安全背景下推进医院信息化建设，也将对数字时代医疗行业的整体发展产生深远影响。

参考文献

[1] 王颖，张丽，刘霞，等 . 医疗信息化中的网络安全挑战：技术管理视角 [J].Journal of Medical Systems(《医学系统杂志》),2021,45(3):112-120.

[2] 陈浩，周明，李琪，等 . 城市健康数据共享平台中的隐私保护机制 [J].Health Informatics Journal(《健康信息学杂志》),2020,26(4):2553-2567.

[3] 古普塔·S, 库马尔·P, 辛格·A K, 等 . 医疗设备网络中的物联网安全漏洞 [J].Computer Communications(《计算机通信》),2022,189:102-115.

[4] 赵锐，王超，黄松，等 . 医疗数据治理的基于区块链解决方案 [J].Future Generation Computer Systems(《下一代计算机系统》),2021,124:273-285.

[5] 刘波，张伟，陈哲，等 . 医疗信息技术基础设施现代化的市政工程路径 [J].Sustainable Cities and Society(《可持续城市与社会》),2019,50:101649.

[6] 金太浩，金成宰，朴英宰，等 . 医院网络安全专业化的人才培养策略 [J].Journal of Healthcare Engineering(《医疗保健工程杂志》),2020,2020:8865807.

[7] 阿尔梅达·F, 席尔瓦·J, 科雷亚·R, 等 . 医疗网络安全系统的预算分配模型 [J].Financial Innovation(《金融创新》),2021,7(1):1-18.

[8] 徐静，刘佳，薛燕，等 . 医疗信息系统的多层防御架构 [J].IEEE Access(《IEEE 接入》),2022,10:23476-23489.

[9] 帕特尔·V, 夏尔马·M, 库马尔·N, 等 . 健康数据管理中的智能合约应用 [J].Neural Computing and Applications(《神经计算与应用》),2021,33(15):9133-9149.

[10] 吴晓，张宇，刘畅，等 . 医疗物联网设备的网络安全认证框架 [J].Mobile Networks and Applications(《移动网络与应用》),2020,25(5):1886-1897.

[11] 张丽，李敏，魏永伟 (Ngai E W T)，等 . 医院信息技术基础设施的弹性投资模型 [J].Information Systems Frontiers(《信息系统前沿》),2022,24(2):599-613.

[12] 汗·S U, 伊斯兰·N, 简·B, 等 . 医疗网络安全的协同培训模型 [J].Education and Information Technologies(《教育与信息技术》),2021,26(5):6017-6038.

[13] 费尔南德斯 - 阿莱曼·J L, 洛佩斯 - 冈萨雷斯·L, 冈萨雷斯 - 塞克罗斯·O, 等 . 医疗数据泄露的事件响应框架 [J].Computer Methods and Programs in Biomedicine(《生物医学计算机方法与程序》),2020,197:105731.

