移动医疗医院信息网络安全分析及措施探究

强　皑
宁夏医科大学总医院信息中心　宁夏　银川　750000

摘　要：本文从多个方面探讨了移动医疗医院信息网络安全的分析及措施，包括网络攻击威胁、数据泄露威胁和设备安全威胁的识别，以及加强网络安全管理、加密存储和传输数据、实施安全审计和监控、加强保密意识、定期开展网络风险评估、合理规划网络安全架构以及强化员工安全意识等措施的落实。同时，医疗机构应积极与专业高防服务商合作以应对DDoS攻击等网络安全威胁。

关键词：移动医疗；医院信息；网络安全；措施探究

引言：随着移动医疗应用的普及和深入，医院信息网络的安全性变得越来越重要。移动医疗应用涉及到大量的敏感信息和患者隐私，一旦发生信息泄露或被非法使用，会对患者的隐私和医院的声誉造成极大的损害。因此，如何保障医院信息网络的安全性和可靠性，成为了一个亟待解决的问题。本文将从移动医疗医院信息网络安全分析及措施探究的多个方面进行详细的阐述，旨在为医疗机构提供一套有效的信息网络安全管理和防护方案，保障患者隐私和数据的安全，提高医疗服务的整体质量和水平。

1 移动医疗医院信息网络安全分析

（1）网络攻击威胁。移动医疗应用涉及到医院内部的大量敏感信息，如患者病历、医生诊断、药物处方等。这些信息如果被非法获取或滥用，会对患者的隐私造成侵犯，同时也会对医院和医生造成声誉和法律风险。网络攻击者可能通过各种手段，如钓鱼邮件、恶意软件、SQL注入等，入侵医院信息网络，获取敏感信息并进行非法活动。（2）数据泄露威胁。移动医疗应用需要处理大量的医疗数据，这些数据往往包含了患者的个人隐私和健康状况等信息。如果数据泄露或被篡改，可能会对患者造成伤害，也可能导致医疗纠纷或法律诉讼。数据泄露可能发生在数据的传输、存储和使用等各个环节，攻击者可能通过截获、分析数据流，窃取敏感信息或者进行恶意攻击[1]。（3）设备安全威胁。移动医疗设备，如可穿戴医疗设备、移动医疗app等，也可能存在安全漏洞。黑客可能利用这些漏洞，控制设备或窃取患者数据，给患者带来安全隐患。例如，攻击者可能通过漏洞利用，在患者不知情的情况下收集患者的敏感信息，或者控制设备的运行，甚至可能导致设备的损坏或失效。

2 移动医疗医院信息网络安全措施

2.1 加强网络安全管理

（1）医院应明确各级人员的职责和权限，实行安全责任制，确保每个人都能够承担起保护信息安全的责任。其次，医院应建立健全的安全管理制度和操作规范，包括数据备份、密码管理、访问控制、网络安全等方面的制度和规定，使员工在进行日常工作时有章可循、有规可依。同时，医院应加强对员工的安全教育和培训，提高员工的安全意识和技能水平，使其能够正确地使用和管理移动医疗设备和应用，避免出现安全风险。（2）设立专门的网络安全管理团队，负责制定和执行安全策略、监控网络运行情况、及时发现和处理安全威胁。这个团队应具备专业的网络安全知识和技能，能够对网络进行全面深入的分析和研究，发现并解决潜在的安全风险。同时，医院应建立健全的安全审计和监控机制，对网络进行实时监控、检测异常行为、记录安全事件，及时发现和处理安全威胁，确保网络的安全稳定。（3）加强对移动医疗设备和应用的管理。对于移动医疗设备，医院应建立严格的安全管理制度，确保设备的采购、使用、维修和报废等各环节都得到安全管理。同时，对于设备的操作系统和应用软件，应定期进行安全更新和升级，以防范安全漏洞。对于设备的访问和使用权限应进行严格控制，防止未经授权的访问和使用。另外，医院还应加强对移动医疗应用的管理，确保应用的数据安全和隐私保护符合国家法律法规和行业标准，避免数据泄露和滥用。

2.2 加密存储和传输数据

（1）医院应认识到加密存储和传输数据的重要性。敏感信息和数据如果未经过加密处理，一旦被非法获取或滥用，不仅会对患者的隐私造成侵犯，也会对医院和医生造成声誉和法律风险。因此，医院应采用高级的加密技术，对敏感信息和数据进行加密存储和传输。（2）应选择经过严格验证的加密算法，确保数据的机密性和

完整性。在选择加密算法时，医院应考虑算法的强度、性能、易用性等多个方面，确保算法能够有效地保护数据安全。同时，医院应定期对加密算法进行更新和升级，以防范新型攻击手段。这可以通过采用最新的加密算法、加强密钥管理、定期更换密钥等方式实现。（3）建立健全的加密管理制度。医院应明确加密密钥的管理责任、加密算法的使用范围、加密操作的流程和规范等内容，使员工在进行加密操作时有章可循、有规可依。同时，医院应加强对加密操作的管理和监督，及时发现和处理加密过程中的问题，确保数据的机密性和完整性。

2.3 严格控制设备安全

（1）建立完善的移动医疗设备管理制度。这个制度应包括设备的采购、使用、维修和报废等各环节的安全管理。在采购环节，医院应选择具有良好安全性能的设备，并进行严格的安全检测和测试，确保设备本身不存在安全漏洞。在使用环节，医院应制定严格的安全操作规程，规范员工的使用行为，避免未经授权的访问和使用。在维修和报废环节，医院应加强设备的安全审查和监督，确保设备的数据安全和隐私保护符合国家法律法规和行业标准。（2）加强对移动医疗设备的操作系统和应用软件的安全管理。设备的操作系统和应用软件是设备安全的关键部分，如果存在安全漏洞，就可能导致未经授权的访问和使用。因此，医院应定期对设备的操作系统和应用软件进行安全更新和升级，以防范安全漏洞。同时，对于存在安全漏洞的设备，医院应立即采取安全措施，例如停用或隔离设备，以防止安全风险的扩大[2]。（3）加强对移动医疗设备的访问和使用权限的管理。医院应建立完善的权限管理制度，规范设备的访问和使用权限。只有经过授权的人员才能访问和使用设备，而且只能访问自己所需的数据或应用程序。

2.4 实施安全审计和监控

随着信息技术的发展，医院的网络系统日益复杂，各种应用系统、设备和数据相互关联，网络安全风险也随之增加。（1）安全审计是指对医院网络系统进行全面、系统的检查和评估，以发现潜在的安全隐患和漏洞。通过安全审计，医院可以了解网络系统的安全状况，为制定相应的安全策略和措施提供依据。安全审计的主要内容包括：对网络设备的审查，如防火墙、路由器等；对网络应用系统的审查，如HIS、PACS等；对网络访问权限的审查，如用户权限分配、访问控制策略等；对网络数据安全的审查，如数据备份、恢复策略等。（2）监控是指对医院网络系统进行实时或定期的观察和检测，以发现异常行为和安全事件。通过监控，医院可以及时发现网络安全威胁，采取相应措施防范和应对。监控的主要内容包括：对网络流量的监控，如数据包捕获、分析等；对异常行为的监控，如非法访问、恶意攻击等；对安全事件的监控，如病毒爆发、数据泄露等。（3）加强组织管理和技术支持。一方面，医院应建立健全的安全管理部门，负责组织、协调、指导网络安全工作。另一方面，医院应加大技术投入，引进先进的安全审计和监控设备和技术，提高网络安全管理水平。同时，医院还应加强员工的安全意识和培训，提高全体员工的网络安全素质。

2.5 加强保密意识

（1）应该制定和实施严格的保密政策和流程。这些政策和流程应该明确规定哪些数据是机密的，谁有权访问这些数据，以及如何存储、传输和销毁这些数据。此外，医疗机构还应该为员工提供相关的培训和教育，使他们了解保密政策的重要性，并掌握正确的数据处理方法。（2）应该采取技术手段来保护数据的安全性。这包括使用加密技术对敏感数据进行加密，以防止未经授权的人员访问。同时，医疗机构还应该建立防火墙和入侵检测系统，以保护网络免受恶意攻击。此外，定期备份数据也是重要的一环，以防止数据丢失或损坏。（3）还应该与供应商和合作伙伴建立保密协议。这些协议应该明确规定对数据的保护要求，包括数据的安全存储、传输和销毁。同时，医疗机构还应该定期审查和评估合作伙伴的保密措施，确保他们符合保密要求。（4）建立监测和报告机制，及时发现和应对潜在的数据泄露风险。这包括定期进行安全审计和漏洞扫描，以及建立紧急响应计划，以便在发生数据泄露时能够迅速采取措施。

2.6 定期开展网络风险评估

随着信息技术的不断发展，医疗机构的信息系统面临着越来越多的网络威胁和攻击。因此，定期开展网络风险评估工作，特别是对医疗信息系统进行渗透测试等技术评估，可以帮助医疗机构及时发现和解决潜在的网络安全问题，提高信息系统的安全性和可靠性。（1）网络风险评估可以全面了解医疗机构的网络安全状况。通过对医疗机构的网络系统、设备和应用进行全面的检查和评估，可以发现系统中存在的漏洞和弱点，确定潜在的安全风险。这包括对网络架构、防火墙配置、访问控制策略、密码策略等进行评估，以及对应用程序的安全性进行审查。通过全面的评估，医疗机构可以了解自身的网络安全水平，为后续的安全改进提供依据[3]。（2）渗透测试是一种有效的技术评估方法，可以帮助医疗机构发现系统中的安全漏洞和弱点。渗透测试是通过模拟

真实的攻击方式，尝试绕过系统的安全防护措施，获取未授权的访问权限。通过渗透测试，医疗机构可以发现系统中存在的安全漏洞，如弱密码、未及时更新的软件补丁、未经授权的访问等。这些漏洞如果被黑客利用，可能会导致患者数据的泄露或丢失，给医疗机构带来严重的法律和声誉风险。因此，渗透测试是医疗机构网络风险评估中必不可少的一环。（3）网络风险评估还可以帮助医疗机构制定和优化信息安全策略和措施。通过对网络风险的评估，医疗机构可以了解自身的安全需求和目标，并制定相应的安全策略和措施。例如，对于发现的漏洞和弱点，医疗机构可以采取修补漏洞、加强访问控制、加密敏感数据等措施来提高系统的安全性。同时，网络风险评估还可以帮助医疗机构优化资源分配，合理规划信息安全预算，确保安全措施的有效实施。（4）网络风险评估需要由专业的安全团队进行。医疗机构应该聘请具有丰富经验和专业知识的安全团队来进行网络风险评估工作。这些安全团队应该具备渗透测试、漏洞分析、安全策略制定等方面的专业技能，能够全面评估医疗机构的网络安全状况，并提供针对性的解决方案和建议。同时，医疗机构还应该与安全团队建立长期的合作关系，定期进行网络风险评估，及时跟进和解决安全问题。

2.7 与专业高防服务商合作

（1）与专业高防服务商合作可以为医疗机构提供专业的DDoS防护解决方案。专业高防服务商拥有丰富的经验和专业知识，能够根据医疗机构的具体需求和情况，提供定制化的DDoS防护方案。这些方案通常包括流量清洗、黑名单管理、入侵检测和防御等功能，能够有效地抵御DDoS攻击，保护医疗机构的网络和业务。（2）专业高防服务商通常拥有强大的防护能力。他们拥有全球分布的防护节点和带宽资源，能够实时监测和分析网络流量，及时发现并阻断恶意流量。同时，他们还具备快速响应和处置能力，一旦发生DDoS攻击，能够迅速采取措施进行防护和恢复，最大限度地减少攻击对医疗机构的影响。（3）还可以为医疗机构提供全天候的技术支持和服务。专业高防服务商通常拥有24小时的技术支持团队，能够及时响应和解决医疗机构在遭遇DDoS攻击时遇到的问题。他们会与医疗机构保持密切的沟通和合作，共同制定应急预案和响应策略，确保在攻击发生时能够迅速采取行动，保障业务的连续性和稳定性。（4）帮助医疗机构降低安全风险和成本。由于专业高防服务商拥有先进的技术和设备，能够提供高效和可靠的DDoS防护服务，医疗机构不需要自行投资和维护安全防护设备和团队。这样不仅可以降低医疗机构的安全风险，还可以节省人力和物力成本，使医疗机构能够更加专注于提供优质的医疗服务。专业高防服务商能够为医疗机构提供专业的DDoS防护解决方案、强大的防护能力、全天候的技术支持和服务，帮助医疗机构降低安全风险和成本。因此，医疗机构应该积极寻求与专业高防服务商的合作，共同应对网络安全挑战，保障患者隐私和数据的安全。

结束语

医院信息网络安全的保护是医疗机构不容忽视的重要问题。本文从多个角度出发，提出了一系列针对性的措施和建议，以帮助医疗机构更好地应对网络安全风险和挑战，确保移动医疗应用的安全性和可靠性，为患者提供更加优质的医疗服务。同时，医疗机构应积极与专业高防服务商合作，共同应对DDoS攻击等网络安全威胁，确保医疗业务的正常运转和持续发展。

参考文献

[1]黄河.移动医疗医院网络信息安全问题的探讨[J].数字通信世界，2020（07）：147-148.

[2]接明利，毕旭峰，陈文涛.移动医疗在医院信息化建设中的实践研究[J].中国新通信，2020，22（09）：103.

[3]姜丛吾.移动医疗医院信息网络安全和对策探索[J].科技创新导报，2020，17（09）：140+142.