

我国中医医院网络安全建设历程及展望^{*}

肖 勇 白文斌

孙 静

田双桂 沈绍武

(湖北中医药大学 武汉 430065) (湖北省中医院 武汉 430061) (湖北中医药大学 武汉 430065)

王 斌

(中国中医科学院 北京 100700)

〔摘要〕 介绍我国中医医院网络安全建设与发展历程,分析中医医院网络安全建设特点,从网络安全责任与意识、管理措施、技术防护体系、数据安全保护、人才队伍、经费投入等方面对我国中医医院网络安全建设进行展望,以期为加强中医医院网络安全建设提供参考。

〔关键词〕 中医医院;网络安全;历程;展望

〔中图分类号〕 R-058 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2021.10.001

The Course and Prospect of Network Security Construction of Traditional Chinese Medicine Hospitals in China XIAO Yong, BAI Wenbin, Hubei University of Chinese Medicine, Wuhan 430065, China; SUN Jing, Hubei Provincial Hospital of TCM, Wuhan 430061, China; TIAN Shuanggui, SHEN Shaowu, Hubei University of Chinese Medicine, Wuhan 430065, China; WANG Bin, China Academy of Chinese Medical Sciences, Beijing 100700, China

〔Abstract〕 The paper introduces the network security construction and development process of Traditional Chinese Medicine (TCM) hospitals in China, and analyzes the characteristics of network security construction of TCM hospitals. From the aspects of network security responsibility and awareness, management measures, technical protection system, data security protection, talent team, funding investment and so on, it prospects the network security construction of TCM hospitals in China, so as to provide references for strengthening the network security construction of TCM hospitals.

〔Keywords〕 Traditional Chinese Medicine (TCM) hospital; network security; course; prospect

〔收稿日期〕 2021-08-26

〔作者简介〕 肖勇,副教授,发表论文 20 余篇;通讯作者:沈绍武,研究员。

〔基金项目〕 “中医药现代化研究”专项课题“多源异构中医科学数据汇交系统的研发”(项目编号:2017YFC1703505);国家中医药管理局中医药项目“‘十四五’中医药信息化高质量发展研究”(项目编号:GZY-GCS-2019-006)。

1 引言

中医医院是振兴发展、传承创新中医药事业的主阵地,承担着满足广大人民群众中医药健康服务需求的主要任务。随着信息技术应用越来越深入、广泛,医院业务与信息化建设日渐紧密,中医医院运转高度依赖信息化,网络建设由局域网向互联网转变,完全物理隔离态势被打破,网络安全变得越

来越重要。本文梳理和总结我国中医医院网络安全建设与发展历程、主要特点,提出中医医院网络安全建设路径与思路,以期为中医医院网络安全建设提供参考。

2 建设与发展历程

2.1 中医医院信息安全建设起步

我国信息安全建设始于20世纪90年代^[1]。随着中医医院信息化建设不断加速,网络安全建设理念和实施得到不同程度重视。1994年施行的《计算机信息系统安全保护条例》明确规定了计算机信息系统安全保护工作相关要求。这一时期中医医院信息化刚刚起步,以财务管理为主的医院信息系统得到初步应用,医院传统手工业务不断实现电子化,信息系统层面的密码设置、权限控制、角色分配、日志管理等信息安全防护措施以及杀毒软件等单机版本安全防护开始得到不同程度应用。2003年11月出台的《中医医院信息化建设基本规范(试行)》是我国中医医院走向全面信息化的重要标志,其将系统安全单列一章,从信息安全组织机构、人员管理、信息安全等级划分、防护策略和措施、应急处置等方面提出信息安全基本要求,为中医医院网络安全建设奠定坚实基础^[2]。

2.2 中医医院网络安全建设快速发展

自2005年起网络基础安全、信息系统安全管理与技术、操作系统安全、数据库管理系统、服务器、终端计算机等技术标准以及信息安全管理程度、组织机构、人员队伍、系统运维等管理标准相继出台。2007年3月首个中医药信息化建设5年规划出台,提出要加强网络信息安全制度建设,建立和完善网络信息安全防御系统^[3]。2007年6月《信息安全等级保护管理办法》颁布实施,要求对信息系统分等级实行安全保护,中医医院信息安全等级保护工作开始进入发展阶段,信息安全意识逐步提升,陆续成立医院信息安全工作领导小组,购置防火墙、漏洞扫描、入侵检测等安全设备,在推广信息系统的同时注重等级保护工作。如广东省中医院

以实施医院信息系统过程中遇到的安全问题为基础,从数据层、网络层和工作站及应用软件3个层次加强医院信息系统安全管理制度、安全保障措施和安全应急措施建设^[4]。2008年10月全国中医医院信息管理人员培训班开设中医医院信息安全建设专题培训;2010年4月全国中医药信息化经验交流会专题讨论中医医院信息安全等级保护工作和建设举措。2011年原卫生部相继印发《卫生行业信息安全等级保护工作的指导意见》《关于全面开展卫生行业信息安全等级保护工作的通知》,明确指出“三级甲等医院核心业务信息系统”等5类卫生信息系统等级保护原则上不低于3级,卫生行业全面实施信息安全等级保护工作正式提上日程。同年国家中医药管理局完成对所有第2级、第3级信息系统的安全测评。修订出台的《中医医院信息化建设基本规范》将原有规范的“系统安全”升级为“信息安全”并提出从技术和管理两个方面构建医院信息平台综合防御机制^[5]。

2.3 新形势下的网络安全建设全面发展

没有网络安全就没有国家安全。网络安全工作得到高度重视,就网络安全和信息化工作的重大决策相继出台,形成了网络强国战略思想。《网络安全法》《数据安全法》相继施行,网络安全各项工作进入法治化轨道,为中医药行业贯彻落实网络安全提供依据、指明方向。《中医药信息化发展“十三五”规划》首次将信息安全建设作为主要任务进行部署。《全国医院信息化建设标准与规范(试行)》对二级以上医院的数据中心安全、终端安全、网络安全及容灾备份提出具体要求^[6]。随着云计算、大数据、物联网、移动互联网、5G等信息技术广泛应用于中医药领域,网络安全已成为中医医院信息化建设的重点工作。中国中医药信息学会专门成立信息安全分会,汇聚中医药领域从事网络信息安全的专家学者和从业者,多次举办中医医院网络安全讨论会。2019年中医医院信息化建设现状数据显示,大部分中医医院注重网络安全建设,采取防火墙、入侵检测、漏洞扫描、病毒防护、数据库审计、主机安全审计等安全措施和手段,仅6.55%的

中医医院未配置任何网络安全设备;在数据灾备方面,49.42%的中医医院采用不同方式和措施,其中29.57%采取同楼异处灾备,1.62%采用不同城市灾备;85.46%的中医医院已建立网络安全管理组织,93.67%建立相关规章制度;27.58%的中医医院实施网络安全等级保护测评^[7]。

3 建设特点

3.1 网络安全建设日益受到重视

中医药信息化“十一五”“十二五”“十三五”规划均对网络安全进行专门部署。“十三五”期间国家中医药管理局每年与国家卫健委联合下发通知,以落实卫生健康行业网络信息与数据安全责任,加强医疗健康与中医药领域网络安全工作,明确责任、增强意识。2019年中医医院信息化建设现状数据显示,85.46%的中医医院建立网络安全管理组织,网络安全建设日益受到各级领导和信息化从业人员重视,实现了网络安全与信息化建设的同步规划、建设和运行,数据安全和应用安全防护能力逐步提升^[8],建立和执行网络安全管理规章制度,不定期开展网络安全应急演练。

3.2 网络安全与业务应用融合深入

业务应用是中医医院信息化建设与发展的核心,也是智慧中医医院建设的根本。随着网络攻击逐步向业务应用层转移,中医医院网络安全建设逐渐升级,从最开始的无安全防护或弱安全防护发展到重视采购与应用杀毒软件、防火墙、漏洞扫描、入侵检测、上网行为管理、网络审计、数据库审计等信息安全设备,推进网络安全态势感知平台、网络安全管理平台、数据安全治理平台等与业务应用系统融合,将医院核心业务应用系统作为重点安全防护对象,构筑平台化的网络安全管理与服务体系,将网络安全产品、技术与服务融入到医院业务系统建设中,关注通信网络、区域边界、主机安全、数据应用、移动应用等,在应用信息技术提供多样化的中医医疗服务、便民惠民服务的同时加强

个人隐私保护等网络安全防护措施。

3.3 网络安全等级保护制度不断落实

实行网络安全等级保护制度能够有效促进信息化建设健康有序发展,是中医药领域信息化高质量发展的重要保障。各级各类中医医院越来越重视网络安全等级保护制度制定、实施的具体化和详细化,主动引入第3方网络安全等级保护测评机构开展网络安全等级测评,组织开展医院网络安全防护检查和整改。2019年中医医院信息化建设现状数据显示,27.58%的医院实施网络安全等级保护测评^[7],27.20%组织开展网络安全防护情况自查。

3.4 网络安全意识得到提升

中医医院在信息化建设过程中,逐步建立起网络安全建设与信息化建设的同步规划、同步建设、同步运行“三同步”模式,改变了重建设轻安全、重技术轻管理的理念和现状。72.62%的中医医院曾举办网络安全知识和技术等培训,通过邀请网络安全专家开展网络安全等级保护制度和标准规范、信息安全技术和管理制度等方面培训,医院信息管理和技术人员的网络安全防护意识得到提升,信息系统使用人员信息安全意识也得到强化。

4 展望

4.1 落实网络与信息安全责任,强化网络安全意识

《网络安全法》《数据安全法》等法律法规已经实施,网络安全成为法定任务,中医医院要高度重视网络安全面临的严峻形势,充分认识做好网络与信息安全的重要性和必要性,坚持“谁主管谁负责、谁建设谁负责、谁运营谁负责”原则,建立网络与信息安全领导机构,将网络与信息安全纳入中医医院信息化建设规划中,落实网络安全主体责任。专题研究信息化建设和网络安全工作,强化网络安全管理责任和担当,设立安全保密管理员、安全审计员和系统管理员等岗位并落实具体人员负责,重视云计算、大数据、物联网、移动互联网、人工智能等信息技术应用带来的安全风险,组织开

展网络安全知识经常性安全教育,树立“网络安全人人有责”理念,不断提升医院全体人员网络安全意识。

4.2 梳理网络安全建设薄弱点,加强网络与信息安全管理措施

以《网络安全法》及网络安全等级保护标准规范为依据,不定期采用自查自评与现场检查、技术检测等形式组织检查网络安全等级保护落实、网络安全技术防护策略、网络安全通报、应急预案及演练、网络安全事件处置、网络安全宣传培训等工作,检测排查业务应用系统安全漏洞隐患、风险和突出问题,梳理总结网络安全建设薄弱点,评估网络安全风险并进行整改,提高网络安全预警、防范水平。坚持网络安全与信息化建设同步规划、建设与发展,切实做好医院信息系统、中医电子病历、医疗大数据平台、互联网医疗平台等核心业务信息系统的安全等级备案、测评和整改。完善网络数据共享、利用等安全管理和技术措施,制定网络安全防护详细策略,建立健全人员、软件、硬件和网站管理以及系统运维、数据安全、灾备管理和应急演练等安全管理制度,构建网络安全信息通报、信息共享、应急联动机制,定期开展网络安全事件应急预案演练。

4.3 构建立体化的网络安全保障体系,加强数据安全防护

网络安全涉及网络、系统、应用、设备、数据和技术等环节,应以“环境可信、合规可达、风险可控”为目标,以业务应用和数据治理为驱动,选择安全工作经验丰富、技术实力较强、符合资质要求的单位协同参与,结合传统业务特性及新型数字化诊疗业务转型的新逻辑^[9],从网络安全威胁预测、防御、监测和响应的闭环管理出发,构建医院安全技术、安全管理、安全运营体系,在物理环境、通信网络、区域边界、计算环境、存储环境、安全管理中心等不同层面加强技术防护^[10-11],搭建网络安全态势感知平台,建立并完善漏洞扫描、入侵检测与防御、防病毒、防

拒绝服务攻击、安全审计、防信息泄露、数据加密等防护手段,防范计算机病毒、网络攻击、网络侵入等危害网络安全行为,重点维护医院信息系统、中医电子病历系统、集成平台等重要信息系统安全。依法依规对数据产生、传输、存储、使用、共享、销毁等环节实行全生命周期安全管理,严格管理患者信息、中医临床数据和生物样本库信息等,强化个人隐私保护,实行中医临床数据资源分级分类管理,划分数据访问权限,强化数据导出共享、交换开放等安全审批管理,实施数据脱敏、日志记录等安全管理措施,有效防范数据丢失、泄露、未授权访问等安全风险。

4.4 加强网络安全人才队伍建设,加大经费投入

人才是网络安全建设发展的关键,网络安全意识是中医医院网络安全建设面临的挑战。中医医院应通过招聘、培训等方式引进和培养网络安全专业人才^[12],加强安全建设、安全管理、安全运维和应急保障队伍建设。同时定期对专业人员进行网络安全教育、技术培训和技能考核,开展网络安全攻防演练比赛,从信息系统安全设计研发维护、网络设备和数据库运维管理、医疗数据安全采集存储共享等多方面、全视角提升网络安全技能^[13];定期对医院其他人员开展网络安全基础知识教育、基本防护技能培训,规范业务信息系统安全操作,建立日常网络安全防护意识。加大网络安全经费投入,设立网络安全专项经费,将网络安全等级保护建设整改、等级测评、信息安全服务、技术培训等费用纳入年度信息化建设预算。

5 结语

中医医院作为中医医疗服务的主阵地,记录和存储大量患者个人信息、诊疗信息、科研数据和运营管理数据,然而在网络安全技术防范、安全管理执行方面尚未达到相关要求,医院数据中心和网络安全面临巨大风险,对此医院管理者必须高度重视、常抓不懈,建立好网络安全主体责任,落实网

(下转第 10 页)

- 2 郭才, 李续然, 陈炎华, 等. 区块链技术在物联网中的应用概述 [J]. 物联网学报, 2021, 5 (1): 72-89.
- 3 毛戈, 李晶, 朱乔, 等. 区块链技术在医疗领域中的应用前景 [J]. 湖北大学学报 (自然科学版), 2021, 43 (1): 86-90.
- 4 黄俊飞, 刘杰. 区块链技术研究综述 [J]. 北京邮电大学学报, 2019, 41 (2): 1-8.
- 5 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究 [J]. 软件学报, 2017, 28 (6): 1474-1487.
- 6 Wan J, Li J, Imran M, et al. A Blockchain-based Solution for Enhancing Security and Privacy in Smart Factory [J]. IEEE Transactions on Industrial Informatics, 2019, 15 (6): 3652-3660.
- 7 Kim H, Laskowski M. Toward an Ontology-driven Blockchain Design for Supply-chain Provenance [J]. Intelligent Systems in Accounting, Finance and Management, 2018, 25 (1): 18-27.
- 8 Tian F. An Agri-food Supply Chain Traceability System for China Based on RFID & Blockchain Technology [M]. Piscataway: IEEE Press, 2016: 1-6.
- 9 Li Z, Kang J, Yu R, et al. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things [J]. IEEE Transactions on Industrial Informatics, 2018, 14 (8): 3690-3700.
- 10 Herger M. 未来驾驶 [M]. 北京: 电子工业出版社, 2020.
- 11 刘炜, 彭宇飞, 田钊, 等. 基于区块链的医疗信息隐私保护研究综述 [EB/OL]. [2021-01-14]. <https://www.doc88.com/p-99759508896276.html>.
- 12 Drosatos G, Kaldoudi E. Blockchain Applications in the Biomedical Domain: A scoping review [J]. Computational and Structural Biotechnology Journal, 2019 (17): 229-240.
- 13 瞿玲玲, 丛鑫. 区块链技术研究与应用 [J]. 仪器仪表学报, 2021, 41 (10): 43-53.
- 14 Feng Q, He D, Zeadally S, et al. A Survey on Privacy Protection in Blockchain System [J]. Journal of network and Computer applications, 2019 (126): 45-58.
- 15 Ali M, Vecchio M, Pincheira M, et al. Applications of Blockchains in the Internet of Things: a comprehensive survey [J]. IEEE Communications Surveys Tutorials, 2019, 21 (2): 1676-1717.

(上接第5页)

络安全等级保护制度和标准规范, 大力推进“一个中心, 三重防御”的立体化网络安全保障体系建设, 构建网络安全建设、测评、整改、检查常态化机制, 全面提升网络信息安全防御和威胁应急响应能力, 全力支撑中医医院诊疗业务服务连续性。

参考文献

- 1 徐金伟. 我国网络空间安全建设历程的回顾与思考 [J]. 网络空间安全, 2016, 7 (8): 4-6.
- 2 国家中医药管理局. 中医医院信息化建设基本规范 (试行) [EB/OL]. [2020-11-07]. <https://www.jdxz.net.cn/article/402881e40c5730e0010c86c9e765006e/2009/3/402881e40c5730e0010ca5ef735c00ef.html>.
- 3 国家中医药管理局. 中医药信息化建设“十一五”规划纲要 [EB/OL]. [2020-04-02]. http://www.gov.cn/zw/gk/2007-04/02/content_569150.htm.
- 4 李小华, 陈达灿, 傅昊阳. 浅谈医院信息系统的安全及对策 [J]. 国际中医中药杂志, 2008 (1): 25.
- 5 国家中医药管理局. 中医医院信息化建设基本规范 [EB/OL]. [2020-04-02]. <http://www.satcm.gov.cn/bangongshi/zhengcewenjian/2018-03-24/951.html>.
- 6 韩作为, 李宏芳, 赵韩. 医疗卫生行业网络安全相关要求梳理与分析 [J]. 中国数字医学, 2021, 16 (6): 1-5.
- 7 肖勇, 沈绍武, 吴小华. 我国中医医院信息化建设思考 [J]. 医学信息学杂志, 2020, 41 (12): 2-6.
- 8 张宇希, 胡建平, 周光华, 等. “十三五”时期卫生健康信息化发展及展望 [J]. 中国卫生信息管理杂志, 2021, 18 (3): 297-302.
- 9 沈彤, 万振. 常态化疫情防控下定点医院网络安全架构的设计与技术运用 [J]. 医疗装备, 2021, 34 (15): 20-22.
- 10 王晓丽, 丁月红, 陆昊. 等保2.0要求下医疗网络安全建设与管理研究 [J]. 中国数字医学, 2020, 15 (12): 5-9.
- 11 莫禹钧, 黄捷, 潘愈嘉. 基于网络安全态势感知的主动防御系统设计与实现 [J]. 医学信息学杂志, 2020, 41 (3): 60-63.
- 12 王松, 张艺然, 朱佳卿. 某市二级以上公立中医医院信息安全的现状调查与分析 [J]. 中国医药导报, 2019, 16 (15): 176-180.
- 13 郑攀, 陈臣. 网络安全态势感知探索与实践 [J]. 中国数字医学, 2021, 16 (6): 5-8.