联网医疗设备网络安全管理规范地方标准构建与实践路径*

——鞠 鑫[1] 徐爱彬[2*] 王华铎[3] 葛长龙[3]

【摘 要】 联网医疗设备的安全性是医疗质量的重要保证。针对联网医疗设备网络安全管理风险以及安全管理难点,苏州市卫生计生统计信息中心构建了基于联网医疗设备网络安全管理框架的地方标准,结合网络安全管理工作实践,指出应全方位落实网络安全监管机构、行业主管部门、联网医疗设备使用机构以及联网医疗设备厂商等多方职责,以确保医疗质量与患者安全。

【关键词】 联网医疗设备;网络安全;管理规范;地方标准;质量信息化
中图分类号:R197 文献标识码:B
Construction and Practice Path of Local Standard for Network Security Management Specification for Connected Medical Devices/JU Xin, XU Aibin, WANG Huaduo, et al. //Chinese Health Quality Management, 2024, 31(8): 63-68

Abstract The security of connected medical devices is an important guarantee of medical quality. In view of the network security management risks and security management difficulties of connected medical devices, Suzhou Health and Family Planning Statistics Information Center built a local standard based on the network security management framework of connected medical devices. Combined with network security management practice, it pointed out that multi-party responsibilities such as network security regulators, industry authorities, connected medical devices users and connected medical devices manufacturers should be fully implemented to ensure medical quality and patient safety.

Key words Connected Medical Devices; Network Security; Management Standard; Local Standard; Quality Information

First-author's address Suzhou Health and Family Planning Statistics Information Center, Suzhou, Jiangsu, 215000, China

当前,医疗设备大量接入医疗机构内部网络,这些设备在智能急救转运、重症患者智能监护、患者体征危机值预警等应用领域呈现诸多优势,但同时也对网络安全管理提出了更高的要求。例如,CT、磁共振、手术机器人等医疗设备多为进口品牌,如何有效保障其网络安全,成为亟待解决的问题[1]。

1 联网医疗设备网络安全管理风险分析

长期以来,医疗卫生行业一直是网络不法分子重要的攻击目标,不法分子往往利用医疗信息系统的漏洞窃取患者信息,同时也会对与网络连接的医疗设备进行破坏性攻击[2],给医疗秩序造成了较大的负面影响。随着越来越多的联网医疗设备应用到医疗机构中,传统网络安全边界被彻底打破,容易导致患者隐私泄露,进而引发医疗纠纷等重大安全风险。

DOI:10.13912/j.cnki.chqm.2024.31.8.13
* 基金项目:苏州市级基金——基于隐私计算的医疗卫生机构数据安全共享应用研究(编号:2023SSD44);苏州市第1批医学重点扶持学科——卫生信息学项目(编号:SZFCXK202146)
鞠 鑫[1] 徐爱彬[2*] 王华铎[3] 葛长龙[3] 通信作者:徐爱彬
1 苏州市卫生计生统计信息中心 江苏 苏州 215000 2 中国联通苏州市高新区分公司 江苏 苏州 215011
3 东软集团股份有限公司 辽宁 沈阳 110179

1.1　设备不可控引发的风险

联网医疗设备很难通过安装外部安全组件的方式进行安全管控，有些设备还存在私接4G、5G模块的现象，这些设备是否被非法植入无法预料，一旦被非法植入，便存在长期下载、存储、编辑患者数据等风险。联网医疗设备同时也存在弱口令、空密码等安全性问题，如果不法分子通过暴力破解等手段对设备进行劫持和仿冒，可能引发更大范围的病毒传播和数据泄露。

1.2　行为不可见引发的风险

远程诊疗活动中患者的病理学诊断、影像学诊断等数据往往以非加密方式通过互联网传送[3]，联网医疗设备通信过程中使用私有协议，以及基于医疗业务专属的HL7、DICOM协议，缺少通信安全方面的考虑，使得不法分子更容易、更隐蔽利用这些通信协议进行攻击。

1.3　漏洞不可知引发的风险

由于设备厂商缺乏安全方面的技术人员，加之对成本的考虑，导致很多联网医疗设备在设计之初就存在安全漏洞。不法分子可利用其安全漏洞窃取患者医疗数据并对设备进行攻击。同时，联网医疗设备补丁更新周期不能及时修复安全漏洞，也会对医疗工作流程、患者安全和医院运营造成负面影响[4]。

1.4　威胁难定位引发的风险

面对联网医疗设备海量复杂的交互信息，如不能准确定位安全威胁的源头，将导致威胁快速蔓延，引发更大范围的网络安全事件，严重的可能会导致医疗核心业务系统异常运行，甚至业务停摆等[5]。

2　联网医疗设备网络安全管理难点分析

医疗数据敏感性较高，一旦泄露可能影响患者个人隐私保护甚至医疗行业发展[6]。医疗卫生机构在开展联网医疗设备网络安全管理工作时面临诸多难题。

(1)安全标准规范不足，难以指引医疗机构有序开展医疗服务。由于指导医疗卫生机构开展联网医疗设备网络安全建设的标准体系尚不完善，在发生网络安全事件时，经常会出现直接断开联网医疗设备连接的情况，严重制约了联网医疗设备的正常使用。

(2)安全管理思路局限，难以落实安全防护策略。联网医疗设备的采购、使用、维护、报废等涉及多个业务科室，不同业务人员对网络安全的理解也各不相同，导致在推动联网医疗设备安全管理时常常遇到阻力。由于缺乏针对联网医疗设备安全的监管体系，部分联网医疗设备甚至出现了无人管、无人问、无人查的“三不管”现象。如果医疗设备管理人员未能充分掌握安全管理的相关标准和技术，会导致管理效率低下且难以达到预期的安全管理目标[7]。

(3)安全技术手段缺失，难以有效应对安全威胁。物联网与信息技术在医疗行业多场景的融合应用，使得联网医疗设备呈现出类型多、系统多、接口多、协议多的现象，单纯依靠传统网络技术手段很难实现对联网医疗设备进行安全漏洞管理、异常行为识别以及设备资产定位。在面对联网医疗设备多样化、突发性和隐蔽性的网络攻击时，经常会出现网络安全防护“盲区”。

为了加强各重要领域网络安全保障，国家有关部门相继发布了《中华人民共和国网络安全法》[8]、《中华人民共和国数据安全法》[9]等法律法规，修订了《信息安全技术 网络安全等级保护基本要求》(GB/T 22239－2019)[10]、《信息安全技术 信息安全风险评估方法》(GB/T 20984－2022)[11]等标准，这为网络安全防护体系提供了保障。国家食品药品监督管理总局(NMPA)发布了《医疗器械网络安全注册技术指导原则》[12]，要求注册人开展网络安全质控工作。同时，《医疗卫生机构网络安全管理办法》中也提出了医疗设备网络安全的相关要求[13]。

3　构建联网医疗设备网络安全管理地方标准

2022年1月11日，国家卫生健康委印发了《“十四五”卫生健康标准化工作计划》，要求在“十四五”期间健全卫生健康标准体系，完善基础类、数据类、应用类、技术类、管理类、安全与隐私类等6类信息标准制定。为了更加规范地开展联网医疗设备网络安全管理标准建设工作，在苏州市卫生健康委的大力支持下，苏州市卫生计生统计信息中心组织公安、网信、卫生健康等部门相关工作人员，以及苏州医学会、10余家医院信息安全负责人以及医疗设备与网络安全企业代表等召开了联网医疗设备网络安全管理标准框架地方标准启动会，围绕监督管理、行业现状以及安全实践进行研讨。在联网医疗设备网络安全管理规范地方标准的编制过程中，采用项目管理方式制定了详尽的标准工作推进计划，见图1。

3.1　标准调研与编制准备阶段

在标准建设意向、组织分工明确后，项目组按照职责开展标准编制前的准备工作，包括资料查阅、内部研

讨，针对需要定量、定性分析问题形成调研表。由苏州市卫生计生统计信息中心统筹协调标准工作构建的参与医院，形成调研计划并组织了为期 2 个月的现场调研工作。对调研结果进行充分地分析、总结，形成每家医院的输出调研报告，并结合现状，提出联网医疗设备网络安全管理的合理化建议，形成标准草案稿。

3.2　标准编写与评审阶段

对于标准草案稿，项目组组织了两轮专家研讨会议，充分讨论了标准的适用性和可操作性，提出了 20 余条价值建议，形成标准征求意见稿，并于 2024 年 4 月底前提交。经过 4 次专题研讨会讨论，初步确定以“联网医疗设备”作为标准方向、以“管理规范”作为标准类型、以“管理通用要求、全过程管理要求、安全技术防护”作为标准框架(图 2)，并拟定以“联网医疗设备网络安全管理规范”作为地方标准选题。

与此同时，标准框架创造性地提出体系化、标准化、可参考、可实践的联网医疗设备网络安全管理框架，以帮助区域医疗机构规范联网医疗设备网络安全管理，提高联网医疗设备网络安全保障能力，确保联网医疗设备临床使用的安全性和有效性。围绕网络安全管理通用要求、过程管理要求和技术防护三方面构建联网医疗设备的网络安全体系框架(图 3)，以确保联网医疗设备的资产可控、威胁可见、漏洞可知、行为可追溯。(1)网络安全管理通用要求从统筹规划的角度对管理组织、管理制度、人员管理、风险管理、安全培训等内容提出具体规范，以统一医疗机构联网医疗设备网络安全管理思想。(2)网络安全过程管理要求从联网医疗设备的全生命周期出发，围绕采购、安装、使用、维护、报废等环节细化网络安全相关要求，以有效防止因设备原因而对患者和操作人员造成的危害[14]。(3)网络安全技术防护从医疗机构现有网络安全体系出发，结合联网医疗设备的特性，针对性提出了网络安全技术措施，以有效弥补传统网络安全技术手段的缺失，改善传统网络安全技术手段的不足。

4　实践效果

为确保标准内容符合当前医疗机构联网医疗设备实际业务场景，在编制联网医疗设备网络安全管理规范地方标准的具体内容时，项目组专门成立了标准工作小组(图 4)，将标准化工作细化到具体应用场景，责任落实到个人。围绕智能急救转运、实时位置跟踪、重症患者智能监护、体征危机值报警等联网医疗设备业务场景展开全面调研，实现了苏州市 95%以上联网医疗设备业务场景覆盖。

4.1　网络安全管理通用要求的实践路径

联网医疗设备网络安全管理通用要求是从全局视角统一网络安全

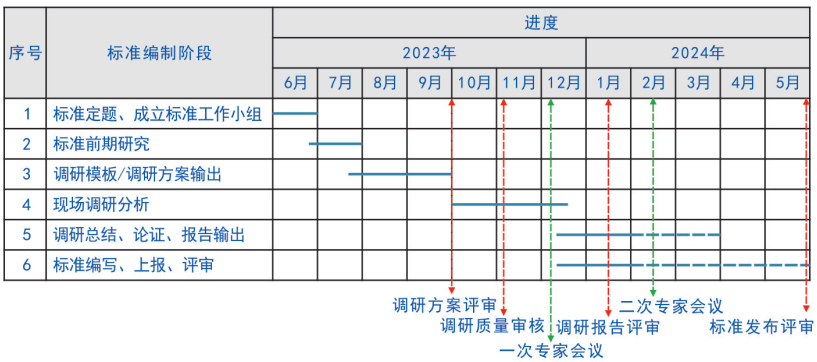

图 1　联网医疗设备网络安全管理框架地方标准工作总体推进计划

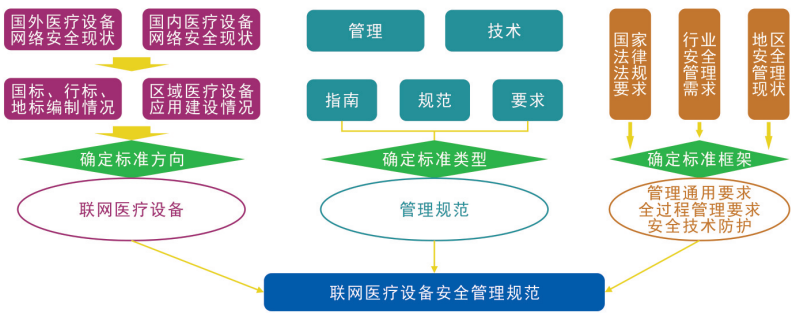

图 2　联网医疗设备网络安全管理标准框架选题思路

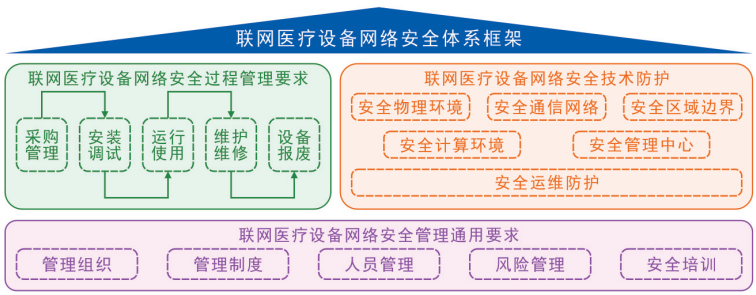

图 3　联网医疗设备网络安全体系框架

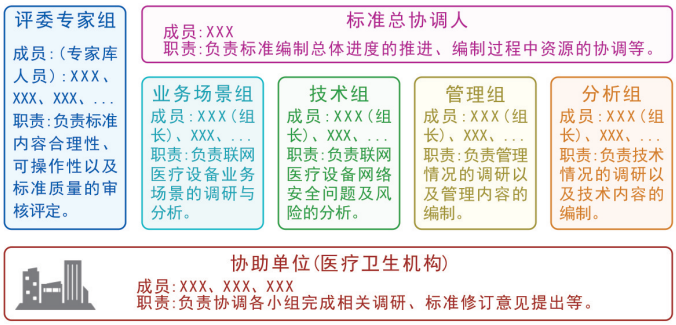

图4　联网医疗设备网络安全管理标准工作小组

防护策略,横向打通了各医疗机构业务科室间面向联网医疗设备网络安全防护体系建设运行的壁垒。

(1)管理组织。设立由医疗机构主管领导及网络安全、设备管理、临床使用、后勤保障等部门共同组成的联网医疗设备网络安全管理机构,统筹协调网络安全管理工作,强化各部门间的沟通与交流,确保达成共识。

(2)管理制度。制订联网医疗设备网络安全工作的总体方针和安全策略,建立健全医疗设备招标采购、安装调试、运行使用、维护维修、报废处置等制度。根据ISO 80001—1标准——“医疗设备集成IT网络的风险管理应用”,明确医疗服务提供者、医疗设备制造商和IT供应商在医疗设备集成IT网络中的责任[15],并有效落实。

(3)人员管理。强化医疗机构工作人员网络安全意识,规范人员操作流程,特别是外部物理访问联网医疗设备的人员必须获得授权。对于信息系统的权限管理,采用访问控制策略,设定角色、用户和具体权限3个相互依赖的层级,将相应权限赋予给角色(管理员、医疗机构网络安全监管人员、医技使用人员、第三方运维人员等),把角色赋予具体用户,避免了用户滥权、越权等现象[16]。

(4)风险管理。开展联网医疗设备网络安全的风险评估,当评估风险不可接受时,采取针对性风险措施干预,以降低或消除风险;当评估为可接受时,按照风险级别进行再次验证,确认其处于合理范围[17],并将风险结果和整改要求向相关部门和人员进行反馈。当发生重大网络安全事件时,立即召开会议,收集相关信息,启动相应的应急预案,强化了联网医疗设备网络安全的风险管理意识。

(5)安全培训。制订针对性的联网医疗设备网络安全培训计划,对相关操作人员开展网络和数据安全意识教育培训,并根据不同联网医疗设备可能产生的网络安全风险制订专项培训计划,提升了操作人员的网络安全意识,规范了操作人员的操作规程。

4.2　网络安全全过程管理要求的实践路径

联网医疗设备网络安全全过程管理实现了全生命周期网络安全管理的全覆盖,从源头避免了因某一环节的缺失引发的网络安全风险。

(1)采购管理。要求供应商提供联网医疗设备的安全保障能力和技术水平证明材料,以及联网医疗设备的安全更新和维护协议,并与供应商约定网络安全义务和违约责任,强化了医疗机构采购部门在设备采购时对联网医疗设备网络安全的综合考量[18]。

(2)安装调试。规范联网医疗设备操作流程,明确联网医疗设备的网络连接方法、异常连接处理方式等内容,对入网前的联网医疗设备开展网络安全脆弱性评估,识别安全漏洞并及时修复,有效避免了“带病”上线的联网医疗设备。

(3)运行使用。对联网医疗设备的运行使用进行规范化管理,编制所有联网医疗设备的清单,仅对联网设备使用人员开放操作指令,并建立联网医疗设备数据导出审批机制,同时指定专人导出数据,避免了因权限过大或操作不当引发的问题。

(4)维护维修。建立规范的联网医疗设备运维操作机制,对远程操作行为由网络安全部门进行审批,对外部维修后需重新接入网络的联网医疗设备进行网络安全检查,完整记录包括维修时间、人员、内容等维修信息,避免了因不当接入造成的数据泄露[19]。

(5)设备报废。建立联网医疗设备报废处置审批机制,及时断开报废处置联网医疗设备的网络连接,删除存储的业务数据,并对报废处置信息进行登记,避免了因联网医疗设备数据被非法恢复引发的信息泄露。

4.3　网络安全技术防护的实践路径

联网医疗设备网络安全技术防护规避了原有传统网络安全防护体系缺陷,提升了联网医疗设备网络安全事件的防护、检测、处置能力。

(1)安全物理环境。强化联网医疗设备所处物理环境的防雷、防火、防水、防静电、防震、防盗、电力供应、电磁防护等措施,合理规划ICU、手术室等重点区域和公共区域联网医疗设备的网络线缆铺设,避免了因物理场所不可控所引发的有意或无意的联网医疗设备违规操作行为。

(2)安全通信网络。划分独立

的联网医疗设备安全区域，根据使用过程中的移动频次选取有线或无线的网络接入方式，并采用校验技术或密码技术加强联网医疗设备通信过程中数据的完整性和保密性。

(3)安全区域边界。采用基于应用层访问控制机制对联网医疗设备专有协议进行限制，监测针对联网医疗设备发起的网络攻击行为，并对非授权设备进行限制，确保了联网医疗设备网络通信行为能够被有效识别和控制。

(4)安全计算环境。建立联网医疗设备“指纹库”，动态监测接入端口和服务协议，识别使用未经授权的接入端口和协议服务，并按照最小权限原则，为不同用户配置不同的访问控制策略，采用可信验证确保医疗设备数据的完整性[20]。

(5)安全管理中心。建立联网医疗设备网络安全管理平台，对分散的联网医疗设备进行集中监测和控制，加强网络安全威胁分析和态势研判，对安全策略、恶意代码、补丁升级进行集中管理[20]，实现了网络安全威胁的精准分析以及异常行为发生时的快速定位和预警处置。

(6)安全运维防护。建立统一的设备运维管理平台，加强联网医疗设备安全运维过程管理，建立完善的联网医疗设备安全监测机制[21]，对联网医疗设备远程接入行为进行集中监控，防止非法用户远程接入和非法操作等造成数据被窃取的安全隐患[22]。

5　讨论

联网医疗设备网络安全管理规范地方标准的建立，为苏州市各级医疗机构联网医疗设备网络安全管理提供了体系化、标准化、可参考、可实践的应用标准，同时为监管机构针对联网医疗设备的网络安全管理情况的颗粒度检查提供了依据。联网医疗设备网络安全管理规范地方标准通过再现联网医疗设备业务场景，厘清联网医疗设备业务流程，掌握联网医疗设备关键技术，形成了系统化、标准化、规范化的安全管理体系[23]，后续项目组将积极推进标准的发布、落地和推广，推动医疗行业监管机构和医疗机构开展更有针对性的网络安全风险管理[24]，在确保联网医疗设备网络安全的基础上实现医疗信息互联互通，助力公立医院实现高质量发展。

下一步，项目组将着力提高联网医疗设备网络安全管理规范地方标准的知晓率和使用率。(1)宣传推广。在苏州市各级卫生健康行政部门、各级医疗机构、行业协会，以及媒体、公共场所等广泛宣传联网医疗设备网络安全管理规范地方标准的作用和意义，提高社会各界对地方标准的认知。(2)培训交流。针对医疗机构实际需要，苏州市卫生计生统计信息中心将邀请行业专家和标准制定单位代表开展专项培训，普及地方标准的运用方法，提高标准化思维和实际操作水平。(3)推进实施。开展联网医疗设备网络安全管理规范地方标准的先行试点，逐步面向全市各级医疗机构推行，发挥标准在联网医疗设备网络安全管理方面的引导作用，提升全市各级医疗机构联网医疗设备网络安全管理能力。(4)监督检查。加强对联网医疗设备网络安全管理规范地方标准宣贯情况的监督检查，确保实施效果，及时反馈问题，确保标准的有效落地。

本研究构建了联网医疗设备网络安全管理规范地方标准，但要全方位落实标准内容还需要网络安全监管部门、行业主管部门、联网医疗设备使用机构、联网医疗设备厂商以及网络安全服务厂商的多方协同，以全面提升医疗卫生机构联网医疗设备的网络安全管理能力。同时，由于相关行业标准的缺失，联网医疗设备的网络安全测试技术和方法尚未得到有效应用[25]，导致很多网络安全缺陷难以有效修复，因此后续研究需要规范医疗设备厂商在上市前和上市后的网络安全责任，避免将网络安全责任遗留给医疗机构。

参考文献

[1]　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(2)：12－16.

[2]　舒　婷，赵　韡，徐　帆，等.患者安全目标：智慧医院建设中的网络安全风险[J].中国卫生质量管理，2020，27(6)：20－27.

[3]　李明鲁.从美国医疗数据泄露案谈信息安全的保护[J].中国检察官，2017(8)：72－75.

[4]　马诗诗，于广军，崔文彬.互联网医疗的隐私保护与信息安全[J].上海医药，2017，38(9)：14－16.

[5]　王凯芸，郑　涛，邵维君.医疗领域中区块链的应用与数据安全问题研究[J].医学信息学杂志，2021，42(4)：6－10.

[6]　田怀谷，黄贤君，陈　涛，等.基于医疗设备全生命周期的智慧医院平台建设实践[J].中国卫生质量管理，2023，30(10)：20－27.

[7]　杨丽晓，鲍　奇，丁秀文.医学检验设备全生命周期管理[J].临床医药文献电子杂志，2020，7(A4)：194－195.

[8]　新华社.中华人民共和国网络安全法[EB/OL].(2016－11－07)[2024－02－10].https：//www.gov.cn/xinwen/2016－11/07/content_5129723.htm.

[9]　新华社.中华人民共和国数据安全法[EB/OL].(2021－06－11)[2024－02－10].https：//www.gov.cn/xinwen/2021－06/11/content_5616919.htm.

[10]　国家市场监督管理总局，中国国家标准化管理委员会.信息安全技术 网络安全等级保护基本要求：GB/T 22239－2019[S].2019.

[11]　国家市场监督管理总局，中国国家标准化管理委员会.信息安全技术 信息安

全风险评估方法:GB/T 20984－2022[S].2022.

[12] 原国家食品药品监管总局.关于发布医疗器械网络安全注册技术审查指导原则的通告:2017年第13号[EB/OL].(2017－01－20)[2024－02－10].https://www.gov.cn/xinwen/2017－01/25/content_5163323.htm.

[13] 国家卫生健康委,国家中医药局,国家疾控局.关于印发医疗卫生机构网络安全管理办法的通知:国卫规划发〔2022〕29号[EB/OL].(2022－08－08)[2024－02－10].https:// www.gov.cn/zhengce/zhengceku/2022－08/30/content_5707404.htm.

[14] 贾　伟.基于标准维护角度探讨医疗设备安全管理现状及问题[J].大众标准化,2022(13):169－171.

[15] 郑　焜,谢松城,管炜桥,等.ISO 80001国际标准:关于医疗设备网络集成之风险管理[J].中国医疗设备,2012,27(8):93－94.

[16] 谭　健,程　铭,贾志刚,等.某大型公立医院医疗设备数据安全管理实践与思考[J].中国医院,2023,27(2):102－104.

[17] 王　非.精细化管理在医院医疗设备管理中的应用[J].医疗装备,2018,31(21):88－89.

[18] 张茫茫,郑　焜,沈云明,等.数字医疗设备信息安全防护探讨[J].中国医疗器械杂志,2014,9(7):33－35.

[19] 刑洪伟,苏悦洪,麦子铭,等.医疗设备网络安全管理的分析与探索[J].网络安全技术与应用,2023(7):115－116.

[20] 魏帅岭,闫国涛,李　星,等.等级保护2.0下医院网络安全体系的建设与探索[J].中国数字医学,2021,16(4):101－105.

[21] 石　馨.医疗设备的监管与维护及其意义和价值[J].医疗卫生装备,2010,31(7):97－99.

[22] 国家标准化管理委员会.信息安全技术 物联网感知终端应用安全技术要求:GB/T 36951－2018[S].北京:中国标准出版社,2019.

[23] 陈　明,林志刚,林传捷.医院网络安全等级保护综合管理平台设计探讨[J].中国医疗管理科学,2023,13(3):42－48.

[24] 姚宗碧.安全风险管理在医院医疗设备管理中的应用效果[J].医疗装备,2019,32(18):55－56.

[25] 刘　炯.数字医疗设备的信息安全测试[J].中国医疗器械杂志,2014,38(4):282－286.

通信作者:
徐爱彬:中国联通苏州市高新区分公司局长
E－mail:15651101109@163.com

收稿日期:2024－04－26
修回日期:2024－05－29
责任编辑:姚　涛

(上接第57页)

[10] 罗　平,尹　桃,刘　韶,等.中国医院质量安全管理:《输液安全》团体标准的制定与实施评价[J].中国卫生质量管理,2021,28(10):24－27.

[11] 郭晓薇.《国家医疗服务与质量安全报告》发布[J].中国卫生,2019(11):104.

[12] 国家卫生健康委办公厅.关于印发2023年国家医疗质量安全改进目标的通知:国卫办医政函〔2023〕45号[EB/OL].(2023－02－28)[2024－02－01].http://www.nhc.gov.cn/yzygj/s7657/202302/a61fc382f3b64c7e99dafbf8cf4da8a1.shtml.

[13] 左　玮,周　亮,高黛慧,等.我国二级及以上综合医院2020年住院患者静脉输液使用情况调研[J].中国卫生质量管理,2023,30(4):30－33.

[14] 张　敏,李武平,成翼娟,等.西部医院践行《静脉治疗护理技术操作规范》的调查分析[J].中国护理管理,2018,18(5):632－635.

[15] 欧阳静,江华容,陈大春.贵州省24家医院《静脉治疗护理技术操作规范》实践现状调查[J].贵州医药,2017,41(9):1006－1008.

[16] 蒋先雁,印　悦,陈剑宇,等.2014—2020年成都市大气污染物与呼吸系统疾病门诊量的时间序列研究[J].江苏预防医学,2022,33(1):12－16.

[17] 王　栋,罗　平,刘　韶,等.住院患者静脉输液专项管理实践[J].中国卫生质量管理,2022,29(5):34－37.

[18] 王　蕾,聂圣肖,孙　红.743家二级和三级医院静脉治疗现状的调查研究[J].中华现代护理杂志,2020,26(32):4494－4500.

[19] 金　欣.基于药物特性选择输液工具降低液体渗出和外渗的研究[J].中国护理管理,2019,19(S1):187－188.

[20] LIU C,CHEN L,KONG D,et al. Incidence, risk factors and medical cost of peripheral intravenous catheter － related complications in hospitalised adult patients [J].J Vasc Access, 2022, 23(1):57－66.

[21] TRIPATHI S, KUMAR S, KAUSHIK S. The practice and complications of midline catheters: a systematic review[J]. Crit Care Med,2021,49(2):140－150.

[22] LESCINSKAS EH, TRAUTNER BW,SAINT S,et al. Use of and patient－reported complications related to midline catheters and peripherally inserted central catheters[J]. Infect Control Hosp Epidemiol, 2020, 41(5):608－610.

[23] 陆海燕,薛　嵋,陆箴琦,等.基于信息平台的血管通路全程管理[J].护理学杂志,2018,33(21):50－53.

[24] 赵　将,王　雁,郭萍利,等.陕西省护理人员化疗职业防护知信行调查[J].中国卫生质量管理,2022,29(6):45－49.

通信作者:
唐梦琳:四川大学华西医院主任护师
E－mail: menglin_tang@163.com

收稿日期:2024－02－02
修回日期:2024－03－27
责任编辑:任红霞