医疗设备的网络安全挑战和应对

田　淼

陆军军医大学第一附属医院　重庆　400000

摘　要：伴随着信息技术的迅速发展，医疗设备在网络连接和数据传输方面取得了显著进展，为医疗行业带来了诸多便利。然而，这种网络化的医疗设备也面临着日益严峻的网络安全挑战。本文旨在探讨医疗设备网络安全的挑战并提出相应的应对策略。希望为医疗设备网络安全挑战和应对提供深入的理解和有效的解决方案，已保障患者的安全和隐私，推动医疗行业的可持续发展。

关键词：医疗设备；网络安全；数据安全；医疗机构

Cybersecurity challenges and responses to medical devices

Tian Miao

The First Affiliated Hospital of Army Medical University Chongqing 400000

Abstract: With the rapid development of information technology, medical equipment has made remarkable progress in network connection and data transmission, which has brought a lot of convenience to the medical industry. However, such networked medical devices also face increasing cybersecurity challenges. This paper aims to discuss the challenges of medical device network security and put forward corresponding countermeasures. We hope to provide in-depth understanding and effective solutions for medical device cybersecurity challenges and responses, which have guaranteed the safety and privacy of patients and promoted the sustainable development of the healthcare industry.

Key words: Medical equipment, Network security, Data security, Medical institutions

1 引言

1.1 背景

随着科技的发展和医疗水平的提高，医院越来越依赖各种各样的

医疗设备来进行诊断和治疗。而伴随着信息技术的迅速发展，特别是“互联网 + 技术”的发展，既是医院建设中医疗机构落地的实施要求，也是智慧医院建设与信息化发展的必然选择 [1]。医疗设备在网络连接和数据传输方面取得了显著进展。通过网络连接，医疗设备可以实现远程监测、远程诊断和远程手术等功能，为医疗行业带来了巨大的便利和效益。然而，随着医疗设备的网络化趋势不断增强，网络安全问题也逐渐成为医疗行业面临的严峻挑战之一。医疗设备在现代医疗体系中扮演着至关重要的角色，它们不仅为疾病的诊断、治疗和监测提供了关键的支持，还直接关系到患者的生命安全和健康。随着医疗设备的数字化、网络化和智能化发展，网络安全问题已经成为医疗领域面临的重大挑战。保障医疗设备的网络安全具有多方面的重要意义，从患者角度来看，网络安全漏洞可能导致患者的个人隐私信息，如病历、诊断结果、治疗方案等被泄露，这将给患者带来极大的困扰和潜在的风险，如身份盗窃、保险欺诈等；若医疗设备受到网络攻击，可能会出现设备故障、数据错误或操作失控等情况，直接影响到患者的诊断和治疗效果，甚至危及生命；对于医疗机构而言，网络安全事件可能导致医疗服务中断，影响医院的正常运营，损害其声誉和公信力。此外，医疗设备的网络安全问题还可能引发医疗行业的信任危机，影响整个社会对医疗体系的信心。

1.2 研究目的

在当今社会中，医疗设备的网络安全问题日益引人关注。随着技术的不断发展和医疗设备的智能化程度的提高，医疗机构面临着越来越多的网络攻击和数据泄露的风险。本论文旨在探讨医疗设备网络安全所面临的挑战，并提出应对策略，以保障医疗设备的安全性和数据的完整性，在深入探讨医疗设备在网络环境中所面临的安全挑战，并提出切实可行的应对策略，通过对医疗设备网络安全的全面分析，期望能够为医疗机构、设备制造商以及相关监管部门提供有价值的参考，从而加强医疗设备的网络安全防护能力，降低网络安全风险，保障患者的安全和医疗服务的质量。

1.3 研究意义

研究医疗设备网络安全的挑战和应对策略对于提高医疗系统的安全性、保护患者隐私和医疗数据的安全至关重要。本研究的结果可以为医疗机构和相关领域的从业人员提供有效的指导和建议。一方面有助于提高医疗机构对医疗设备网络安全的重视程度，推动其建立完善的网络安全管理体系；另一方面，促进医疗设备制造商在设计和生产过程中更加注重网络安全，提高设备的安全性和可靠性。同时，也为相关法规和标准的制定与完善提供理论依据，促进整个医疗行业的网络安全水平提升，以适应数字化医疗时代的发展需求。

2 医疗设备的网络安全

2.1 网络化的医疗设备

医疗设备的网络安全至关重要，因为它涉及到人们的生命和健康。现代医疗设备普遍具备网络连接功能，可以与医疗信息系统进行数据交互，支持远程协作和远程监控等功能。这些设备包括但不限于医疗影像设备、手术机器人、健康监测设备等。医疗设备的数据交互使得医疗机构的信息系统更加脆弱和容易受到攻击。由于医疗设备与医疗信息系统之间的数据传输需要经过网络，这就增加了黑客入侵的可能性。如果黑客成功侵入系统，他们可以窃取敏感的病人数据、篡改医疗报告或者干扰医疗过程，对患者的生命和隐私构成威胁。由于医疗设备的复杂性和多样性，其网络安全管理也变得更加困难。医疗机构通常拥有大量的医疗设备，每个设备都需要进行网络配置、漏洞修补和访问权限管理等工作。这些任务对于医疗机构的 IT 团队来说是一项巨大的挑战，要求他们具备专业的知识和技能来应对各种不同类型的设备和安全问题 [2]。

2.2 医疗设备联网规模不断扩大

随着信息技术的迅猛发展和医疗行业数字化转型的加速，医疗设备的联网规模呈现出持续增长的态势。如今，从大型的医院影像设备如 CT、MRI 到小型的床边监护仪、输液泵，再到便携的血糖仪、智能手环等可穿戴设备，越来越多的医疗设备实现了与网络的连接。这种联网规模的扩大得益于多种因素。医疗技术的进步使得设备的智能化程度不断提高，为实现联网功能提供了技术基础。例如，先进的传感器技术能够实时采集患者的生理数据，并通过网络传输到医疗信息系统中，方便医生进行远程诊断和监测。医疗机构为了提高医疗服务的效率和质量，积极推动医疗设备的联网化。通过将设备接入网络，实现医疗数据的共享和协同处理，有助于优化医疗流程、减少医疗差错。医疗设备联网规模的不断扩大也带来了一系列新的挑战。大量设备的接入增加了网络的复杂性，使得网络管理和维护的难度加大。同时，由于联网设备数量众多，潜在的攻击面也随之扩大，网络安全风险显著增加。此外，不同类型和厂家的医疗设备在联网标准和协议上可能存在差异，导致设备之间的兼容性问题，影响数据的准确传输和系统的稳定运行。为了应对这些挑战，医疗机构需要加强网络基础设施建设，提升网络的承载能力和稳定性。同时，应建立统一的设备联网标准和规范，确保设备之间的互联互通和数据安全。此外，还需加强对联网医疗设备的安全监测和管理，及时发现和处理潜在的安全威胁，保障医疗设备的正常运行和患者的医疗安全。

2.3 数据安全

医疗设备涉及大量敏感患者信息和医疗数据，保护数据的安全性是医疗设备网络安全的重要方面 [3]。数据加密、访问控制、审计等措施都是保障数据安全的关键。在医疗领域，数据保护不足是一个严峻的问题。随着医疗设备的联网和数字化，大量敏感的患者数据被生成、收集和存储。然而，当前的数据保护措施往往未能跟上技术发展的步伐。医疗设备在收集和传输患者数据时，缺乏足够的加密和认证机制。这使得数据在传输过程中容易被窃取或篡改。许多设备使用的是不安全的通信协议，为黑客入侵提供了可乘之机。而医疗机构在存储患者数据时，存在数据存储位置不明确、访问控制不严格等问题。部分医疗机构可能将数据存储在安全性较低的服务器或云端，容易遭受网络攻击导致数据泄露。同时，内部人员对数据的访问权限管理不善，可能导致未经授权的人员获取患者敏感信息。医疗机构在处理数据时，可能未遵循严格的数据处理规范和隐私政策。例如，在数据分析和共享过程中，未能充分去标识化患者数据，增加了患者隐私泄露的风险。数据保护不足不仅损害了患者的隐私权，还可能导致患者对医疗机构的信任度下降，甚至引发法律纠纷。同时，大规模的数据泄露事件还可能对整个医疗行业的形象和发展造成负面影响。为解决数据保护不足的问题，医疗机构应加强数据加密技术的应用，完善访问控制机制，建立严格的数据处理流程和规范，并加强对员工的数据安全培训，提高数据保护意识。

3 应对策略

3.1 加强设备安全性

医疗设备制造商应加强设备的硬件和软件安全性设计，包括漏洞修复、访问控制、身份认证等机制，减少设备被攻击的风险。首先，医疗设备制造商应定期对设备进行漏洞修复，随着技术的发展和黑客攻击手段的不断演进，设备中可能存在的漏洞会成为黑客入侵的突破口。因此，制造商应密切关注漏洞信息，及时发布补丁程序，并提醒用户技师进行更新。再者，医疗设备制造商还应在设计过程中考虑安全性。如可靠的芯片、加固物理安全措施等，防止设备被非法拆解或篡改；同时在软件开发阶段采用安全编码规范，并进行安全审计和测试。

3.2 建立有效的网络防护

医疗机构应建立完善的网络安全防护措施，包括入侵检测系统、防火墙、网络隔离等，及时发现和应对网络攻击

行为，通过实时监控和分析数据包，入侵检测系统能迅速发现黑客攻击、漏洞利用或其他恶意行为，从而提供医疗机构确保网络安全的第一道防线。其次，医疗机构还应配置强大的防护墙技术，组织未经授权的访问、防范恶意软件的传播，并限制医疗数据的泄露风险。此外，为进一步确保网络安全，医疗机构还可以采用网络隔离措施。通过分割内部网络，将不同系统和设备隔离开来，可以有效减少可能的攻击面。通过限制特定用户或设备的访问权限，医疗机构可以降低潜在攻击者获取敏感信息的风险。

3.3 加强数据加密

医疗设备在数据传输和存储过程中应采用强大的数据加密算法，确保数据的机密性和完整性。首先，医疗设备应采用强大的数据加密算法，以保证数据的秘密性和完整性。这些算法应基于最新的密码学标准，如 AES-256 或 RSA，以提供高强度的加密保护；其次，为有效应对日益复杂的网络威胁，医疗设备应采取多重层级的加密措施，除了端到端的数据传输加密，设备本身也应具备数据存储加密功能。为确保数据加密的有效性和可信性，医疗设备制造商和相关机构应建立同意的数据加密标准和认证机制。这些标准应涵盖加密算法选择、密匙管理、安全审计等方面，以确保医疗设备在涉及和生产阶段就具备数据安全的基础。还要建立全面的安全管理体系，包括访问控制、身份认证、漏洞修补等方面的措施，只有在这样的综合保护机制下，医疗设备才能确保数据传输和存储过程中的机密性、完整性和可用性。

3.4 加强人员培训

医疗机构应加强员工的网络安全培训，提高其网络安全意识和技能，增强对网络威胁的防范能力。首先，医疗机构可以定期举办网络安全培训课程，以提高员工的网络安全意识和技能。这些培训应包括识别和防范常见的网络威胁，如钓鱼攻击、恶意软件和数据泄露，以及正确使用和保护个人设备的方法。其次，医疗机构可以组织模拟演习和实践活动，让原亲身体验网络共计并学习应对策略，以提高员工迅速识别和应对网络攻击的能力，从而提高他们的反应速度和处理能力。加强员工的网络安全培训，可以提高其整体的网络安全防护能力，减少网络威胁对患者隐私和数据安全的潜在风险。这不仅是对寂寥机构自身的责任，也是对患者和数据保护的一种保障。

3.5 完善法律和监管机制

应加强对医疗设备网络安全的监管，制定相应的法律法规和标准，推动医疗机构和设备制造商履行网络安全责任。首先，相关机构应加强对医疗设备网络安全的监管，这包括成立专门的机构来负责监督和评估医疗设备的网络安全性能，及时发现和解决潜在的漏洞和威胁。同时，应建立健全网络安全标准，明确规定医疗设备商和医疗机构在网络安全方面的责任和义务。其次，我们需要制定相应的法律法规来规范医疗设备的网络安全[4]。这些法律法规应涵盖设备设计、生产、销售、维护和使用等各个环节，保证医疗设备在设计和制造过程中就具备良好的网络安全性能，并规定了必要的测试和验证程序。此外，法律法规还应明确医疗机构和设备制造商的网络安全责任和违规行为的处罚措施。最后医疗机构应建立完善的网络安全管理体系，加强设备的安全审查和监测，确保设备在运行过程中不受到网络攻击和数据泄露的威胁。

4 结论与展望

针对医疗设备网络安全所面临的挑战，本论文提出了一系列应对策略，包括加强设备安全性，医疗设备制造商应在设计阶段就强化安全性，进行严格的安全测试与认证，确保设备的硬件和软件具备足够的安全性，并及时提供更新和维护服务；建立有效的网络防护、加强数据加密，运用先进的技术防护手段，如加密技术、防火墙、入侵检测系统等，保障数据传输和存储的安全；加强人员培训，医疗机构需建立全面的安全管理制度，涵盖设备采购、使用、维护等环节，定期进行安全审计，及时发现和处理潜在的安全隐患，加强对医务人员和相关工作人员的网络安全培训，提升其安全意识和应急处理能力，制定并演练应急响应机制；完善法律和监管机制，政府和行业应推动完善相关法规和标准，加强对医疗设备网络安全的监管，确保行业规范的及时性和有效性。这些策略的实施能够有效提升医疗设备网络安全水平，保障医疗系统的稳定运行和患者数据的安全性。在当今数字化时代，医疗设备网络的安全至关重要，我们应不断探索创新的的剖剿方案，比如人工智能与机器学习的应用，可否用于实时监测和预测潜在的网络安全威胁，实现更快速和精准的安全防护；再比如零信任架构的普及，医疗行业将逐渐采用零信任原则，默认不信任任何内部和外部的访问请求，在访问前进行严格的身份验证和授权；还有持续的安全意识教育，不仅针对医疗机构的工作人员，还包括患者，以形成全民重视医疗设备网络安全的良好氛围。积极参与相关讨论和研究，以推动医疗设备网络安全的进一步发展。

参考文献：

[1] 何辉 . 5G 技术下的医院急救医疗设备及其网络安全体系探究 [J]. 中国设备工程 ,11671-0711（2023）05（下）-en0063-03

[2] 于雪梅 . 医疗设备网络与数据安全防护体系研究 [J]. 中国数字医学，2022,17（02）：13-16

[3] 国家标准化管理委员会物联网术语：GB/T33745-2017[S] 北京：中国标准出版社，2017

[4] 张茫茫，郑焜，沈云明，等 . 医院联网医疗设备安全管理 [J]，中国医疗器械杂志，2018,42（04）：303-312