ICS 35.040
CCS L 80
备案号：XXXX-XXXX

DB3205/T

苏 州 市 地 方 标 准

DB3205/T XXXX—2024

联网医疗设备网络安全管理规范

Specifications for cyber security management of connected medical devices

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

苏州市市场监督管理局　发　布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由苏州市卫生健康委员会提出并归口。

本文件起草单位：苏州市卫生计生统计信息中心、苏州市卫生健康委员会、苏州市公安局、苏州市质量和标准化院、东软集团股份有限公司、工业和信息化部电子第五研究所华东分所、苏州大学附属第二医院、中国联合网络通信有限公司苏州市分公司。

本文件主要起草人：鞠鑫、朱杰、夏燕、马振刚、张俊杰、刘旭哲、周文渊、王宝燕、赵亚、姚永刚、顾嘉奇、汤景云、沈婷、金建芳、徐爱彬、王华铎、许静。

引　言

随着我国医疗数字化不断发展，融合物联网、AI、5G等新一代信息技术的联网医疗设备已经深入到患者医疗服务的各个领域。与此同时，因其互联互通所引发的网络安全风险也日益凸显，特别是CT、磁共振、手术机器人等高端医疗设备依赖进口，由于缺乏体系化的网络安全管理措施，设备厂商远程运维引发数据泄露事件屡有发生，如何加强联网医疗设备的网络安全管理，已成为苏州市卫生健康行业普遍关注的问题。

从全行业的角度看，我国现有《中华人民共和国网络安全法》《中华人民共和国数据安全法》GB/T 22239-2019《网络安全等级保护基本要求》等文件；从卫生健康行业看，现有《医疗卫生机构网络安全管理办法》等文件，以上文件对网络安全已经提出了纲领性的要求，但缺乏针对联网医疗设备具体的网络安全管理要求，医疗卫生机构在落实联网医疗设备网络安全管理时缺少规范性文件的指导。因此，我们决定制定《联网医疗设备网络安全管理规范》地方标准填补行业空白。

起草组对苏州市有代表性的10余家联网医疗设备规模较大的医疗卫生机构开展调研，搜集联网医疗设备网络安全管理中存在的难点和痛点问题，针对普遍困扰管理者的问题，起草组经过谨慎、细致的讨论提出了解决方案。标准稿件经过行业主管部门、监管部门、科研单位、设备厂家、检测评估机构以及行业专家多次研讨与论证，具备较强的可操作性。可用于指导苏州市各医疗卫生机构开展联网医疗设备网络安全管理工作，解决由于地区产业结构差异、信息化建设差异产生的地区性共性及有代表性和个性化的联网医疗设备网络安全问题，从而提升医疗卫生机构的联网医疗设备安全管理和防护水平。

联网医疗设备网络安全管理规范

1 范围

本文件规定了联网医疗设备的管理要求和控制要求。

本文件适用于指导苏州市各级医疗卫生机构加强对联网医疗设备的网络安全管理，也可供卫生健康主管部门、网络安全监管部门以及第三方评估机构开展联网医疗设备网络安全监督检查等工作时参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20278 信息安全技术 网络脆弱性扫描产品安全技术要求与测试评价方法

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 20278、GB/T 25069 中界定的以及下列术语和定义适用于本文件。

3.1

联网医疗设备 connected medical devices

具有网络连接功能并接入到医疗卫生机构内部网络进行数据通信的用于预防、诊断、治疗、缓解疾病或者其他医疗过程中的设备、器械、仪器和其他相关物品，包括但不限于：血透机、呼吸机、心电图机、B超机、放射类设备、检验类设备、血压监测仪、血糖测量仪、睡眠监测仪等。

3.2

医疗器械网络安全注册申报资料 medical device network security registration application materials

具备电子数据交换、远程访问与控制、用户访问三种功能当中一种及以上功能的第二、三类独立软件和含有软件组件的医疗器械注册申请人在产品注册时根据医疗器械产品特性提交的网络安全描述文档和常规安全补丁描述文档。

4 缩略语

下列缩略语适用于本文件。

ICU：重症加强护理病房（Intensive Care Unit）

DICOM：医学数字影像和通信（Digital Imaging and Communications in Medicine）

HL7：卫生信息交换标准（Health Level 7）

MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）

5 管理要求

5.1 组织管理

a） 应设立由医疗卫生机构主管领导、网络安全管理部门、医疗业务管理部门、医疗设备管理部门、医疗设备临床使用部门和后勤保障部门共同组成的联网医疗设备网络安全管理组织，负责联网医疗设备的网络安全管理工作；

b） 应明确联网医疗设备网络安全管理组织的职责、分工和技能要求。

5.2 制度管理

a） 应制定联网医疗设备网络安全工作的总体方针和安全策略，通过技术措施和管理措施实现联网医疗设备的网络安全管理；

b） 应在执行 GB/T 22239 的基础上，按照本文件附录 A 的要求建立健全联网医疗设备网络安全防护体系；

c） 应建立健全联网医疗设备的设备采购、安装调试、运行使用、维护维修、报废处置等相关网络安全管理制度；

d） 应采取分类分级（参考附录 B）的方式对联网医疗设备进行网络安全管理。

注：各医疗卫生机构应结合自身实际情况对不同类别和级别的联网医疗设备采取相应等级的管理。

5.3 人员管理

a） 应根据医疗卫生机构内、外部人员的岗位职责和工作需要签订保密协议，协议明确保密的对象、范围、内容和期限等；

b） 在外部人员物理访问联网医疗设备前应提出书面申请，批准后由专人全程陪同，并登记备案；

c） 在外部人员使用网络访问联网医疗设备前应提出书面申请，批准后由专人开设账号、分配权限，并登记备案；

d） 应及时终止离职人员对联网医疗设备的使用权限。

5.4 风险管理

a） 新购置或新引入的联网医疗设备应由网络安全管理部门会同医疗设备管理部门对其进行网络安全风险评价，并按照规定程序将分析结果和整改要求向相关部门和人员进行反馈和通报；

b） 医疗卫生机构网络安全管理部门应定期检查或评估联网医疗设备的网络安全风险状况，并按照规定程序将分析结果和整改要求向相关部门和人员进行反馈和通报。

5.5 应急管理

a） 应建立并落实联网医疗设备网络安全常态化监测预警、快速响应机制；

b） 应对联网医疗设备发生的网络安全事件进行识别和评估，制定专项网络安全应急预案，并定期开展演练；

c） 应及时将可能危害关键业务的联网医疗设备网络安全事件通报到相关部门和人员；
d） 应在联网医疗设备网络安全事件发生后及时收集证据，形成完整的事件处理报告，并采取措施防止联网医疗设备遭受再次破坏、危害或故障。

5.6 培训管理

a） 应制定联网医疗设备网络安全培训计划，并定期更新；
b） 应对联网医疗设备操作使用人员开展网络和数据安全意识培训，并保留相关记录；
c） 应根据不同联网医疗设备日常操作过程中可能产生的网络安全风险制定专项培训计划。

6 控制要求

6.1 设备采购

a） 应要求联网医疗设备供应商提供网络安全能力证明材料，如医疗器械网络安全注册申报资料等；
b） 应审核联网医疗设备供应商的安全保障能力和技术水平，在采购文件中要求供应商提供安全保障能力和技术水平的评估报告；
c） 应在采购合同中明确规定联网医疗设备供应商网络安全职责，对联网医疗设备的维护、医疗设备数据的外发等进行承诺说明；
d） 应与联网医疗设备供应商签订设备的安全更新和维护协议，明确保障时间和服务内容。

6.2 安装调试

a） 应根据联网医疗设备的分类分级情况建立操作规程，明确网络连接方法、异常连接处理方式等内容；
b） 应对入网前的联网医疗设备开展网络脆弱性扫描，识别设备可能存在的安全漏洞，并协调设备供应商开展漏洞修复，对于无法修复的漏洞，可采取外部网络安全防护措施进行补充；
c） 应根据联网医疗设备供应商提供的网络安全能力证明材料，如医疗器械网络安全注册申报资料等，对缺失的网络安全能力采取外部措施补充。

6.3 运行使用

a） 应编制并维护联网医疗设备资产清单，包括设备类型、厂商、IP/MAC 地址、设备唯一标识码等；
b） 应建立联网医疗设备资产安全管理制度，明确设备管理的责任部门和人员，对设备的运行使用进行规范化管理，确保设备在出现网络安全异常时能够及时进行跟踪和处置；
c） 应对操作联网医疗设备的人员，仅开放必需的、供其日常运行和维护所需的操作指令，确保不因权限过大导致联网医疗设备操作异常；
d） 应采取必要的措施识别联网医疗设备安全漏洞和隐患，评估其影响后及时修补；
e） 应建立健全联网医疗设备数据导出审批机制，严格控制数据导出流程，指派专人负责管理联网医疗设备数据的导出工作；
f） 应对联网医疗设备的电子数据交换接口执行全面封闭管理。

6.4 维护维修

a） 应对联网医疗设备的远程运维采取有效的安全防护管理措施；

b） 应对因外部维修而重新接入网络的联网医疗设备开展网络安全检查；
c） 应完整记录联网医疗设备的维护维修信息，包括维修时间、维修人员、维修内容等。

6.5 报废处置

a） 应对报废处置的联网医疗设备进行登记，包括报废时间、处置方式、数据删除情况等；
b） 联网医疗设备的报废处置应经过联网医疗设备网络安全管理组织的审批；
c） 应及时断开报废处置联网医疗设备的网络连接，对其内部存储的业务数据妥善处理后删除，确保数据不能恢复。

附 录 A
（规范性）
联网医疗设备网络安全技术防护要求

A.1 安全物理环境

a） 重要联网医疗设备应部署在安全的物理环境，充分考虑防雷、防火、防水、防静电、防震、防盗、电力供应、电磁防护等要求，应在设备存放处部署视频监控和警报系统；
b） 应将有线方式连接的联网医疗设备通信线缆铺设在隐蔽安全处；
c） 应合理规划重点区域（如 ICU、手术室等）联网医疗设备网络线路的铺设；
d） 涉及患者诊断、治疗、监护和护理的联网医疗设备应具有可供长时间稳定工作的电力供应。

A.2 安全通信网络

a） 应为联网医疗设备划分独立的网络区域，并按照方便管理的原则为联网医疗设备分配地址；
b） 应为移动式联网医疗设备提供安全的无线网络；
c） 应采用校验或密码技术保证联网医疗设备通信过程中数据的完整性；
d） 应采用密码技术保证联网医疗设备通信过程中数据的保密性。

A.3 安全区域边界

a） 应对非授权联网医疗设备私自联到内部网络、内部联网医疗设备非授权联到外部网络的行为进行监测和限制；
b） 应基于联网医疗设备所使用的通信协议建立细粒度的访问控制策略；
c） 应识别和检测联网医疗设备利用医疗专属协议（如 DICOM、HL7）、医疗物联网协议（如 MQTT）等发起的网络攻击行为；
d） 应对联网医疗设备远程访问行为、重要安全事件进行审计和分析；
e） 应完整收集联网医疗设备网络通信过程中的网络流量，确保在发生网络安全事件时能够回溯和分析。

A.4 安全计算环境

a） 应确保联网医疗设备在接入网络时具备唯一标识，实现联网医疗设备的准入控制；
b） 应严格限制联网医疗设备访问权限，动态监测设备的端口、服务和协议，为不同用户配置不同的访问控制策略；
c） 应及时对联网医疗设备的系统及固件进行升级，修复其网络安全缺陷；
d） 联网医疗设备应支持对登录的用户进行身份标识和鉴别，具有登录失败处理功能；
e） 应限制联网医疗设备所采集患者个人信息存储的数量和时长。

A.5 安全管理中心

a） 应对联网医疗设备自身的远程接入端口进行管控，建立统一的设备运维管理平台，实现认证、授权、账号、审计的集中管控；
b） 应建立区别于传统网络安全的联网医疗设备网络安全监控平台，对联网医疗设备网络安全事件集中收集，实现网络异常行为的精准分析和异常行为发生源的快速定位，并纳入主管部门的联网医疗设备安全监测体系；
c） 应记录联网医疗设备活动的日志，包括系统日志、操作日志、通信日志、安全日志等；

d） 应对联网医疗设备的安全策略、恶意代码补丁升级等事项进行集中管控。

附 录 B
（资料性）
联网医疗设备分类分级

确定联网医疗设备的分类，应依据联网医疗设备的使用形式和使用状况两方面情况综合判定。

联网医疗设备按照风险程度由低到高，等级依次分为1级、2级和3级。联网医疗设备风险程度应根据联网医疗设备的预期目的，通过使用形式、使用状态、是否接触人体等因素综合判定。

根据不同的预期目的，联网医疗设备的使用形式有：能量治疗、诊断监护、输送体液、电离辐射、实验室仪器、医疗消毒以及其他联网医疗设备等。

根据使用中对人体产生损伤的可能性、对医疗效果的影响，联网医疗设备使用状况可分为接触或进入人体和非接触人体联网医疗设备，具体可分为：

- 接触或进入人体联网医疗设备

联网医疗设备失控后造成的损伤程度分为：轻微损伤；损伤；严重损伤。

- 非接触人体联网医疗设备

对医疗效果的影响，其程度分为：基本不影响；有间接影响；有重要影响。

表 B.1 联网医疗设备分类分级判定表

接触或进入人体联网医疗设备				
使用形式		失控后造成的损伤程度对应风险程度		
		轻微损伤	损伤	严重损伤
1	能量治疗类	2级	2级	3级
2	诊断监护类	2级	2级	3级
3	输送体液类	2级	2级	3级
4	电离辐射类	2级	2级	3级
5	植入类	3级	3级	3级
6	其他一般联网医疗设备	2级	2级	3级
非接触人体联网医疗设备				
使用形式		对医疗效果的影响对应风险程度		
		基本不影响	有间接影响	间接重要影响
1	实验室仪器设备	1级	2级	3级
2	独立软件	-	2级	3级
3	消毒设备	-	2级	3级
4	其他辅助设备	1级	2级	3级

使用说明：

1.本表作为用于具体联网医疗设备的分类分级。表中符号"－ " 表示没有这种分类。

参 考 文 献

[1] WS/T 654—2019 医疗器械安全管理
[2] 中华人民共和国网络安全法（中华人民共和国主席令第53号）
[3] 中华人民共和国数据安全法（中华人民共和国主席令第84号）
[4] 数据出境安全评估办法（国家互联网信息办公室）
[5] 医疗卫生机构网络安全管理办法（国家卫生健康委、国家中医药局、国家疾控局）