互联网背景下医疗信息安全面临的挑战及对策

王映涛　朱永坚

（无锡市锡山人民医院，江苏 无锡　214105）

摘　要：互联网技术在医疗领域的应用既提升了医院的信息化水平，也有助于医疗资源的优化配置，为患者就医带来了极大的便利。但伴随着移动互联网的快速发展，医疗信息安全也开始受到广泛重视。基于此，笔者针对互联网背景下我国医疗信息安全面临的挑战展开分析，并对推动医疗信息安全的升级发展提出了几点建议，希望能够为相关研究提供借鉴。

关键词：互联网；医疗；信息化；信息安全

中图分类号：R197.323　　**文献标识码：**A　　**文章编号：**1003-9767（2019）19-218-02

The Challenges and Countermeasures of Medical Information Security under the Background of Internet

Wang Yingtao, Zhu Yongjian

(Xishan People's Hospital of Wuxi City, Wuxi Jiangsu 214105, China)

Abstract: The application of Internet technology in medical field not only improves the level of hospital informatization, but also helps to optimize the allocation of medical resources, which brings great convenience to patients. However, with the rapid development of mobile Internet, medical information security has also begun to receive extensive attention. Based on this, the author analyzed the challenges faced by medical information security in China under the background of the Internet, and put forward some suggestions to promote the upgrade and development of medical information security, hoping to provide reference for relevant research.

Key words: internet; medical; information; information security

0　引言

网络信息技术在医疗领域的快速发展，促使互联网医疗成为一种新兴的医疗模式，既加快了医疗卫生事业的信息化建设步伐，也给医疗机构和患者带来了诸多便利，极大地提升了医院的诊疗效率和服务水平。然而随着“互联网＋医疗”的日益推广，大数据、云计算等技术在医疗领域得到广泛应用，这使得医疗数据在采集、存储和应用过程中交互的数据量越来越多，医疗数据资源变得更集中、更容易获得，但这也导致信息泄露、设备入侵、数据滥用及篡改等问题频频发生，给医疗信息安全带来了极大的威胁和隐患[1]。因此，信息安全成为互联网医疗建设的一个重要内容，是医疗行业需要正视并亟待解决的难题。

1　互联网时代医疗信息安全面临的挑战

1.1　安全管理方面

随着各种信息化系统、医疗健康平台在医疗领域应用比例的不断提高，医疗机构之间交互、共享的数据量呈爆炸式增长，直接给医疗机构在安全管理方面的工作带来了巨大的挑战。首先，由于医疗机构缺乏足够的信息安全专家、信息系统维护人员缺乏专业的培训、员工缺乏安全操作意识等因素导致医疗机构在日常人员管理、设备管理方面存在很多漏洞，导致医疗机构管理水平整体不高，从而增加了医疗数据在互联网传输过程中的信息泄露风险。其次，受技术发展水平限制，医疗机构在数据管理方面的水平偏低，缺乏成熟的技术和完善的安全制度支撑。而且由于医疗数据资源具有巨大的商业价值，借助互联网平台获取这些数据变得更加容易，无疑会增加医疗数据泄露的可能，在信息安全、隐私保护方面存在巨大的隐患。

1.2　网络设备方面

医疗设备和网络技术的缺陷也使医疗信息安全工作面临着巨大的安全隐患。首先，由于医疗信息系统软件的安全防护性能差，在设计之初对于互联网因素考虑较少，这些因素

作者简介：王映涛（1981—），男，江苏无锡人，本科，信息科科长。研究方向：信息化建设规划与管理。

都会给医疗信息安全留下很多隐患，增加数据泄露或者丢失的风险。其次，由于医疗机构对硬件设备环境缺乏安全保护意识和管理经验，从而容易导致信息存在丢失的风险。最后，针对互联网医疗开放共享的特点，医疗机构采用的传统内外网物理隔离的网络模式难以实现信息一体化建设，对于非法网络入侵，很难有效地进行追踪和及时反馈。因此网络安全也是当前医疗信息安全管理面临的一大难题。

1.3 法律体制方面

目前，缺少健全的法律法规保护体制是医疗信息安全管理面临的最大难题之一。首先，我国在医疗信息安全方面，保护用户个人信息和隐私大都采用间接方式，尚未出台正式、系统性的法律法规来确保医疗数据的法律地位，针对个人隐私数据的保护规定则更少。而且目前我国有关个人信息的保护规定通常都分散在效力层次不一的各种法律法规甚至规范性文件中，针对非法窃取医疗信息行为的处罚缺少健全的法律体制。由于缺乏法律震慑力，一方面容易为不法分子窃取、破坏医疗数据提供投机取巧的可能，另一方面当出现侵权行为时往往也无法可依。其次，大部分医疗机构或者组织都缺少风险管控意识，没有健全的信息安全保障机制，从而也会给信息管理带来很大的安全隐患 [2]。

2 医疗信息安全的发展对策

2.1 从制度层面建立医疗信息安全管理体系，保证医疗数据和信息的安全

科学管理是互联网时代医疗信息安全的重要保障，各医疗机构应结合现实情况，制定符合自身发展战略的管理规范和制度。第一，加强医疗机构统筹力度，建立信息安全体系架构，健全责任追究制度，实现监管主体多元化、一体化发展。通过建立完善的信息安全体系架构，在使用医疗信息过程中做到主体明确、多方协调一致，形成一个立体化、多层级、多部门、多机构相互配合的监察、监督体系，提高医疗信息安全的管理水平 [3]。第二，加强培训制度建设，提升信息技术人员的专业技能和职业素养。由于医疗信息从业者在工作过程中不可避免地要频繁接触大量的医疗数据，如财务信息、患者健康数据等，其中有可能涉及个人隐私。因此为了防止这些信息泄露，既要加强对信息技术人员的专业技能培训，培养行业安全专家，建立行业网络安全专控队伍；也要增强他们的安全防范意识，从而提高医疗信息和隐私数据保护效果，促进和实现互联网医疗服务的健康、可持续发展。

2.2 从技术层面加强信息系统防御，强化医疗数据保护

从技术层面确保医疗数据的安全存储、传输和应用包括以下几项措施。第一，建立数据分级、分类管理办法。根据医疗数据的重要性，医院应建立完善的信息安全认证平台，按照不同的数据分类分别进行分级管理，加强对医疗信息合理使用的监管力度，为信息安全提供可靠的法律保障。此外，通过制定医疗数据的分级管理办法，当出现信息泄露时，能够帮助技术人员及时追踪到泄密者。第二，互联网医疗中的各类安全隐患大部分可以通过先进的技术手段来解决，因此针对医疗数据的传输和存储可以通过加密技术、访问控制技术、数据分割、数据授权以及安全监控和身份认证等技术，提高医疗数据的安全管理水平，减少医疗数据在传输使用过程中的信息泄露风险和经济损失。第三，加强对医疗设备的安全审查机制，完善网络隔离措施，提高医疗信息系统的安全性能。一方面医疗机构要加强对医疗设备的安全审查和检测；另一方面也要对互联网中的接入用户设置严格的分级分类权限，同时要加大资金和人力投入力度，加强各类医疗信息系统的安全性能，以此从安全审计、安全感知和安全处置等多维度加强对医疗数据的防护能力。

2.3 从立法层面健全相关法律法规制度，确定信息安全的法律地位

随着互联网医疗发展规模的不断壮大，国家有关部门应高度重视并给予关注，通过制定科学合理的医疗信息安全政策，完善相关法律法规制度，将其上升到立法层面予以保护，从而能够为医疗信息安全提供可靠的法律保障，以适应互联网医疗的发展需求。医疗信息安全需要有法律的保护，通过结合我国互联网医疗信息安全的现存问题，应加快制定健全的法律法规体制，对恶意破坏、非法窃取医疗数据和泄露个人隐私等一些违法行为予以制止和惩罚，对违反法律法规的无论是企业还是个人，一定要严惩并追究相应的违法责任，从而才能营造良好的社会氛围，确保医疗信息安全有法可依，实现对医疗信息的全面保护。

3 结 语

技术本身是中性的，但技术的应用却要面对安全、伦理等一些列的挑战。医疗机构在享受互联网医疗带来巨大便利的同时，也应时刻保持警惕，高度重视医疗信息安全问题。医疗机构应主动出击，从法律层面、技术层面、管理层面多角度、多维度地进行医疗信息安全防护，确保医疗资源畅通无阻、安全可靠地共享，为我国医疗卫生事业的改革发展保驾护航。

参考文献

[1] 李璐，谢颖夫，胡光阔．“互联网＋医疗”中信息安全的探讨 [J]. 价值工程，2017(9):49-50.

[2] 吴超．“互联网＋医疗”信息安全问题及对策 [J]. 集成电路应用，2019(3):74-75.

[3] 刘孝男，付嵘，李连磊．大数据时代医疗行业信息安全面临的机遇与挑战 [J]. 网域前沿，2018(7):100-102.