ICS 11.040
CCS C 30

团　　体　　标　　准

T/CAME 82—2026

医疗机构联网医疗设备网络安全指南

Cybersecurity guidelines for hospital network connected medical devices

2026-01-15发布　　2026-01-15实施

中国医学装备协会　发布
中国标准出版社　出版

目　　次

前言 ……Ⅲ
1　范围 ……1
2　规范性引用文件 ……1
3　术语和定义 ……1
4　缩略语 ……1
5　基本原则 ……2
6　综合管理 ……2
7　风险管理 ……3
8　安全防护体系 ……3
9　设备生命周期网络安全工作 ……4
附录A(规范性)　联网医疗设备网络安全管理职责划分 ……10
附录B(资料性)　联网医疗设备资产分级分类参考 ……11
附录C(资料性)　联网医疗设备网络安全能力声明示例 ……12
附录D(资料性)　设备安全台账登记内容参考 ……19
附录E(规范性)　联网医疗设备网络安全风险管理 ……20
附录F(规范性)　网络安全防护与数据安全要求 ……22
附录G(资料性)　联网医疗设备安装验收相关评估样表 ……25
参考文献 ……28

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。

本文件由中国医学装备协会提出并归口。

本文件起草单位：中国医学装备协会、中国医学装备协会医学装备信息交互与集成分会、中国医院协会信息专业委员会、清华大学、北京大学第一医院、浙江大学医学院附属第一医院、首都医科大学附属北京天坛医院、首都医科大学附属北京友谊医院、首都医科大学附属首都儿童医学中心、北京协和医院、江苏省人民医院、中南大学湘雅医院、上海交通大学医学院附属瑞金医院、广东省人民医院、四川大学华西医院、解放军总医院、山西省人民医院、福州大学附属省立医院、中国信息通信研究院、国家信息技术安全研究中心、飞利浦（中国）投资有限公司、西门子医疗系统有限公司、通用电气医疗系统贸易发展（上海）有限公司、深圳迈瑞生物医疗电子股份有限公司、上海联影智元医疗科技有限公司、北京数字认证股份有限公司、杭州安恒信息技术股份有限公司、上海柯渡医学科技股份有限公司、福建中信网安信息科技有限公司、深信服科技股份有限公司、北京惠泽智信科技有限公司。

本文件主要起草人：侯岩、李志勇、王才有、王韬、刘海一、孙晓伟、冯靖祎、李瑞、王力华、于雪梅、行辰、羊月祺、冯嵩、芮欣凯、李丹、石锐、邱明辉、吕晋栋、陈礼团、张涛、彭盼、何友斌、江海、薛瀚、葛鑫、杨志勇、于淄、黎耀、陈燕祥、汪胜平、霍天宇、李方舟、刘钰、傅大鹏、王琼霄、高学玲、武进、倪军、张建、何颖、邓宙锦、何凯杰、白云云、宋平、陈顺云。

医疗机构联网医疗设备网络安全指南

1 范围

本文件提供了医疗机构联网医疗设备网络安全的基本原则、综合管理、风险管理、安全防护体系，以及设备生命周期各环节中的网络安全相关工作的指南。

本文件适用于医疗机构使用。

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 35273 信息安全技术 个人信息安全规范

GB/T 43697 数据安全技术 数据分类分级规则

GB/T 44585.1 风险管理在接入IT网络的医疗器械中的应用 第1部分：联网医疗器械或健康软件在其实施和使用中的安全、有效性和网络安全

3 术语和定义

下列术语和定义适用于本文件。

3.1

联网医疗设备 network 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医疗设备。

注：本文件中的“设备”“医疗设备”无特殊说明均指“联网医疗设备”。

3.2

安全域 security domain

遵从共同安全策略的资产和资源的集合。

[来源：GB/T 25068.1—2020，3.357]

4 缩略语

ACL(Access Control List)访问控制(列)表

ATNA(Audit Trail and Node Authentication)审计追踪和节点认证

DICOM(Digital Imaging and Communications in Medicine)医学数字成像和通信

HL7 (Health Level Seven)健康信息交换第七层协议

IDS(Intrusion Detection Systems)入侵检测系统

IHE(Integrating the Healthcare Enterprise)医疗机构企业级集成规范

SBOM(Software Bill of Materials)软件物料清单

USB(Universal Serial Bus)通用串行总线

VLAN(Virtual Local Area Network)虚拟局域网
VPN(Virtual Private Network)虚拟专用网

5 基本原则

5.1 统一管理:纳入医疗机构统一安全管理体系,统筹安全规划,落实安全策略。
5.2 最小必要:仅授予必要的数据和系统访问权限,仅启用必要的端口、接口及服务等。
5.3 分层防护:构建网络边界、终端、数据和应用的多层防护体系。
5.4 数据保护:数据分级分类,并制定相应的访问控制和审批流程。
5.5 平衡兼顾:平衡业务与安全管理需求,在不影响医疗业务正常开展的前提下,做好安全防护。
5.6 持续改进:定期评估风险,动态优化安全策略。

6 综合管理

6.1 组织管理

6.1.1 组织架构

6.1.1.1 联网医疗设备网络安全应由医疗机构网络安全和信息化工作领导小组统一管理。
6.1.1.2 联网医疗设备网络安全工作应由医疗设备管理部门(包括配置、采购、运维和处置等职能)、信息管理部门(涵盖系统、网络及终端管理职责)、医疗管理部门以及设备使用部门的负责人组建工作组,落实相关要求,完成日常工作。
6.1.1.3 医疗机构应明确各部门职责分工,联网医疗设备网络安全工作组定期组织开展联网医疗设备网络安全形势监测、分析和评估工作,制定突发事件应急预案,并定期组织演练。

注:本文件中的管理部门以管理职责作为依据,与医疗机构实际管理部门设置可能有所不同(例如文中提及的医疗设备管理部门,其采购管理职责可能由医学工程处承担,也可能由独立的招标采购中心承担)。

6.1.2 职责划分

医疗机构各部门应分工合作、明确职责,划分安全责任。具体职责划分见附录A。

6.2 制度管理

6.2.1 医疗机构应遵照国家法律法规要求,参考相关标准,建立完善覆盖生命周期各环节的《联网医疗设备网络安全管理制度及技术规范》,明确安全策略、管理流程及岗位职责,并定期检查制度落实情况。
6.2.2 管理制度及工作流程宜定期评估,对标上位文件变化,根据安全态势及安全检查发现的问题及时修订,并开展培训。
6.2.3 工作记录应规范完整,可充分反映制度和工作流程的落实情况。

6.3 人员管理

6.3.1 明确医疗机构内、外部人员岗位网络安全职责和保密内容(包含但不限于保密对象、范围、内容和期限)并签署医疗机构统一格式的网络安全与保密协议,网络安全与保密协议内容明确联网医疗设备网络安全要求。
6.3.2 设备管理部门联合信息管理部门定期组织联网设备网络安全培训,培训对象包含管理、使用、运维、数据处理等人员;设备操作人员接受培训后方可授权使用设备。

6.3.3 按最小必要、职责分离原则进行统一权限分配管理，并记录完整的审批日志。

6.3.4 人员变动时，及时更新或撤销其权限，确保权限分配与实际工作需求一致。审批备案并重新签署网络安全与保密协议。

6.3.5 外部服务人员采取白名单制度，验证身份，登记备案。

6.3.6 医疗机构内、外部人员均严格遵守医疗机构的网络安全政策和操作规程，及时上报网络安全事件。

6.4 资产管理

6.4.1 联网医疗设备资产清单

医疗机构宜根据联网情况、网络安全风险对医疗设备进行分类分级并登记备案，形成联网医疗设备清单。定期进行资产盘点，并补充未登记在册的资产，包括联网低值设备、开展科研合作的联网医疗设备等。联网医疗设备安全分级方法可见附录B中B.1。

6.4.2 设备数据资产清单

医疗设备的数据应纳入医疗机构数据安全管理体系，按照《数据安全法》《个人信息保护法》的要求，依据国家卫生健康委等医疗健康行业主管部门的指导意见，进行数据分类分级，形成数据资产清单，对其用途进行登记，并对不同数据资产进行针对性保护。设备数据分类原则可见B.2。

6.5 设备网络安全台账管理

6.5.1 医疗机构宜在资产管理登记信息基础上，为联网医疗设备建立设备网络安全台账，确保信息真实、准确、完整和可追溯，宜使用信息系统记录设备安全关键信息。

6.5.2 医疗设备管理部门宜指定专人(兼职/专职)负责设备网络安全台账管理工作，制定安全台账权限管理和授权访问策略。

6.5.3 医疗机构可参照附录C，要求医疗设备制造商提供产品网络安全能力说明文件，设备管理部门审核并登记归档相关文件。联网部署信息由信息管理部门提供。设备安全台账登记内容可见附录D；

6.5.4 医疗机构应对设备运维过程及设备软硬件的变更信息进行记录，包括运维工程师及其授权信息、变更信息、升级信息、设备安全检查及加固信息等；

a) 医疗设备报废与处置，应记录数据销毁时间、执行人、操作内容、数据资产处置情况等；

b) 设备安全台账信息的变更操作应有双人复核并保留日志或记录。

7 风险管理

按照GB/T 44585.1，在联网医疗设备的生命周期各环节落实风险管理，具体风险管理要点见附录E。

8 安全防护体系

8.1 网络规划设计

8.1.1 组网方式

联网医疗设备组网遵循安全性、稳定性、可扩展性及标准化原则，按照医疗机构网络安全统一管理要求，采用分层分域的方式，宜为联网医疗设备建立专用网络(例如逻辑隔离的医疗设备网络区域)。

8.1.2 安全域规划

对联网医疗设备专用网络进行安全域划分，按设备类型、业务功能属性或设备网络安全级别等多种划分方式将各类医疗设备归至各自安全域，实施分域安全管理，避免因网络风暴或其他网络安全因素造成医疗设备全域网络不稳定或瘫痪。

a） 按设备类型：如按放射影像、心电、超声、监护类设备等划分。

b） 按业务属性：考虑业务场景或空间进行划分，业务场景如临床诊疗域（含手术室、ICU设备）、医技检查域（含放射影像、检验科设备）等；业务空间如门诊、病房等。

c） 按设备网络安全级别：如医疗机构中业务使用的具有网络安全高风险联网医疗设备，考虑独立划分。

8.2 网络安全防护

网络安全防护宜包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等内容，具体要求见附录F中F.1。

a） 安全物理环境，对在独立机房部署应用的联网医疗设备实现物理环境安全保障。

b） 安全通信网络，对具有对外通信功能的联网医疗设备实现通信网络安全保障。

c） 安全区域边界，基于联网医疗设备部署应用的安全域实现区域边界安全保障。

d） 安全计算环境，对接入医疗机构信息系统的联网医疗设备实现计算环境安全保障。

e） 安全管理中心，医疗机构根据联网医疗设备的网络安全管理需求和整体的网络安全规划，采取共享或独立的联网医疗设备网络安全管理中心进行设备的网络安全管理。

8.3 数据安全与个人信息保护

联网医疗设备数据安全与个人信息管理纳入医疗机构整体数据安全管理体系。

a） 对联网医疗设备在医疗机构中收集与产生、存储与传输、使用与共享等医疗设备数据全生命周期的管理过程，实现数据安全保护，具体要求见F.2.1。

b） 遵守《个人信息保护法》的相关规定，按照GB/T 35273要求开展个人信息保护工作，确保联网医疗设备收集信息限定在合理且必要的最小范围，个人信息保护受限可控，具体要求见F.2.2。

c） 在向境外提供联网医疗设备中的患者个人信息或医疗数据时，遵守国家的相关法律法规及卫生健康行业的数据管理规定，进行全面的安全评估，并持续接受相关部门的监督。

9 设备生命周期网络安全工作

9.1 设备论证与招标采购

9.1.1 配置论证

使用科室提出设备需求申请，说明设备是否需要联网、数据使用场景等内容；设备管理部门和信息管理部门组织专家对拟配置的联网医疗设备网络安全进行论证，为是否配置此种设备提供辅助决策；论证内容包含：

a） 联网方式是否与医疗机构现有网络资源匹配，是否符合医疗机构网络安全规划要求；

b） 是否存在敏感数据；

c） 数据是否在医疗机构内部存储、是否出境；

d） 必要时收集相关产品的网络安全资料，判断是否具有安全防护能力。

9.1.2 安全评估

对于已纳入采购计划的医疗设备，在采购意向公开后，由设备管理部门、信息管理部门、医疗管理部门、设备使用部门共同参与，对响应采购意向公告的厂商及其产品进行网络安全评估，包括联网技术可行性、数据使用合规性、安全防护方案可靠性。

a) 评估拟采购设备网络安全风险，重点关注个人信息和敏感数据、加密方式、互联网连接、云计算、数据出境、数据存储方式等方面的风险。
b) 评估设备厂商的网络安全保障技术能力和资质。
c) 依据风险评估结果，必要时，要求厂商提供网络安全应对方案。
d) 形成联网医疗设备的网络安全需求。

9.1.3 招标采购

9.1.3.1 根据拟采购联网医疗设备的网络安全需求，拟定标书中网络安全要求，宜在标书中明确设备接口应支持的医疗设备网络安全相关接口技术标准(例如IHE ATNA等)。

9.1.3.2 网络安全要求中包括需要医疗设备厂商提供的网络安全相关资料，如设备网络安全能力声明(见附录C)、必要的网络安全方案等。

9.1.3.3 对参与竞标的医疗设备网络安全能力进行评估，并将其作为评标指标。

9.1.4 合同要求

拟定合同中建议包含网络安全相关内容，或签订专门的网络安全协议。重点包括以下内容。

a) 明确厂商在设备软件安装升级、运行维护、故障处理等环节中需承担的网络安全责任、义务及违约后果。
b) 将设备网络安全能力声明及竞标中提供的网络安全方案等材料作为合同附件一并签署。
c) 宜在合同中说明以下的网络安全要点：
   1) 厂商未经授权不得使用医疗设备存储的医疗数据；
   2) 明确由厂商承担的数据保密的责任、义务及违约后果；
   3) 厂商提供全生命周期的安全技术支持，如安全加固、安全补丁升级等；
   4) 厂商承诺在提供的医疗设备软硬件中不得包含恶意代码及后门程序；
   5) 厂商承诺在设备安装、维修、保养等服务中，确保参与服务的员工知晓和能够遵守医疗机构网络安全的要求。

9.2 设备联网安装调试验收

9.2.1 环境准备

设备厂商提出联网设备网络安装环境需求，设备管理部门按照规划组织相关人员实地踏勘，信息管理部门审核需求、依据网络安全管理规划和策略，准备环境，三方达成共识，对网络安装环境进行确认(见附录G中G.1)。

9.2.2 安全方案

设备厂商根据已确认的网络安装环境和业务场景、资源情况及网络安全管理策略提出安全方案，包含联网和安全防护技术方案。联网方案包括网络接入方式、网络带宽、网络配置，以及安装调试方案、软件安装清单等；安全防护技术方案可参考第8章，并包括应急保障等。设备管理部门、设备使用部门和信息管理部门共同审核及确认安全方案。

9.2.3 到货核验

医疗设备管理部门与设备使用部门核验装箱清单，对网络安全相关硬件（如独立组网设备，外联设备等）进行清点，暂不安装的硬件可由设备管理部门统一保管和登记，对软件许可证、授权码等进行核验。

9.2.4 联网部署

9.2.4.1 医疗机构信息管理部门根据网络规划分配网络资源，设置并协助部署医疗设备的网络参数及安全策略。

9.2.4.2 设备管理部门协调设备供应商对联网医疗设备依据安全方案进行配置。重点关注：

a) 默认口令更改：宜根据网络安全防护要求修改默认账号初始口令（尤其是启用高权限访问账号的口令）；
b) 账号管理：按职责分离，最小特权原则配置账号及其权限，原则上宜禁用通用账号，改为实名登录。不包括紧急情况下用户紧急访问机制；
c) 存储加密：医疗设备宜开启存储加密；
d) 禁用非必要端口和服务：在不影响医疗设备使用和运维的前提下，禁用系统配套的主机USB端口，网络端口及服务；
e) 落实网络安全策略配置：如防火墙（ACL）、网络分段、关键资源（如数据库和操作系统）访问控制配置；
f) 审计日志：启用审计日志；
g) 软件安装：按照软件清单安装，不安装未经测试和来历不明的软件，符合要求但不在清单范围内的软件，可另行申请报批，通过后更新软件安装清单；
h) 安全补丁更新：确保厂商将最新已验证的安全补丁更新到医疗设备中；
i) 备份与校验：对关键资源建立备份机制（如数据，恢复镜像等），配置备份任务，开启校验功能；
j) 物理锁：有条件宜对独立的网络和数据机柜上锁，对无法关闭的非必要端口进行物理封堵等。

9.2.5 网络安全测试

部署完成后，依据安全方案要求，信息管理部门、设备管理部门和设备使用部门共同对联网设备进行网络安全测试，必要时可邀请具有资质的第三方机构测评。测试中发现的问题及时整改，复测后出具安全网络测试报告。

9.2.6 网络安全培训

医疗设备管理部门和信息管理部门按需组织对医疗设备管理、使用、运维人员的网络安全培训。医疗设备厂商需提供培训的技术支持。见G.2记录培训参与人员及内容。

9.2.7 网络安全验收

设备网络安全验收时，由设备管理部门和信息管理部门共同组织，重点内容包括网络配置、系统配置、权限配置、端口管理、安全策略、数据备份、安全台账、培训记录、运维方案及应急保障。参见附录G.3进行医疗设备网络安全验收记录。未通过安全验收的设备不能联网使用。

9.3 设备使用与运维

9.3.1 使用管理

设备使用部门与设备网络安全相关的管理工作包括但不限于内容。

a) 按要求规范使用设备，不得违规更改设备相关配置。
b) 按职责分离、最小必要原则配置账号及权限。对于无法禁用但应使用的通用账号，每次使用时登记使用人员与时间，确保与系统操作日志记录匹配。
c) 妥善保管账号和口令，不得共享、主动泄露。
d) 不在设备上安装非软件安装清单内的软件。确需安装的，另行申请报批。
e) 对于数据的使用、加工、共享等操作（例如数据导入、导出、拷贝），申请并经授权后方可实施。该操作仅限于被授权的特定场景。
f) 不违规接入USB等移动存储介质。
g) 设备数据拷贝时，宜对拷贝存储介质做病毒扫查，防止拷贝过程中病毒或木马程序的植入。
h) 设备退网使用时，通知设备和信息管理部门回收网络配置资源，删除网络操作权限。
i) 设备移出医疗机构使用时，向设备管理部门报备，宜清除敏感数据，并保留数据清除处理记录。
j) 设备使用过程中，如发现异常情况，及时报告相关部门处理。

9.3.2 运维管理

9.3.2.1 日常运行中的网络安全管理

9.3.2.1.1 设备系统管理员账号，宜由设备管理部门指定专人管理。
9.3.2.1.2 设备巡检宜包含安全巡检，记录安全状态。
9.3.2.1.3 定期对设备日志进行分析与审计，发现异常时记录并及时采取措施。
9.3.2.1.4 在医疗设备技术兼容的前提下，医疗机构可配置专业工具，监测设备外围状态和网络行为，发现异常时记录并及时采取措施。
9.3.2.1.5 宜采取适宜的技术手段识别设备安全漏洞和隐患，明确漏洞风险等级及修复时间要求，及时修复并进行验证。

9.3.2.2 维护维修中的网络安全管理

9.3.2.2.1 验证设备维护维修人员身份及授权情况。
9.3.2.2.2 记录维护维修过程。
9.3.2.2.3 维护维修完成后，由专人确认设备状态并检查是否存在潜在风险，尤其需要注意是否有网络安全风险、数据安全风险等。
9.3.2.2.4 外部维修人员对高风险设备开展现场维修，由医疗机构专人陪同。
9.3.2.2.5 未经授权不得通过互联网远程连接到医疗设备开展远程监控及维护维修。如确需开展，经过医疗机构相关管理部门审批后，通过医疗机构控制的网络安全管理设备接入互联网，采用有效的运维管控措施，包括开设账号、分配权限、设置访问起止时间、登记备案并监控操作行为。
9.3.2.2.6 维护维修过程中，原则上不得使用设备中的个人信息。如确需使用，取得管理部门同意，采取安全防范处理和监督措施后，方可使用。
9.3.2.2.7 设备召回、返厂维护维修时，应清除敏感数据，并保留数据清除处理记录。

9.3.2.3 更新升级中的网络安全管理

9.3.2.3.1 对于设备软件补丁及功能升级，报设备管理部门和信息管理部门进行安全评估，经审批后实施。
9.3.2.3.2 升级申请内容包括但不限于：升级背景，升级内容说明，升级技术方案（含回退方案）。

9.3.2.4 网络安全事件处置与记录

9.3.2.4.1 遵循国家及医疗机构内部相关要求对网络安全事件进行处置与响应。

9.3.2.4.2 对网络安全事件进行登记和管理，形成网络安全事件记录。记录包括事件发生时间、事件摘要、上报部门、上报人、处置记录、原因分析、加固处理、升级处理、召回处理等内容。

9.3.3 网络安全检查

9.3.3.1 检查方式

可通过人工问询、设备检查、记录审阅、检测工具检测、或通过有资质的第三方安全检测机构的安全检测与评估等方式，开展网络安全检查。

9.3.3.2 医疗设备使用与运维检查

对医疗设备使用与运维进行网络安全检查，检查安全制度与要求的落实情况。检查内容宜包括但不限于：

a) 医疗设备专网接入及访问日志；
b) 医疗设备外联链路；
c) 医疗设备安全配置；
d) 医疗设备巡检、运维、更新升级记录。

9.3.3.3 数据安全与个人信息保护检查

对医疗设备使用与运维过程中涉及的数据安全与个人信息保护措施的落实情况进行安全检查。检查内容宜包括但不限于：

a) 数据使用、加工、共享操作的审批；
b) 数据传输与存储安全措施的实施；
c) 数据访问控制是否遵循最小必要原则；
d) 用户操作是否追溯到个人。

9.3.4 安全整改与加固

a) 对于网络安全检查发现的问题，及时采取安全整改与加固措施，包括管理层面，如制度、流程优化，以及技术层面，如网络、终端加固；
b) 安全整改与加固措施宜考虑问题产生的根因；
c) 安全整改与加固措施宜与问题可能造成的影响相适应；
d) 核验安全整改与加固措施实施的有效性；
e) 记录上述问题、采取的安全整改与加固措施，以及采取措施后的结果。

9.4 报废与处置

9.4.1 处置场景

医疗设备处置场景包括设备报废、设备转让等。

9.4.2 处置方式

9.4.2.1 处置前，评估设备中是否存在残留的数据资产，重点关注设备中个人信息和敏感数据。

9.4.2.2 设备停用后，进行安全检查，必要数据归档后，销毁数据。

9.4.2.3 数据销毁在相关方见证下（如医疗设备管理部门、信息管理部门等），可采用物理销毁、消磁处理、加密清除、复写处理等方法进行，验证销毁的有效性，并做好记录。

9.4.2.4 数据销毁后，方可将报废医疗设备交由具备资质的处置单位进行统一处置。

9.4.2.5 禁用设备相关账号，回收相关网络资源，并纳入设备安全台账。

9.4.3 销毁记录

在设备安全台账中详细记录处置及销毁过程及相关信息，确保全过程可追溯。

附 录 A
（规范性）
联网医疗设备网络安全管理职责划分

A.1 部门职责

医疗机构各部门应分工合作、明确职责：

——信息管理部门负责制定安全规划，部署网络安全策略、协助联网医疗设备网络安全调试验收，定期开展安全检查；

——医疗设备管理部门在设备全生命周期管理各环节组织督办落实安全管理要求并监督运维与整改；

——医疗管理部门监督设备使用部门人员权限管理、审批数据应用申请；

——设备使用部门在日常使用中落实安全管理要求及上报发现的安全问题。

A.2 岗位职责

联网医疗设备网络安全关键人员应明确工作职责，承担相应工作任务和责任。

——信息管理部门网络安全管理员，牵头制定联网医疗设备网络安全规划，审核联网医疗设备网络安全技术方案，指导并配合完成联网医疗设备的网络配置和安全部署，参与设备网络安全验收；定期组织对联网医疗设备的安全检查，跟进网络安全相关政策和安全事件，反馈指导设备管理部门排查和整改。

——医疗设备管理部门宜设立联网医疗设备安全协调员，根据管理要求统筹落实联网医疗设备网络安全日常管理工作，组织定期培训；监督、落实安全任务；收集、汇总、分析各设备使用部门发现和上报的安全问题，并向部门负责人汇报；接受信息管理部门的安全指导，共同制定联网设备网络安全整改方案并督办检查整改成果。

——医疗设备管理部门运维人员，负责所管理设备的系统管理员账号的保管及合规使用，完成安全和配置工作；监督外部人员对重要设备或高风险设备运维过程，并做好记录。

——医疗管理部门宜指定专人负责联网医疗设备网络安全相关事宜（如权限管理、数据应用审批）；设备使用科室宜设立本科室的联网医疗设备网络安全协调员（可由本科室设备保管人兼职），除承担设备常规管理工作外，宜明确网络安全职责，如组织本科室人员参加安全培训，收集使用中发现的网络安全问题及时上报到设备管理部门，配合落实安全检查及整改等。

附 录 B
（资料性）
联网医疗设备资产分级分类参考

B.1 联网医疗设备安全分级方法

设备分级参照GB/T 22240—2020进行，具体方法见B.1.1～B.1.4。

B.1.1 根据联网医疗设备网络安全被破坏时可能侵害的客体以及客体被侵害的程度，重点考虑以下因素：

a） 网络安全事件可能导致的患者人身安全和设备故障问题；

b） 医疗设备网络的攻击可能对医疗机构内部网络或系统的侵害；

c） 医疗数据泄露的危害。

B.1.2 依据表B.1可得到联网医疗设备安全等级。

表B.1 联网医疗设备安全分级矩阵表

设备网络安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

B.1.3 设备网络安全被破坏时所侵害的客体类型举例：

a） 公民、法人和其他组织的合法权益：设备，设备直接影响的患者，医疗机构内部网络、系统、数据等；

b） 社会秩序、公共利益：医疗机构提供的就诊服务。

B.1.4 对相应客体的侵害程度举例：

a） 一般损害：设备自身故障短时间无法正常运转，设备直接影响的患者服务短时间中断；

b） 严重损害：设备自身故障长时间无法正常运转，设备直接影响的患者人身安全受轻微影响，设备直接影响的患者数据遭泄露，医疗机构内部少数非核心网络与系统受影响，就诊服务局部中断；

c） 特别严重损害：设备损毁，设备直接影响的患者人身安全受重大影响（如人员伤亡），医疗机构内部多数或核心网络与系统受影响，大量医疗数据泄露，就诊服务全面中断。

注：联网医疗设备通常不涉及国家安全，安全等级通常不超过第三级。

B.2 设备数据分类原则

设备数据宜参考如下原则进行分类：

a） 设备配置参数数据：医疗设备运行所需要配置的设备参数和联网运行所需要配置的网络通信参数等数据；

b） 设备运行状态数据：设备记录的运行过程状况、维护与升级操作等信息的数据（含日志），主要用于监测医疗设备运行，这类数据不包含个人信息和诊疗记录；

c） 设备医疗数据：医疗设备在诊疗使用中所产生的医疗记录数据，通常包含个人信息和诊疗记录。

附 录 C
（资料性）
联网医疗设备网络安全能力声明示例

联网医疗设备网络安全能力声明示例见表C.1～表C.24。

表C.1 基本信息

序号	问题	回答(是/否/不适用)	备注
1	制造商名称		
2	设备描述		
3	设备型号		
4	制造商联系信息		
5	协调漏洞披露：制造商是否有针对此设备的漏洞披露计划？		
6	设备在网络连接环境中的预期用途 是否有网络或数据流图可用于指示与其他系统组件或预期外部资源的连接？		

表C.2 数据的管理

序号	问题	回答(是/否/不适用)	备注
1	此设备是否可以显示、传输、存储或修改医疗记录数据或个人信息？		明确存储的时长、容量、数量等信息
2	设备是否可配置在将本地数据存储到数据中心后自动删除本地数据？		
3	设备是否允许运维人员移除内部介质(例如用于单独销毁或交由医疗机构保留)？		明确销毁方式的限制
4	设备是否可打印包含个人信息的硬拷贝与报告？		
5	设备是否通过外部网络(例如互联网)传输/接收医疗记录数据或个人信息？		
6	设备是否通过专有协议传输/接收数据？		

表C.3 自动注销

序号	问题	回答(是/否/不适用)	备注
1	设备是否可以配置为在预定的非活动时间(例如自动注销、会话锁定、受密码保护的屏幕保护程序)后强制对登录用户进行重新授权？		
2	用户或管理员在自动注销/屏幕锁定之前的不活动时间长度是否可配置？		

表C.4 审核

序号	问题	回答(是/否/不适用)	备注
1	医疗设备是否可以创建标准操作系统日志之外的其他审核日志或报告？		

表 C.4 审核（续）

序号	问题	回答(是/否/不适用)	备注
2	事件是否记录在审核日志中？如果是，请指示审核日志中记录了以下哪些事件？		
3	所有者/操作员是否可以定义或选择在审计日志中记录哪些事件？		
4	是在审核日志中捕获的可用事件的数据属性列表？		
5	可以导出审核日志内容？		
6	所有者/操作员可以监控/审查审计日志？		
7	是否保护审核日志不被修改？		
8	设备是否可以分析审核日志？		

表 C.5 授权

序号	问题	回答(是/否/不适用)	备注
1	设备是否有阻止未经授权的用户访问的能力？		
2	是否可以根据“角色”(例如用户、管理员和/或服务等)为用户分配不同的权限级别？		
3	设备所有者/操作员是否可以授予自己不受限制的管理权限(例如通过本地 root 或管理员账户访问操作系统或应用程序)？		
4	设备是否授权或控制所有 API 访问请求？		
5	默认情况下，设备是在受限访问模式下运行，还是在“熟台 kiosk 模式”下运行？		

表 C.6 网络安全补丁升级

序号	问题	回答(是/否/不适用)	备注
1	设备是否包含任何在其运行生命周期内可能需要安全更新的软件或固件，无论是设备制造商还是软件/固件的第三方制造商？		
2	设备文档是否提供所有者/操作员安装修补程序或软件更新的说明？		
3	制造商是否在批准安装更新时通知客户？		
4	设备是否执行软件更新的自动安装？		
5	制造商是否有可在设备上安装的第三方软件的批准列表？		
6	所有者/运营商能否自行在设备上安装制造商认可的第三方软件？		
7	制造商是否有适当的流程来评估设备漏洞和更新？		

表 C.7 数据去标识化与匿名化

序号	问题	回答(是/否/不适用)	备注
1	设备是否提供对个人身份信息进行去标识化的功能？		

表 C.8　数据备份与灾难恢复

序号	问题	回答(是/否/不适用)	备注
1	设备是否为长期保留个人信息(例如PACS)的主要存储?		
2	设备是否具有"恢复出厂设置"功能,以恢复制造商提供的原始设备设置?		
3	设备是否具有完整备份至可移动媒介的功能?		
4	设备是否具有远程备份的功能?		
5	设备是否具有备份功能可恢复系统配置信息、修补还原和软件恢复?		
6	设备是否提供检查备份完整性和真实性的功能?		

表 C.9　紧急访问

序号	问题	回答(是/否/不适用)	备注
1	设备是否包含紧急访问(即"破窗")功能?		

表 C.10　数据完整性与真实性

序号	问题	回答(是/否/不适用)	备注
1	设备是否提供存储的健康数据的数据完整性检查机制(例如哈希或数字签名)?		
2	设备是否为存储的健康数据(例如RAID-5)提供错误/故障保护和恢复机制?		

表 C.11　恶意软件探测与防护

序号	问题	回答(是/否/不适用)	备注
1	设备是否支持使用防病毒软件(或其他反恶意软件机制)? 在注释中提供详细信息或参考。		
2	设备是否使用应用程序白名单来限制允许在设备上运行的软件和服务?		
3	设备是否采用基于主机的入侵检测/防御系统?		

表 C.12　节点鉴别

序号	问题	回答(是/否/不适用)	备注
1	设备是否提供/支持任何节点身份验证方式,以确保数据的发送方和接收方彼此知道并有权接收传输的信息(例如Web API、SMTP、SNMP)?		
2	是否支持网络访问控制机制(例如设备是否具有内部防火墙,或使用网络连接白名单)?		
3	设备是否使用基于证书的网络连接身份验证?		

表 C.13　连通性

序号	问题	回答(是/否/不适用)	备注
1	设备是否具有硬件连接功能?		
2	制造商是否提供设备上已使用或可能使用的网络端口和协议的列表?		
3	设备能否与客户环境中的其他系统通信?		
4	设备能否与客户环境外部的其他系统(例如设备厂商的服务主机、第三方存储)通信?		
5	设备是否发出或接收API调用?		
6	设备是否需要互联网连接才能实现其预期用途?		
7	设备是否支持传输层安全性(TLS)?		提供版本号和密码算法
8	设备是否从单独的设备(例如远程医疗)提供操作员控制功能?		

表 C.14　人员鉴别

序号	问题	回答(是/否/不适用)	备注
1	设备是否支持并强制所有用户和角色(包括服务账户)使用唯一标识和密码?		
2	设备是否配置为通过外部身份验证服务(例如AD、NDS、LDAP、OAuth等)对用户进行身份验证?		
3	设备是否配置为在一定次数的不成功登录尝试后锁定用户?		
4	文档中列出了所有默认账户(例如技术人员服务账户、管理员账户)?		
5	可以更改所有密码吗?		
6	设备是否可配置,以强制创建满足既定(组织特定)复杂性规则的用户账户密码?		
7	设备是否支持设置账户密码过期?		
8	设备是否支持多重身份验证?		
9	设备是否支持单点登录(SSO)?		
10	是否可以在设备上禁用/锁定用户账户?		
11	设备是否支持生物识别(如指纹、人脸等)控制?		
12	设备是否支持物理令牌(例如U盾)?		
13	应用程序或设备是否存储或管理身份验证凭据?		

表 C.15　物理防护

序号	问题	回答(是/否/不适用)	备注
1	设备是否仅是软件? 如果是,请对本节中的其余问题回答"不适用"。		

表 C.15 物理防护（续）

序号	问题	回答(是/否/不适用)	备注
2	维护个人身份信息的所有设备组件(可移动媒体除外)是否在物理上安全(即,在没有工具的情况下无法删除)?		
3	是否所有维护个人身份信息(可移动媒体除外)的设备组件都物理地固定在单独键控锁定设备后面?		
4	设备是否允许客户附加物理锁以限制对可移动媒介的访问?		

表 C.16 现成软件维护

序号	问题	回答(是/否/不适用)	备注
1	在产品开发过程中是否遵循了安全的软件开发过程?		
2	制造商是否评估设备中包含的第三方应用程序和软件组件以确保安全开发实践?		
3	制造商是否有管理第三方组件生命周期终止的计划?		

表 C.17 现成软件清单

序号	问题	回答(是/否/不适用)	备注
1	此产品是否有可用的软件物料清单?		
2	软件物料清单是否识别了软件组件?		
3	设备是否包含可用于生成设备上安装的软件组件列表的命令或进程方法?		
4	软件物料清单是否有更新流程?		

表 C.18 系统加固

序号	问题	回答(是/否/不适用)	备注
1	设备是否按照任何行业标准进行了加固?		
2	设备是否获得了任何网络安全认证?		
3	设备是否采用任何软件完整性检查机制		
4	所有者/操作员是否可以执行软件完整性检查(即验证系统未被修改或篡改)?		
5	系统是否可配置以允许实施文件级、患者级或其他类型的访问控制?		
6	在系统交付时,制造商是否对任何系统或用户账户进行不受限制或禁用?		
7	是否禁用了设备预期用途不需要的所有共享资源(例如文件共享)?		
8	是否禁用了设备预期用途不需要的所有通信端口和协议?		
9	是否已删除/禁用设备预期用途不需要的所有服务(例如 telnet、文件传输协议[FTP]、互联网 信息服务器[IIS]等)?		
10	是否删除/禁用了设备预期用途不需要的所有应用程序(商用现成应用程序以及操作系统包含的应用程序,例如浏览器等)?		

表 C.18 系统加固（续）

序号	问题	回答(是/否/不适用)	备注
11	设备是否可以禁止从不受控制的或可移动的介质(即内部驱动器或内存组件以外的来源)启动?		
12	是否可以在不使用物理工具的情况下在设备上安装未经授权的软件或硬件?		
13	产品文档是否包含有关用户操作网络安全扫描的信息?		
14	设备是否可以在默认提供状态之外进行加固?		
15	系统是否可以在引导期间阻止访问 BIOS 或其他引导加载程序?		

表 C.19 网络安全使用指导

序号	问题	回答(是/否/不适用)	备注
1	设备是否包含所有者/运营商的安全文档?		
2	设备是否具有从设备或媒体中永久删除数据的功能并提供说明?		
3	是否记录了所有访问账户?		
4	产品是否包含有关设备的推荐补偿控制的文档?		

表 C.20 数据存储保密性与完整性

序号	问题	回答(是/否/不适用)	备注
1	设备可以加密静态数据吗?		
2	是否可以更改或配置加密密钥?		
3	数据存储在设备上的数据库中吗?		
4	数据是否存储在设备外部的数据库中?		

表 C.21 数据传输保密性

序号	问题	回答(是/否/不适用)	备注
1	个人身份信息只能通过点对点专用电缆传输吗?		
2	个人身份信息在通过网络或可移动媒体传输之前是否加密?		
3	个人身份信息传输是否不受限制地传输到固定的网络目的地列表?		
4	连接是否仅限于经过身份验证的系统?		
5	是否支持/实施安全传输方法(DICOM、HL7、IEEE 11073)?		

表 C.22 数据传输完整性

序号	问题	回答(是/否/不适用)	备注
1	设备是否支持任何旨在确保数据在传输过程中不被修改的机制(例如数字签名)?		
2	设备是否包含多个通过外部电缆连接的子组件?		

表 C.23 远程访问与控制

序号	问题	回答(是/否/不适用)	备注
1	设备是否允许远程服务连接以进行设备分析或维修?		
2	设备是否允许或使用远程服务连接来获取预测性维护数据?		
3	设备是否具有任何其他远程访问功能(例如软件更新、远程培训)?		

表 C.24 网络安全特征配置

序号	问题	回答(是/否/不适用)	备注
1	是否具有根据用户需求配置网络安全特征的能力?		

附 录 D
（资料性）
设备安全台账登记内容参考

设备安全台账登记内容包含但不限于以下关键信息：

a） 医疗设备组网设备清单：组网设备名称、型号、SN、协议、用途等；
b） 医疗设备联网信息记录：所属网域、VLAN、端口、IP地址、MAC地址；
c） 账号清单：账号类别、使用者、口令类别、强度及权限范围；
d） 是否具有远程组件和端口，远程设备类别、型号、保管人；
e） 软件物料清单(SBOM)：软件名称、版本号、补丁；
f） 数据存储介质清单：介质类别、容量、压缩方式、扩展方式；
g） 数据清单：数据的种类、分级、内容、来源、字段名称、存储路径(如文件系统、数据库名称等)、是否敏感数据、读取权限、用途等；
h） 接口清单：对接系统名称、传输方式、传输数据。

附 录 E
（规范性）
联网医疗设备网络安全风险管理

E.1 风险分析与评估

E.1.1 风险分析方法

E.1.1.1 资产识别

梳理联网医疗设备清单，结合访谈、文档查阅、现场查验、技术扫描等方式，明确设备资产及数据资产。

E.1.1.2 威胁分析

全面评估联网医疗设备内外部威胁。内部威胁如未知信息资产、操作失误、违规访问、恶意行为等，外部威胁如网络攻击（黑客攻击、恶意软件入侵、分布式拒绝服务攻击等）、数据泄露（因漏洞导致的信息被窃取）。

E.1.1.3 脆弱性识别

检测和识别联网医疗设备网络基础设施、软件应用、安全策略与流程中的漏洞、应用程序脆弱性、网络配置错误，以及安全管理机制的不完善之处等。

E.1.2 风险评估方法

依据风险分析梳理的资产、威胁与脆弱性等内容形成风险清单，采取适当的方法与工具确定安全事件发生的可能性，综合判断安全事件可能造成的侵害范围和侵害程度，评定风险的高、中、低级别，形成风险评估报告，识别不可接受的风险纳入风险管控。

E.1.3 分析评估节点

宜在如下节点开展风险分析评估：

a） 在新购置、新引入、更新或升级联网医疗设备前；
b） 在用设备与信息系统集成及接口发生变更时；
c） 发生重大网络安全事件后；
d） 定期（如每年）评估联网医疗设备的网络安全风险；
e） 国家及监管部门发布联网医疗设备风险指导意见时，进行针对性排查；
f） 定期（如每月、每季度）收集联网医疗设备网络安全风险态势与漏洞通报，开展专项排查。

注：在不同的分析评估节点，所需要分析评估的内容和侧重点可能不同。

E.2 风险管控

E.2.1 医疗机构应根据设备特性和风险评估报告，对于不可接受的风险制定针对性的防控措施。技术方面，可采取部署防火墙、VPN、堡垒机等措施，建立网络隔离、安全监控与预警机制。管理方面，可以在医疗设备采购合同或维保合同中增加安全网络条款等，以降低风险带来的影响。

E.2.2 将联网医疗设备网络安全应急管理纳入医疗机构网络安全应急响应体系，完善应急预案。

——对联网医疗设备网络安全事件进行分类分级。

——制定不同级别类别事件的处置流程，明确各部门职责。

——针对不同级别类别事件制定应急响应技术方案，明确应急资源（如联系人、备机、备件、处置工具等）。

——定期开展应急演练，规范应急演练记录。

——根据法律法规政策、新增资产、业务调整等变化及时修订应急预案。

E.2.3 如落实防控措施后仍存在剩余风险，则应通过审批、记录并定期评估剩余风险并制定风险发生后的处置预案。

附 录 F
（规范性）
网络安全防护与数据安全要求

F.1 网络安全防护要求

F.1.1 安全物理环境

部署在独立机房的联网医疗设备的物理环境安全考虑如下：

a） 对设备机房进行物理安全访问控制（如安装电子门禁系统），设置访问权限，防止未经授权的物理访问；

b） 在设备机房的敏感区域安装视频监控或警报系统。

F.1.2 安全通信网络

联网医疗设备在医疗机构通信网络的安全考虑如下：

a） 根据医疗机构安全域规划，为有关医疗设备划分网络区域，宜分配静态IP地址并与MAC地址绑定；

b） 避免将医疗设备网络区域部署在医疗机构网络边界处，联网医疗设备网络区域与其他网络区域之间采取可靠的技术隔离手段（如防火墙）；

c） 对支持无线方式的移动式联网医疗设备，进行严格网络管控，无线网络接入应设置身份鉴别机制，至少使用WPA2-PSK（统一口令）实现，宜使用WPA2-Enterprise（用户名/口令）实现；

d） 采用校验技术或密码技术保障联网医疗设备通信过程中有完整性保护需求的数据安全；

e） 采用密码技术保证联网医疗设备通信过程中有机密性保护需求的数据安全；

f） 联网医疗设备在接入医疗机构网络时具备可管理的唯一标识，实现联网医疗设备的网络准入控制。

F.1.3 安全区域边界

医疗机构联网医疗设备的区域边界安全考虑如下。

a） 保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信：

——对非授权联网医疗设备联入到内部网络的行为进行检查或限制；

——对内部联网医疗设备非授权联出到外部网络的行为进行检查或限制。

b） 在网络边界或区域之间根据访问控制策略设置访问控制规则，对进出网络的数据流实现基于应用协议和应用内容的访问控制。

c） 宜部署入侵检测设备，发现或阻断网络安全风险行为，入侵检测设备宜支持对医疗专用协议（如DICOM、HL7等）的检测。

d） 在网络边界实现安全审计功能，能够对访问医疗设备的网络安全行为进行审计和分析，能对远程访问的用户行为单独进行行为审计和数据分析。

e） 医院信息系统访问医疗设备遵循最小必要原则，可采用设备接口访问授权控制、设备节点身份验证、防火墙、白名单、用户角色与权限管理等技术措施保障设备访问安全。

f） 部署医疗设备入侵检测系统（IDS），宜支持DICOM、HL7等医疗专用协议的入侵检测。

F.1.4 安全计算环境

联网医疗设备接入医疗机构的计算环境安全考虑包括以下内容。

a) 对登录医疗设备的用户进行身份标识和鉴别，按照统一授权管理原则进行账户管理和权限分配，建立安全身份认证与访问控制机制，包括：
——用户实名登录，不得使用无法追溯到个人的通用账号；
——需修改默认账户的初始口令，确保口令具有一定复杂度，宜采用基于密码技术的强身份鉴别；
——宜针对不同安全等级的设备采用不同安全强度的身份鉴别方式（如口令、基于密码技术、多因素等）高安全等级的设备宜采用多因素身份鉴别，其中至少一种基于密码技术实现；
——具有登录失败处理功能；
——按照授权分配，对注册用户合理分配账户和权限。
b) 限制与医疗设备预期用途无关网络端口、服务和协议的使用，并对设备端口、服务和协议等网络行为进行网络安全管控。
c) 在不影响医疗业务正常开展的条件下，选择适当技术对联网医疗设备进行安全加固。
d) 启用安全审计功能，对重要的用户行为和重要安全事件进行审计。
e) 需要数据加密保护的，使用的密码技术应符合国家密码管理相关要求。

F.1.5 安全管理中心

医疗机构根据联网医疗设备的网络安全管理需求和整体的网络安全规划，采取共享或独立的联网医疗设备网络安全管理中心进行设备的网络安全管理，安全考虑如下。

a) 实现对网络运行、网络边界、安全，准入等活动进行统一管理，实现边界防护、协议管控、设备准入、资产分域、网络运维日志审计等管理功能。
b) 未经授权不得通过互联网远程连接到医疗设备进行远程监控及维护维修。如确需开展，申请批准后，采取有效的运维管控措施，对联网医疗设备远程接入进行管控，实现账号管理、认证授权、监控和审计功能；未经审批授权不得通过互联网传输医疗设备产生的医疗数据。
c) 对设备产生的网络安全事件进行集中收集与管理，对网络异常行为进行分析及快速定位。
d) 收集汇总并集中分析各个联网医疗设备的活动日志，包括系统日志、操作日志、通信日志、审计日志和安全日志等，日志保留6个月以上。
e) 联网设备宜使用统一时间源。

F.2 数据安全与个人信息保护要求

F.2.1 数据安全保护

联网医疗设备在医疗机构中收集与产生、存储、传输、使用与共享等医疗设备数据全生命周期管理过程中，数据安全保护的安全考虑如下。

a) 按GB/T 43697，根据医疗设备数据在医疗机构业务应用中的重要程度，以及一旦遭到篡改、损毁、泄露或者非法获取、非法使用，对医疗机构、个人、以及相关组织合法权益造成的危害与风险程度，对医疗设备数据进行分类分级管理。
b) 针对不同风险级别的医疗设备数据，在数据全生命周期各个环节，根据实际情况采取相应的数据保护技术措施，包括但不限于身份鉴别技术、访问控制技术、数据加密技术、去标识化技术、匿名化技术、设备安全加固技术、网络管控技术、访问设备用户（包括访问设备的人员、连接设备的系统等）管控技术、日志审计技术等技术与手段：
——在数据收集和产生环节，宜采用身份鉴别、访问控制、网络管控等技术与手段，防止设备配置参数数据、设备运行状态记录及医疗记录数据的假冒和伪造，确保采集数据的真实性和完整性；
——在数据存储环节，宜采用数据加密、数据备份等技术与手段进行数据保护；

——在数据使用环节，宜采用身份鉴别、访问控制（如基于身份/基于属性的访问控制）等保护措施实现数据的授权访问与使用，可采用密码技术、机密计算等技术手段提供数据使用过程中的机密性保护；

——在数据传输环节，宜采用密码技术（如TLCP、TLS）实现传输过程中数据机密性与完整性保护；

——在数据共享环节，对非医疗用途（如科研、教学等）的数据共享，符合最小必要原则，申请审批通过后，宜采用授权管理、去标识化、数据加密等技术实现安全共享；

——在数据销毁环节，对于符合规定且经审批可以销毁的数据，应用采用不可恢复原始数据的方式对数据执行销毁操作，数据销毁具体方式可参考9.4.2.3。

c） 在数据全生命周期各个环节，加强数据处理的日志记录和行为审计，可对数据处理的时间、处理者、类型、数量、频度、流向等进行记录。

F.2.2 个人信息保护

按照GB/T 35273要求开展个人信息保护工作，确保联网医疗设备收集信息限定在合理且必要的最小范围，个人信息保护受限可控：

a） 敏感个人信息宜采用加密、访问控制等技术手段保证个人信息的安全；

b） 敏感个人信息用于非医疗用途（如科研、教学等），宜采用必要手段对数据进行去标识化或匿名化处理。

附 录 G
（资料性）
联网医疗设备安装验收相关评估样表

G.1 联网医疗设备安装网络安全资源确认

联网医疗设备安装网络安全资源确认见表G.1。

表G.1 联网医疗设备安装网络安全资源确认表

使用科室		设备名称	
设备品牌		设备型号	
工作环节	工作内容	完成情况	备注
网络和接口资源	网络布局	是□ 否□ 不适用□	
	虚拟子网	是□ 否□ 不适用□	
	IP地址数量	是□ 否□ 不适用□	
	端口数量及协议	是□ 否□ 不适用□	
	远程访问需求	是□ 否□ 不适用□	
	数据接口	是□ 否□ 不适用□	
	其他网络和接口资源（请在备注中列明）	是□ 否□ 不适用□	
计算资源	服务器	是□ 否□ 不适用□	
	存储	是□ 否□ 不适用□	
物理安全	机房安全	是□ 否□ 不适用□	
	访问控制	是□ 否□ 不适用□	
	监控安装	是□ 否□ 不适用□	
	其他（请在备注中列明）	是□ 否□ 不适用□	
其他			
人员及联系方式			

G.2 网络安全培训记录

网络安全培训记录表见表G.2。

表G.2 医疗设备网络安全培训记录表

使用科室：	
培训教师：厂家专业人员、医疗设备管理部门人员、信息管理部门人员	
监督科室：医疗设备管理部门、信息管理部门、运营部门	
设备名称：	设备数量：
设备品牌与产地：	设备型号/序列号：
培训地点：	培训时间：
培训内容(包括但不限于以下项目)： 1.医疗设备网络安全相关功能概述(厂家) □具备电子数据交换 □远程访问与控制 □用户访问 2.医疗设备网络安全设置操作方法与流程(厂家) 3.医疗设备网络安全维护方法与巡查要点(厂家) 4.医疗设备网络安全的注意事项与风险点(厂家) 5.医疗设备网络安全常见故障与处理方法(厂家) 6.医疗设备网络安全事件应急响应与处置方案(医疗设备管理部门、信息管理部门) 7.出入医疗设备机房的安全管理(医疗设备管理部门) (包括但不限于人员身份识别，出入信息登记、工作事项登记，可查询追溯等) 8.数据管理规范(医疗设备管理部门、信息管理部门) 9.其他	
培训教师反馈： 参加培训人员掌握情况：□熟练掌握 □基本掌握 □未掌握，需再次培训 单位名称： 培训教师(手签)： 联系方式：	
参加培训人员签到 使用科室： 医工部门： 信息管理部门： 其他：	

G.3 联网医疗设备网络安全验收

联网医疗设备网络安全验收表(内容)见表G.3。

表G.3 联网医疗设备网络安全验收表(内容)

设备基本信息	
设备名称：	设备数量：
安装位置(批量设备可另行设表)：	
…(医疗机构根据验收需要另行设表)	
设备网络信息安全管控评估： 1.设备唯一标识验证(序列号、注册证号、合格证) □通过 □不通过 □不适用 2.数据来源可追溯(医疗机构内网传输) □通过 □不通过 □不适用 3.口令安全性评估(口令的唯一性、复杂度和时效性) □通过 □不通过 □不适用 4.风险发现评估(安全漏洞可查、高危漏洞清零、设备日志可分析) □通过 □不通过 □不适用 5.安全防护评估(有无安全补丁、防火墙、杀毒软件等) □通过 □不通过 □不适用 6.网络配置(网络安全策略,网络分段等) □通过 □不通过 □不适用 7.权限配置(职责分离、最小权限等) □通过 □不通过 □不适用 8.端口管理(关闭非必要端口等) □通过 □不通过 □不适用 9.安全策略(超时锁定,开启审计日志,访问权限控制等) □通过 □不通过 □不适用 10.数据备份(数据备份策略,验证等) □通过 □不通过 □不适用 11.安全台账 □通过 □不通过 □不适用 12.培训记录 □通过 □不通过 □不适用 13.运维方案(含远程运维) □是 □否 □不适用 14.应急保障方案 □是 □否 □不适用 15.其他	

参 考 文 献

[1] GB/T 20984—2022 信息安全技术 信息安全风险评估方法

[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

[3] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

[4] GB/T 25068.1—2020 信息技术 安全技术 网络安全 第1部分:综述和概念

[5] GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

[6] 医疗卫生机构网络安全管理办法(国卫规划发〔2022〕29号)

[7] 医疗器械软件注册审查指导原则(2022年修订版)[国家药监局(2022年第9号)]

[8] 医疗器械网络安全注册审查指导原则(2022年修订版)[国家药监局(2022年第7号)]

[9] 公立医院高质量发展促进行动(2021—2025年)(国卫医发〔2021〕27号)

[10] 医疗器械临床使用管理办法(国家卫生健康委员会令第8号)

[11] 医疗器械分类目录[国家药监局(2017年第104号)]

[12] 信息安全等级保护管理办法(公通字〔2007〕43号)

[13] 医疗器械使用质量监督管理办法(国家食品药品监督管理总局令〔2015〕第18号)

[14] 数据出境安全评估办法(国家互联网信息办公室令第11号)

[15] 网络安全审查办法(国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局令第8号)

[16] 郭扬帆,魏书山.医院网络安全建设指引[M].广州:暨南大学出版社,2019.

[17] ISO 14971:2019 医疗设备 风险管理在医疗设备中的应用

[18] UL 2900系列 网络产品的软件网络安全

中国医学装备协会
团 体 标 准
医疗机构联网医疗设备网络安全指南
T/CAME 82—2026

•

中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲2号(100029)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
北京联兴盛业印刷股份有限公司印刷
各地新华书店经销

•

开本 880×1230 1/16 印张 2.25 字数 48 千字
2026年1月第1版 2026年1月第1次印刷

•

书号:155066·5-19821 定价 59.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107

T/CAME 82-2026