医疗器械的网络安全挑战与对策

郑新波

广东迈科医学科技股份有限公司，广东省广州市，510700；

摘要：随着医疗器械越来越多地联网和集成智能功能，网络安全问题变得日益突出。本文分析了医疗器械在联网后面临的网络安全挑战，包括数据泄露、设备操控和恶意软件攻击等风险。文章探讨了如何通过技术手段和管理措施来保护医疗器械免受网络攻击，包括加密技术、安全协议和定期的安全评估。同时，讨论了医疗器械制造商和医疗机构在确保网络安全方面的责任和合作。

关键词：医疗器械；网络安全；数据泄露；设备操控；防护措施。

DOI:10.69979/3029-2808.24.7.032

引言

随着信息技术的飞速发展，医疗器械行业正经历着数字化转型。作为医疗服务中不可或缺的组成部分，医疗器械的功能不再局限于传统治疗诊断，且集成互联智能功能，如远程监控、数据分析和云计算等。这些技术的应用，大大提高医疗服务的效率质量，但也带来网络安全挑战。所以医疗器械的网络安全不仅关系患者的健康和隐私，还影响医疗机构的运营、医疗行业的声誉。

所以，全球医疗行业关注的焦点风险，包括联网医疗器械的数据泄露、设备操控和恶意软件攻击等。数据泄露将导致患者隐私受侵犯、敏感医疗信息外泄，设备操控将威胁患者生命安全，而恶意攻击则容易导致医疗服务中断，造成重大影响和经济损失。因此，医疗器械的网络安全已成为医疗行业亟待解决的问题。

本文旨在分析医疗器械联网后面临的安全挑战，并探讨如何通过技术手段和管理措施来保护医疗器械免受攻击。同时，本文还将讨论医疗器械制造商和医疗机构在确保网络安全方面的责任和合作，以及建立有效的合作机制应对网络安全威胁。

1 医疗器械网络安全的当前态势

目前，越来越多的医疗器械趋于智能化，也需联网使用，大大提高了医疗服务的效率质量。然而也存在网络安全风险隐患，导致医疗器械像其他计算机系统一样，容易受安全漏洞的影响，并影响其安全性和有效性。目前世界各国对医疗器械网络安全越来越重视，逐步完善相关法规标准。

通过现状和发展趋势表明，保护医疗器械产品自身及相关数据不受未授权活动影响，尤为重要。这涉及到医疗器械的保密性、完整性、可得性及真实性、抗抵赖性、可核查性、可靠性等特性。这些特性的相关风险，需在医疗器械全生命周期中处于可接受水平，确保安全及有效性。

而网络安全对医疗器械行业的影响是深远的。恶意软件、勒索软件和数据泄露等网络威胁的发生，促使更强大的网络安全解决方案，用于保护医疗设备。此外，医疗器械网络安全解决方案市场，未来几年内将实现显著增长，从 2022 年的 82 亿美元增长至 2030 年的 405 亿美元，显示出市场对医疗器械网络安全的高度关注和需求，也从侧面了解医疗器械网络安全保护的重要性和紧迫性

综上，医疗器械网络安全的当前态势是挑战与机遇并存。随着医疗器械的网络化和智能化，网络安全已成为行业发展的关键因素，需要行业内外的共同努力和持续关注，以确保医疗器械的安全性和有效性，保护患者健康和数据安全。

2 医疗器械网络安全的挑战

2.1 数据泄露风险

由于在提供医疗过程中，医疗器械会处理大量敏感数据，包括患者身份信息、医疗记录和健康数据，如果泄露将导致患者隐私受到侵犯。该风险可能来自于黑客攻击，还可能因为内部人员的操作不当导致。例如，使用不安全的通信协议或网络设置、默认密码、未加密的通信等都容易使设备受攻击导致数据泄露。

2.2 设备操控威胁

医疗器械设备操控威胁，涉及到攻击者通过远程或物理手段操控医疗设备，如监护仪、输液泵等，干扰设备正常功能，危害患者生命安全。这种操控可能通过未授权访问设备控制系统、利用设备的漏洞或通过其他方式实现。其严重性在于它能直接导致临床医疗事故，对患者造成严重影响。

2.3 恶意软件攻击

恶意软件攻击是医疗器械网络安全面临的另一个重要挑战。恶意软件会影响医疗设备和系统，导致服务中断或数据损坏，破坏医疗设备的正常运行，影响患者治疗的连续性和效果，造成巨大损失，凸显恶意软件攻击严重性。

这些挑战表明，医疗器械网络安全复杂的问题，需从技术、管理和法律等多方面考虑。随着网络威胁的演变，医疗器械网络安全的挑战也不断变化，要求行业、医疗机构和监管部门持续关注，并采取有效措施，确保保障医疗器械的网络安全。

3 技术手段在网络安全中的应用

多方面的技术手段，为医疗器械提供了必要的识别、保护能力，以及适当的探测、响应和恢复能力。

3.1 加密技术

加密技术是保护医疗器械数据传输安全的重要手段之一。通过加密数据降低泄露风险。主要方式包括：（1）数据传输加密：在经认证的节点之间传输健康数据时，采用数据传输加密技术，如 SSL/TLS 加密协议，确保数据的保密性和完整性；（2）固态加密设备：此方式可保护存储在医疗器械中的数据，防止未经授权的访问和数据泄露；（3）密钥管理：包括采用对称加密、非对称加密或混合加密技术来管理密钥，确保安全性。

3.2 安全协议

除加密技术外，安全协议在增强医疗器械网络安全方面，也起着核心作用，为数据传输提供标准化的安全措施。一是节点身份验证。在传输健康数据时使用该技术，可确保发送方和接收方相互识别并授权传输。二是基于角色的访问控制（RBAC）。为设备创建基于角色的访问控制，控制监视网络活动，并对不同用户设定使用权限。

3.3 定期安全评估

定期安全评估是预防网络攻击的重要环节。而其可以通过不同方式来发现潜在风险；包括采取定期扫描查找代码漏洞、利用渗透测试来发现计算机系统的安全脆弱性、进行安全风险评估识别潜在威胁源等等。也包括制定相应的风险管理政策。

当然除上面提及的技术外，还需要做好网络安全补丁定时升级、对医疗器械中所使用的现成软件指定明确清单及记录，确保网络安全性的同时，也更方便进行安全管理和更新。

3.4 管理措施在网络安全中的重要性

管理措施的重要性，在于不仅能为医疗器械网络安全，提供组织架构和政策支持，还能确保技术措施得到有效执行，并在发生事件时快速响应。

1.人员培训和意识提升

对医护人员和相关管理人员进行定期网络安全培训，以提升网络安全意识，使其可以感受到潜在的网络威胁，如钓鱼攻击、恶意软件等，并知道如何采取预防措施。此外，培训还应包括如何在发生安全事件时报告响应，以及维护数据的保密性和完整性。

2.政策和法规遵从

遵从医疗器械网络安全的的法律法规，是确保网络安全的基石。如《中华人民共和国网络安全法》《中华人民共和国数据安全法》等，及行业特定的网络安全标准和指南，例如 IEC 80001 系列标准。这些法律法规为网络安全提供了法律框架，确保了医疗器械在设计、开发、生产、使用和维护过程中的网络安全。

3.应急响应计划

建立应急响应计划是管理网络安全的关键措施之一。计划应包括对网络安全事件的识别、评估、响应和恢复等步骤。要求负责的团队应实时监测网络安全状态。一旦发现安全威胁，能迅速启动应急响应流程，采取措施控制和缓解安全事件的影响，并事后进行彻查恢复工作。

4.审计和合规性检查

定期进行网络安全审计和合规性检查是确保医疗器械网络安全的重要环节。通过审计，组织可以识别和评估网络安全风险，确保现有的安全措施和控制有效，并符合相关的法律法规要求。审计结果可以用来更新和优化网络安全策略，提高组织的网络安全管理水平。

4 网络安全对策的实施与案例分析

4.1 对策实施的策略

为有效应对医疗器械网络安全挑战，实施策略需要从预防、检测、响应和恢复四个关键阶段进行规划和执行。

（1）预防阶段。一是做好风险评估，识别潜在的安全漏洞和威胁；二是做好安全设计。即在医疗器械的设计阶段就融入安全原则，确保产品一旦成型便具备安全特性；三是做好使用人员的培训工作；四是实施严格的访问控制政策，确保只有授权人员才能访问敏感数据和系统。

（2）检测阶段。在机器使用运行期间，应做好实时监控，以便及时发现可疑活动和潜在威胁，同时做好

操作日记的管理工作，以便于在发生安全事件时进行追踪和分析。如果条件允许的情况下，为医疗器械部署入侵检测系统级防御系统，用于识别和阻止恶意行为

（3）响应阶段。应急计划的指定、安全团队的有效响应、沟通机制的健全和通畅，都是确保网络安全受到挑战的时候，能快速处理。

（4）恢复阶段。在消灭隐患后，保护团队应制定计划、做好数据备份、分析总结，确保发生事件后能快速恢复业务，更新安全策略，最小化对患者护理和医疗服务的影响。

4.2 案例分析

在全球范围内，医疗器械网络安全事件时有发生，它们揭示了网络安全风险的严重性，以及应对措施的重要性。

（1）山西原平市第一人民医院网络安全事件。该医院因门户网站存在安全漏洞而被处以行政警告处罚。调查发现，医院网络安全意识淡薄，未履行网络安全等级保护制度，未采取防范计算机病毒和网络攻击等技术措施，严重影响了医院网站的信息安全。此案例凸显了医疗机构在网络安全防护上的不足，以及遵守网络安全法规的必要性。

（2）黑客入侵医院服务器事件。在 2018 年，广东、重庆多家三甲医院服务器被黑客入侵，攻击者利用有道笔记的分享文件功能下载多种挖矿木马，独占服务器资源挖矿。我国医疗机构开放远程登录服务的比例高达 50%，这意味着有一半的服务器可能遭遇相同的攻击。

（3）上海市公安局通报医院 CT 机遭黑客软件破解事件。2022 年 12 月 27 日，上海市公安局发布了一则案例。不法分子利用黑客软件破坏医学影像设备技术防护措施，私自复制刻录盗版软件并制作非法破解工具，销售后牟利千万元。此事件导致上海多家医学影像领域头部企业的 CT 机、核磁共振等设备屡屡出现故障。

（4）Tenet Healthcare 医疗集团网络安全事件：2021 年 4 月，总部位于达拉斯的 Tenet Healthcare 医疗集团遭受攻击，其 550 多个急诊医疗业务被迫中断，其中包括在马萨诸塞州救护车无法调度，佛罗里达州的医院无法使用电子病历系统。由于网络漏洞的存在，该医疗集团停止了业务运营，并在一周后发布了相关事件情况公告。

这些案例分析表明，医疗器械网络安全事件，不仅导致患者隐私泄露、医疗服务中断，还可能对患者的生命安全构成威胁。因此，医疗机构必须重视网络安全建设，加强防护措施，提高应急响应能力，以确保患者安全和数据保密性。

4.3 效果评估

在医疗器械网络安全对策的效果评估中，可采取综合性方法，从技术层面、管理流程和法规遵从等多个维度进行。评估过程中，应依据国家药监局发布的《医疗器械网络安全注册审查指导原则（2022 年修订版）》等标准，对网络安全能力进行了细致的检查，确保满足行业最新要求。同时参考了国际标准，如 IEC 80001 系列，以评估网络安全和风险管理的实践。

在技术层面，可运用深度学习方法来识别和响应网络攻击，更准确地评估网络安全态势。管理流程方面，通过建立信息安全事件管理机制，包括事件响应计划和准备，确保在发生网络安全事件时能够迅速有效地应对。

综合评估，能全面了解网络安全对策的效果，不仅在技术防护上取得进步，也在管理流程和法规遵从上实现提升，确保医疗器械的网络安全措施能够适应不断变化的网络威胁环境。

5 结论

本文综合探讨了医疗器械网络安全的挑战与对策，强调了随着医疗器械的联网和智能化，网络安全问题变得尤为突出。面对数据泄露、设备操控和恶意软件攻击等风险，医疗器械制造商和医疗机构必须采取全面的技术与管理措施，以确保医疗器械的安全性和有效性。

网络安全是一个动态领域，随着技术发展和网络威胁的演变，医疗器械网络安全的挑战也在不断变化。因此，持续关注网络安全的最新发展，不断更新和改进网络安全策略和措施是必要的。总之，通过有效的对策、合作和技术创新，可以有效地应对网络安全挑战，保护医疗器械免受网络攻击，确保医疗服务的连续性和患者数据的安全。

参考文献

[1]陈钿,曾祥卫,孙志刚,等.人工智能医疗器械软件网络安全技术考量[J].中国医疗器械信息,2022,28(15):5-7.DOI:10.15971/j.cnki.cmdi.2022.15.047.

[2]吴琼,兰坤,王艳.医院网络安全与系统监控管理平台建设应用与实践[J].电子技术与软件工程,2019,(09):189.

[3]肖斌,陆晓琳.医疗器械的网络安全质量控制途径分析[J].中国设备工程,2023,(10):247-249.