附件

医疗器械网络安全注册审查指导原则
(2022年修订版)

本指导原则旨在指导注册申请人规范医疗器械网络安全生存周期过程和准备医疗器械网络安全注册申报资料，同时规范医疗器械网络安全的技术审评要求，为医疗器械软件、质量管理软件的体系核查提供参考。

本指导原则是对医疗器械网络安全的一般要求，注册申请人需根据产品特性和风险程度确定本指导原则具体内容的适用性，若不适用详述理由。注册申请人也可采用其他满足法规要求的替代方法，但需提供详尽的研究资料。

本指导原则是在现行法规、强制性标准体系以及当前科技能力、认知水平下制定的，随着法规、强制性标准体系的不断完善以及科技能力、认知水平的不断发展，本指导原则相关内容也将适时调整。

本指导原则作为注册申请人、审评人员和检查人员的指导性文件，不包括审评审批所涉及的行政事项，亦不作为法规强制执行，应在符合法规要求的前提下使用本指导原则。

本指导原则是数字医疗（Digital Health）指导原则体系的重要组成部分，亦是医疗器械软件指导原则的补充，采用和遵循医疗器械软件、独立软件生产质量现场检查等相关指导原则的

概念和要求。

本指导原则是医疗器械网络安全的通用指导原则，其他涉及网络安全的医疗器械产品指导原则可在本指导原则基础上进行有针对性的调整、修改和完善。

一、适用范围

本指导原则适用于医疗器械网络安全的注册申报，包括具备电子数据交换、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（包括体外诊断医疗器械）；适用于自研软件、现成软件的注册申报。

其中，网络包括无线、有线网络，电子数据交换包括基于网络、存储媒介的单向、双向数据传输，远程访问与控制包括基于网络的实时、非实时的访问与控制，用户（如医务人员、患者、维护人员等）访问包括基于软件用户界面、电子接口的人机交互方式。

本指导原则也可用作医疗器械软件、质量管理软件的体系核查参考。

二、主要概念

（一）医疗器械网络安全

医疗器械网络安全是指保护医疗器械产品自身和相关数据不受未授权活动影响的状态，其保密性（Confidentiality）、完整性（Integrity）、可得性（Availability）[1]相关风险在全生命周期

[1]在信息安全领域 availability 译为可用性，而在医疗器械领域 usability 译为可用性，为避免引起歧义本指导原则将 availability 译为可得性。

均处于可接受水平[2]。

其中，保密性是指信息不被未授权实体（含产品、服务、个人、组织）获得或知悉的特性，即医疗器械产品自身和相关数据仅可由授权用户在授权时间以授权方式进行访问和使用。完整性是指信息的创建、传输、存储、显示未以非授权方式进行更改（含删除、添加）的特性，即医疗器械相关数据是准确和完整的，且未被篡改。可得性是指信息可根据授权实体要求进行访问和使用的特性，即医疗器械产品自身和相关数据能以预期方式适时进行访问和使用。

除保密性、完整性、可得性三个基本特性外，医疗器械网络安全还包括真实性（Authenticity）、抗抵赖性（Non-Repudiation）、可核查性（Accountability）、可靠性（Reliability）等特性。其中，真实性是指实体符合其所声称的特性，抗抵赖性是指实体可证明所声称事件或活动的发生及其发起实体的特性，可核查性是指实体的活动及结果可被追溯的特性，可靠性是指实体的活动及结果与预期保持一致的特性。

保密性、完整性、可得性等网络安全特性通常是相互制约的关系，在同等条件下，某一特性的能力提升可能会使得另一特性或多个特性的能力下降，如可得性的提升可能会降低保密性和完整性，因此需要基于产品特性进行平衡兼顾。注册申请人需结合医疗器械的预期用途、使用场景、核心功能进行综合考量，从而确定医疗器械网络安全特性的具体要求。

[2]详见 IMDRF/CYBER WG/N60FINAL:2020。

此外，尽管信息安全、网络安全、数据安全的定义和范围各有侧重，既有联系又有区别，不尽相同，但本指导原则从医疗器械安全有效性评价角度出发对三者不做严格区分，统一采用网络安全进行表述，即从网络安全角度综合考虑医疗器械的信息安全和数据安全。

（二）医疗器械相关数据

医疗器械相关数据可分为医疗数据和设备数据。

医疗数据是指医疗器械所产生的、使用的与医疗活动相关的数据(含日志),从个人信息保护角度又可分为敏感医疗数据、非敏感医疗数据，其中敏感医疗数据是指含有个人信息的医疗数据[3]，反之即为非敏感医疗数据。个人信息是指以电子或者其他方式记录的能够单独或与其他信息结合识别自然人个人身份的各种信息，如自然人的姓名、出生日期、身份证件号码、个人生物识别信息（含容貌信息）、住址、电话号码等。

设备数据是指记录医疗器械运行状况的数据（含日志），用于监视、控制医疗器械运行或者医疗器械的维护与升级，不得含有个人信息。

注册申请人需基于医疗器械相关数据的类型、功能、用途，结合网络安全特性考虑医疗器械网络安全要求。同时，保证敏感医疗数据所含个人信息免于泄露、滥用和篡改，以及医疗数据和设备数据的有效隔离（如访问权限控制等方法）。

（三）医疗器械电子接口

[3]敏感医疗数据属于 IEC 80001 所定义的健康数据（Health data）。

本指导原则所述医疗器械电子接口（含硬件接口、软件接口）包括网络接口、电子数据交换接口，若无明示均指外部接口，分体式医疗器械各独立部分的内部接口视为外部接口，如服务器与客户端、主机与从机的内部接口。

1.网络接口

网络接口是指基于网络的电子接口。医疗器械可通过网络接口（含转接接口）进行电子数据交换或远程访问与控制，此时需考虑网络的技术特征要求，包括但不限于网络形式（有线、无线）、网络类型（如广域网、局域网、个域网）、接口形式（如电口、光口）、数据接口（此时即数据协议，含标准协议、私有协议）、远程访问与控制方式（实时、非实时）、性能指标（如端口、传输速率、带宽）等。

无线网络包括 Wi-Fi（IEEE 802.11）、蓝牙（IEEE 802.15）、射频、红外、4G/5G 等形式，其中医用无线专用设备（即未采用通用无线通信技术的医疗器械）应符合中国无线电管理相关规定。标准协议即业内公认标准所规范的数据传输协议，如 DICOM、HL7 等，需考虑其定制化功能的兼容性问题；私有协议需考虑兼容性问题。远程访问与控制亦包括操作系统软件所提供的远程会话或远程桌面功能。

2.电子数据交换接口

电子数据交换接口是指基于非网络的电子接口。医疗器械可通过非网络接口的其他电子接口（如串口、并口、USB 口、视频接口、音频接口，含调试接口、转接接口）或存储媒介（如

光盘、移动硬盘、U 盘）进行电子数据交换。此时需考虑其他电子接口或数据存储的技术特征要求。

其他电子接口可参照网络接口明确其技术特征要求。数据存储的技术特征要求包括但不限于存储媒介形式、数据接口（此时即文件存储格式，含标准格式、私有格式）、数据压缩方式（有损、无损）、性能指标（如传输速率、容量）等。标准格式即业内公认标准所规范的文件存储格式，如 JPEG、PNG 等，需考虑其文件格式完整性问题；私有格式需考虑兼容性问题。

注册申请人需结合医疗器械电子接口的类型、方式、技术特征，基于网络安全特性考虑其网络安全的具体要求。

（四）医疗器械网络安全能力

考虑到预期用途、使用场景的限制，医疗器械对于网络安全威胁应具备必要的识别、保护能力和适当的探测、响应、恢复能力。

本指导原则所述医疗器械网络安全能力包括：

1.自动注销（ALOF）：产品在无人值守期间阻止非授权用户访问和使用的能力。

2.审核（AUDT）：产品提供用户活动可被审核的能力。

3.授权（AUTH）：产品确定用户已获授权的能力。

4.节点鉴别（NAUT）：产品鉴别网络节点的能力。

5.人员鉴别（PAUT）：产品鉴别授权用户的能力。

6.连通性（CONN）：产品保证连通网络安全可控的能力。

7.物理防护（PLOK）：产品提供防止非授权用户访问和使

用的物理防护措施的能力。

8.系统加固（SAHD）：产品通过固化措施对网络攻击和恶意软件的抵御能力。

9.数据去标识化与匿名化（DIDT）：产品直接去除、匿名化数据所含个人信息的能力。

10.数据完整性与真实性（IGAU）：产品确保数据未以非授权方式更改且来自创建者或提供者的能力。

11.数据备份与灾难恢复（DTBK）：产品的数据、硬件或软件受到损坏或破坏后恢复的能力。

12.数据存储保密性与完整性（STCF）：产品确保未授权访问不会损坏存储媒介所存数据保密性和完整性的能力。

13.数据传输保密性（TXCF）：产品确保数据传输保密性的能力。

14.数据传输完整性（TXIG）：产品确保数据传输完整性的能力。

15.网络安全补丁升级（CSUP）：授权用户安装/升级产品网络安全补丁的能力。

16.现成软件清单（SBOM）：产品为用户提供全部现成软件清单的能力。

17.现成软件维护（RDMP）：产品在全生命周期中对现成软件提供网络安全维护的能力。

18.网络安全使用指导（SGUD）：产品为用户提供网络安全使用指导的能力。

19.网络安全特征配置（CNFS）：产品根据用户需求配置网络安全特征的能力。

20.紧急访问（EMRG）：产品在预期紧急情况下允许用户访问和使用的能力。

21.远程访问与控制（RMOT）：产品确保用户远程访问与控制（含远程维护与升级）的网络安全的能力。

22.恶意软件探测与防护（MLDP）：产品有效探测、阻止恶意软件的能力。

注册申请人需根据医疗器械的产品特性分析上述网络安全能力的适用性。若适用，明确网络安全能力的实现方式，可通过产品自身功能实现，亦可通过必备软件、外部软件环境等外部措施实现。同时，根据产品风险水平明确网络安全能力的强弱程度，例如：用户访问控制可采用用户名和口令方式，其中口令强度可采用不同强度设置或采用动态口令，亦可采用生物识别技术，通常情况下医疗器械的风险水平越高则其用户访问控制要求越严格。反之，若不适用详述理由并予以记录。

值得注意的是，对于特定医疗器械产品，上述各项网络安全能力可能不足以保证其网络安全，需结合产品具体情况补充其他网络安全能力要求。

（五）网络安全验证与确认

网络安全验证与确认作为软件验证与确认的重要组成部分，需在软件验证与确认的框架下，结合产品网络安全特性开展相关质控工作，如源代码安全审核、威胁建模、漏洞扫描、渗透

测试、模糊测试等。软件验证与确认相关要求详见医疗器械软件指导原则第二章。

注册申请人需针对不同类型网络威胁，采用相应技术手段来保证医疗器械的网络安全。例如：针对读取攻击、操作攻击、欺骗攻击、泛洪攻击、重定向、勒索攻击等网络威胁，可采用用户访问控制、端口与服务关闭、加密、数字签名、标准协议、校验、防火墙、入侵检测、恶意代码防护、防护规则配置等方法与技术来保证产品的网络安全。

（六）网络安全可追溯性分析

网络安全可追溯性分析作为网络安全验证与确认的重要活动之一，是指追踪网络安全需求、网络安全设计、源代码、网络安全测试、网络安全风险管理之间的关系，分析已识别关系的正确性、一致性、完整性、准确性。

医疗器械网络安全生存周期过程均应开展网络安全可追溯性分析活动，具体要求可参照软件可追溯性分析活动要求，详见医疗器械软件指导原则第二章。

（七）网络安全事件应急响应

医疗器械设计开发只能针对已知网络安全漏洞采取相应风险控制措施，上市后仍会面临潜在未知的网络安全漏洞引发的网络安全事件的威胁，可能造成医疗器械无法访问和使用、医疗数据发生泄露或遭到篡改，进而可能导致患者受到伤害或死亡以及隐私被侵犯。同时，医疗器械网络安全事件具有影响因素多、涉及面广、扩散性强和突发性高等特点，对于医疗器械

上市后监测要求相对较高。因此，注册申请人需基于相关标准和技术报告建立网络安全事件应急响应机制，保证医疗器械的安全有效性并保护患者隐私。

应制定网络安全事件应急响应预案，涵盖现成软件要求，明确计划与准备、探测与报告、评估与决策、应急响应实施、总结与改进等阶段的任务和要求。建立网络安全事件应急响应团队，根据工作职能形成管理、规划、监测、响应、实施、分析等工作小组，必要时可邀请外部网络安全专家成立专家小组。

根据网络安全事件的严重程度、紧迫程度、广泛程度等因素进行分类分级管理，结合产品风险级别，按照风险管理要求开展应急响应措施的验证工作并予以记录，在事件发生期间及时告知用户应对措施。若适用，按照医疗器械不良事件、召回相关法规要求处理；必要时，向国家网络安全主管部门报告。

（八）医疗器械网络安全更新

1.网络安全更新

医疗器械网络安全更新从内容上可分为功能更新、补丁更新，类似于增强类软件更新、纠正类软件更新。根据其对医疗器械安全性和有效性的影响程度分为以下两类：

（1）重大网络安全更新：影响到医疗器械的安全性或有效性的网络安全更新，即重大网络安全功能更新，应申请变更注册。

（2）轻微网络安全更新：不影响医疗器械的安全性与有效性的网络安全更新，包括轻微网络安全功能更新、网络安全补

丁更新。轻微网络安全更新通过质量管理体系进行控制，无需申请变更注册，待下次变更注册时提交相应注册申报资料。

此外，涉及召回的网络安全更新，无论功能更新还是补丁更新均属于重大网络安全更新，按照医疗器械召回相关法规要求处理，不属于本指导原则讨论范畴。

网络安全更新同样遵循风险从高原则，即同时发生重大和轻微网络安全更新按重大网络安全更新处理。同时，软件版本命名规则应涵盖网络安全更新情况，区分重大和轻微网络安全更新。

2.重大网络安全更新判定原则

网络安全功能更新若影响到医疗器械的预期用途、使用场景或核心功能原则上均属于重大网络安全更新，包括但不限于：产品预期运行的网络环境发生改变，如由封闭网络环境变为开放网络环境、局域网变为广域网、有线网络变为无线网络；产品预期使用的电子接口发生改变，如接口形式由网口变为USB口、接口类型由少变多、接口功能由电子数据交换扩至远程控制；产品网络安全能力发生实质性改变，如自动注销能力由操作系统自带功能实现改为产品自身功能实现、物理防护能力由有变无等。

除非影响到医疗器械的安全性或有效性，以下网络安全功能更新和网络安全补丁更新通常视为轻微网络安全更新：产品预期运行的网络环境数据传输效率单纯提高，预期使用的电子接口原有功能单纯优化、传输效率单纯提高，产品网络安全能

力发生非实质性改变；医疗器械软件、必备软件、外部软件环境的网络安全补丁更新。其中，必备软件是指医疗器械软件正常运行所必需的其他医疗器械软件及医用中间件，外部软件环境是指医疗器械软件正常运行所必需的系统软件、通用应用软件、通用中间件、支持软件，详见医疗器械软件指导原则。

三、基本原则

（一）网络安全定位

随着网络技术的发展，越来越多的医疗器械具备网络连接功能以进行电子数据交换或远程访问与控制，在提高医疗服务质量与效率的同时也面临着网络攻击的威胁。医疗器械网络安全出现问题不仅可能会侵犯患者隐私，而且可能会产生医疗器械非预期运行的风险，导致患者或用户受到伤害或死亡。因此，医疗器械网络安全是医疗器械安全性和有效性的重要组成部分之一。

信息共享是保障医疗器械网络安全的基本原则[4]。及时获得网络安全漏洞、事件等相关信息有助于识别、评估和应对网络安全风险，保证医疗器械的安全有效性以及医疗活动的业务持续性，因此，鼓励所有利益相关方在医疗器械全生命周期中主动积极共享网络安全相关信息。注册申请人需充分利用网络安全漏洞披露机制加强医疗器械网络安全的设计开发和上市后监测，如基于国家互联网应急中心（CNCERT/CC，www.cert.org.cn）的国家信息安全漏洞共享平台（CNVD，www.cnvd.org.cn），或

[4]详见 IMDRF/CYBER WG/N60FINAL:2020。

其互认的国际信息安全漏洞库所披露的漏洞信息，定期开展网络安全风险管理工作。

医疗器械网络安全需要注册申请人、用户、信息技术服务商等利益相关者的共同努力和通力合作方能得以保障。虽然医疗器械在使用过程中常与非预期的设备或系统相连，使得注册申请人在保证医疗器械网络安全方面存在诸多困难，但这不意味注册申请人可以免除医疗器械网络安全相关责任。注册申请人需保证医疗器械产品自身的网络安全，明确预期的网络环境和电子接口要求，持续监测、评估、应对、分享网络安全相关风险，与其他利益相关者密切合作，从而保证医疗器械的安全有效性。

医疗器械网络安全也是网络安全国家战略的重要组成部分，因此医疗器械网络安全亦应符合网络安全相关法律法规和部门规章的要求，如网络安全法、数据安全法、个人信息保护法以及数据出境、重要数据识别等要求。注册申请人应持续跟踪相关法律法规和部门规章的制修订情况，并满足相应适用要求。

网络安全新技术（如人工智能技术）研究处于快速发展阶段，医疗器械若采用网络安全新技术来保证网络安全，亦需基于新技术特性，并结合风险管理开展相应验证与确认工作。

（二）风险导向

综合考虑行业发展水平和风险分级管理导向，医疗器械网络安全的风险级别不同，其生命周期质控要求和注册申报资料要求亦不同。

虽然网络安全风险与软件风险存在差异，但是网络安全风险作为软件风险的重要组成部分，其风险级别亦可参照软件采用安全性级别进行表述[5]。在通常情形下，医疗器械网络安全的安全性级别与所属医疗器械软件的安全性级别相同；在特殊情形下，网络安全的安全性级别可低于软件的安全性级别，此时需详述理由并按网络安全的安全性级别提交相应注册申报资料。

医疗器械网络安全风险同样结合医疗器械的预期用途、使用场景、核心功能进行综合判定，特别是使用场景。不同使用场景的网络环境不同，甚至存在巨大差异，对于医疗器械网络安全的影响亦不同，如门诊、手术、住院、急救、家庭、转运、公共场所等使用场景的网络环境均有所不同，因此对于适用于多个使用场景的医疗器械，注册申请人需保证医疗器械在每个使用场景的网络安全。

医疗器械网络安全风险管理活动通常包括：识别资产（Asset，对个人或组织有价值的物理和数字实体）、威胁（Threat，可能导致对个人或组织产生损害的非预期事件发生的潜在原因）和脆弱性（Vulnerability，可能会被威胁所利用的资产或风险控制措施的弱点），评估威胁和脆弱性对于医疗器械和患者的影响以及被利用的可能性，确定风险水平并采取充分、有效、适宜的风险控制措施，基于风险接受准则评估网络安全综合剩余风险，保证网络安全综合剩余风险均处于可接受水平。

注册申请人可结合医疗器械风险管理和网络安全风险管理

[5]详见医疗器械软件指导原则关于软件安全性级别的说明。

相关标准和技术报告的要求，开展医疗器械网络安全风险管理工作。值得注意的是，医疗器械风险管理与网络安全风险管理在传统上存在一定差异，注册申请人若无法对二者进行有效整合，则需分别独立开展相应风险管理活动并予以记录，同时考虑不同类型风险控制措施的相互影响问题。

（三）全生命周期质控

与医疗器械软件类似，注册申请人应在医疗器械全生命周期中持续关注网络安全问题，包括上市前、上市后等阶段。

医疗器械上市前结合质量管理体系要求和医疗器械产品特性开展网络安全质控工作，保证医疗器械的安全有效性；上市后根据网络安全更新情况开展更新请求评估、验证与确认、风险管理、用户告知等活动，持续保证医疗器械的安全有效性。同时，建立网络安全事件应急响应过程，定期开展医疗器械网络安全漏洞风险评估工作，根据网络安全漏洞披露相关要求，及时将必要的网络安全相关信息以及应对措施告知用户。此外，可采用信息安全领域的良好工程实践[6]来完善医疗器械网络安全质控工作，以保证医疗器械的安全有效性。

四、医疗器械网络安全生存周期过程

考虑到行业实际情况，本指导原则不要求注册申请人单独建立医疗器械网络安全生存周期（又称生命周期）过程，而是将其作为医疗器械软件生存周期过程的重要组成部分予以整体考虑，待时机成熟时予以考量。

---

[6]在信息安全领域，IEC 27000 系列标准规范信息安全管理体系（ISMS）认证要求，本指导原则不要求注册申请人进行 ISMS 认证，但建议参考相关标准要求。

注册申请人需在医疗器械软件生存周期过程考虑医疗器械网络安全的质控要求，并可基于医疗器械网络安全能力建设要求予以实施，具体要求详见医疗器械软件指导原则第六章以及独立软件生产质量管理规范及其现场检查指导原则。

同时，注册申请人可参考信息安全领域相关标准和技术报告，完善医疗器械网络安全生存周期过程的质控要求，本指导原则不再赘述。

五、技术考量

（一）现成软件

现成软件同样存在网络安全问题，注册申请人应根据质量管理体系要求建立现成软件网络安全更新过程，结合风险管理要求，及时将必要的现成软件网络安全信息及应对措施告知用户。

同时，根据现成软件与医疗器械软件的关系类型开展相应网络安全质控工作。对于现成软件组件（即作为医疗器械软件组成部分的现成软件），重点关注其网络安全问题对医疗器械使用效果的影响，网络安全的安全性级别判定亦需将其纳入考量。对于外部软件环境（即作为医疗器械软件运行环境组成部分的现成软件），重点关注其网络安全补丁对医疗器械安全有效性的影响，网络安全的安全性级别判定通常无需将其纳入考量；需要说明的是，网络安全补丁对于医疗器械而言属于设计变更，需对医疗器械进行验证、确认。

（二）医疗数据出境

根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国人类遗传资源管理条例》等法律法规相关规定，在中国境内收集和产生的重要数据、个人信息和人类遗传资源信息原则上应在中国境内存储，因业务需要确需向境外提供的，应按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

《国家健康医疗大数据标准、安全和服务管理办法(试行)》明确：健康医疗大数据应存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应按照相关法律法规及有关要求进行安全评估审核。

医疗数据通常属于重要数据[7]，特别是敏感医疗数据含有个人信息，因此医疗数据出境应符合重要数据、个人信息、人类遗传资源信息出境安全评估相关规定。

（三）远程维护与升级

远程维护与升级虽为非医疗器械功能，但会影响医疗器械的安全有效性，故亦需纳入考量。

具有远程维护与升级功能的医疗器械可访问和使用设备数据，本身虽不涉及医疗数据，但若未能实现设备数据和医疗数据的有效隔离，则存在医疗数据未授权访问和使用以及被篡改的可能性。远程维护与升级所用电子接口也面临网络攻击的威胁，可能会影响医疗器械正常运行，导致患者受到伤害或死亡以及隐私被侵犯。医疗器械在远程维护与升级过程中若无人值

[7]根据国家标准《信息安全技术 重要数据识别指南》进行判定。

守，则可能存在医疗器械非授权访问和使用的风险。家用医疗器械的远程维护与升级需考虑其对产品正常使用的影响及其风险。

因此，注册申请人需明确远程维护与升级的实现方法、所用电子接口情况、设备数据所含内容、设备数据与医疗数据的隔离方法、网络安全保证措施等技术特征，并提供相应研究资料和风险管理资料。

此外，境外远程维护与升级若可访问医疗数据，亦应符合医疗数据出境要求。

（四）遗留设备[8]

本指导原则所述遗留设备是指不能通过补丁更新、补偿控制等合理风险控制措施抵御当前网络安全威胁的医疗器械。遗留设备可能无法应对当前网络安全威胁，导致产品综合剩余风险无法降至可接受水平，降低医疗器械的安全有效性。

医疗器械实际使用情况极为复杂，使得遗留设备的判定较为困难。通常情况下可结合医疗器械的停售（EOL）、停止售后服务（EOS）两个时间点判定其是否属于遗留设备：在售（以注册证时效为准）的医疗器械均非遗留设备；停售但未停止售后服务的医疗器械，若无法通过合理风险控制措施抵御当前网络安全威胁则为遗留设备，反之不属于遗留设备；停止售后服务的医疗器械均为遗留设备。

对于遗留设备，注册人应按照质量管理体系要求开展相应

[8]详见 IMDRF/CYBER WG/N60FINAL:2020。

质控工作，以保证产品网络安全，详见独立软件生产质量管理规范及其现场检查指导原则。

对于注册证失效但尚未停止售后服务、注册证有效但已停售的医疗器械，注册人应根据质量管理体系要求向现有用户提供必要的网络安全相关信息以及应对措施，以保证医疗器械的网络安全。若无法保证医疗器械的网络安全，按遗留设备处理。

对于注册证有效且在售的医疗器械，若无法通过合理风险控制措施抵御当前网络安全威胁，则注册人应根据质量管理体系要求制定相应风险控制措施，并申请变更注册。

六、医疗器械网络安全研究资料

医疗器械网络安全研究资料框架详见图 1，包括自研软件和现成软件（含现成软件组件、外部软件环境），具体要求如下。

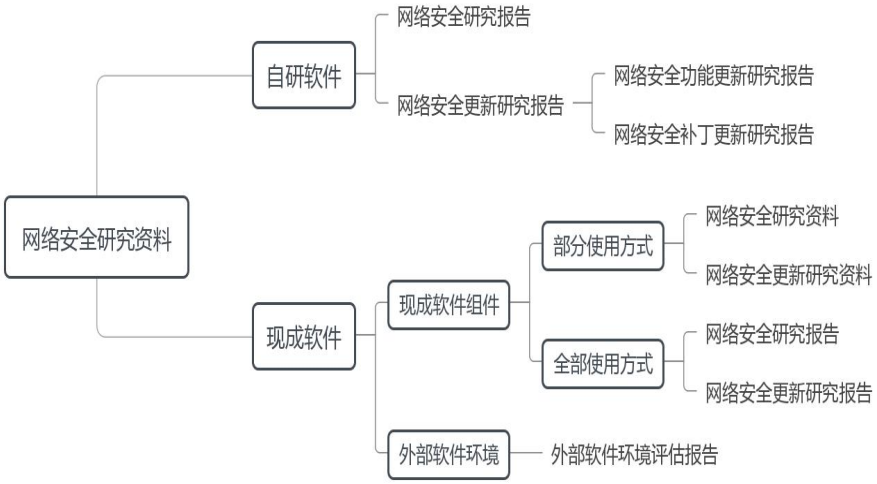

图 1 医疗器械网络安全研究资料框架

（一）自研软件网络安全研究报告

自研软件网络安全研究报告适用于自研软件的初次发布和

再次发布，内容框架详见表1，包括基本信息、实现过程、漏洞评估、结论，详尽程度取决于软件安全性级别，不适用内容详述理由。

1.基本信息

（1）软件信息

明确申报医疗器械软件的名称、型号规格、发布版本以及软件安全性级别。

若网络安全的安全性级别低于软件的安全性级别，详述理由并按网络安全的安全性级别提交相应注册申报资料。

（2）数据架构

提供申报医疗器械在每个使用场景（含远程维护与升级，下同）下的网络环境和数据流图，并依据图示描述医疗器械相关数据和电子接口的基本情况。

数据情况明确医疗器械相关数据的类型（敏感医疗数据、非敏感医疗数据、设备数据），并依据数据类型明确每类数据的具体内容（如个人信息、医疗活动信息、设备运行信息）、功能（如单向、双向电子数据交换，实时、非实时远程访问与控制）、用途（如医疗活动、设备维护）等。

电子接口情况逐项说明每个网络接口、电子数据交换接口的预期用户、使用场景、预期用途、数据类型、技术特征、使用限制，其中技术特征要求详见第二章。

（3）网络安全能力

基于第二章所述各项网络安全能力，逐项分析申报医疗器

械对于该项网络安全能力的适用性，详述适用网络安全能力的实现方法以及不适用理由。若适用，提供其他网络安全能力的适用情况说明。

（4）网络安全补丁

提供申报医疗器械（含必备软件、外部软件环境）的网络安全补丁列表，明确网络安全补丁的名称、完整版本、发布日期。可另附文件。

（5）安全软件

描述申报医疗器械兼容或所用的安全软件（如杀毒软件、防火墙等）的名称、型号规格、完整版本、供应商、运行环境、防护规则配置要求。

2.实现过程

（1）风险管理

提供申报医疗器械网络安全的风险分析报告、风险管理报告，另附网络安全开发所形成的原始文件。亦可提供医疗器械软件的风险管理文档，但需注明网络安全情况。

（2）需求规范

提供申报医疗器械的网络安全需求规范文档，另附网络安全开发所形成的原始文件。亦可提供医疗器械软件的需求规范文档，但需注明网络安全情况。

（3）验证与确认

提供申报医疗器械的网络安全测试计划和报告，另附网络安全开发所形成的原始文件。亦可提供医疗器械软件的系统测

试计划和报告，但需注明网络安全情况。

对于安全软件，提供兼容性测试报告。对于标准传输协议或存储格式，若其满足医疗器械网络安全需求出具真实性声明即可，反之提供相应证明材料；对于私有传输协议或存储格式，提供完整性测试总结报告。对于实时远程访问与控制功能，提供完整性和可得性等网络安全特性的测试报告。对于医用无线专用设备，提供符合无线电管理相关规定的证明材料。

（4）可追溯性分析

提供申报医疗器械的网络安全可追溯性分析报告，汇总列明网络安全需求规范文档、网络安全设计规范文档、源代码（明确软件单元名称即可）、网络安全测试报告、网络安全风险分析报告之间的对应关系。亦可提供医疗器械软件的可追溯性报告，但需注明网络安全情况。

（5）维护计划

轻微级别：提供申报医疗器械网络安全更新的流程图，并依据图示描述相关活动。

中等、严重级别：在轻微级别的基础上，提供网络安全事件应急响应的流程图，并依据图示描述相关活动；或者提供网络安全事件应急响应预案文档。

若适用，全部级别均需提供远程维护与升级的流程图，并依据图示描述相关活动。

3.漏洞评估

轻微级别：按照现行有效的通用漏洞评分系统（CVSS）所

定义的漏洞等级，明确申报医疗器械（含必备软件、外部软件环境，下同）已知漏洞总数和已知剩余漏洞数。

中等级别：提供网络安全漏洞自评报告，明确漏洞扫描所用软件工具、漏洞库（基于国家信息安全漏洞库或互认的国际信息安全漏洞库）的基本信息（如名称、完整版本、发布日期、供应商等），按照 CVSS 漏洞等级明确申报医疗器械已知漏洞总数和已知剩余漏洞数，列明已知剩余漏洞的内容、对产品的影响及综合剩余风险，确保产品综合剩余风险均可接受。亦可补充网络安全评估机构出具的网络安全漏洞评估报告。

严重级别：提供网络安全漏洞自评报告、网络安全评估机构出具的网络安全漏洞评估报告，明确已知剩余漏洞的维护方案，确保产品综合剩余风险均可接受。

4.结论

概述申报医疗器械的网络安全实现过程的规范性和网络安全漏洞评估结果，判定申报医疗器械的网络安全是否满足要求，受益是否大于风险。

表 1 自研软件网络安全研究报告框架

报告条款		软件安全性级别		
		轻微	中等	严重
基本信	软件信息	明确软件的基本情况和安全性级别		
	数据架构	提供每个使用场景的网络环境和数据流图，描述医疗器械相关数据和电子接口的基本情况		

息	网络安全能力	明确网络安全能力情况		
	网络安全补丁	列明网络安全补丁的基本情况		
	安全软件	明确安全软件的基本情况		
实现过程	风险管理	提供网络安全的风险分析报告、风险管理报告		
	需求规范	提供网络安全需求规范文档		
	验证与确认	提供网络安全的测试计划和报告		
	可追溯性分析	提供网络安全可追溯性分析报告		
	维护计划	提供网络安全更新、远程维护与升级的流程图及活动描述	提供网络安全更新、网络安全事件应急响应、远程维护与升级的流程图及活动描述	
漏洞评估		按照漏洞等级明确已知漏洞总数和剩余漏洞数	提供网络安全漏洞自评报告，按照漏洞等级明确已知漏洞总数、已知剩余漏洞情况	提供网络安全漏洞自评报告、网络安全评估机构出具的网络安全漏洞评估报告，明确已知剩余漏洞的维护方案
结论		概述网络安全实现过程的规范性和网络安全漏洞评估结果,判定网络安全是否满足要求		

（二）自研软件网络安全更新研究报告

自研软件网络安全更新研究报告适用于自研软件的再次发布，包括网络安全功能更新、网络安全补丁更新等研究报告。

网络安全功能更新研究报告适用于自研软件发生重大、轻微网络安全功能更新，或合并网络安全补丁更新的情形，内容框架详见表 2，不再赘述。

网络安全补丁更新研究报告适用于自研软件（含必备软件、外部软件环境）仅发生网络安全补丁更新的情形。其内容包括软件信息、网络安全补丁、风险管理、验证与确认、可追溯性分析、维护计划、漏洞评估、结论，具体要求详见表 2 相应说明。

表 2 自研软件网络安全功能更新研究报告框架

报告条款		软件安全性级别		
		轻微	中等	严重
基本信息	软件信息	明确本次申报软件情况，详述变化		
	数据架构	明确本次申报软件情况，详述变化		
	网络安全能力	明确本次申报软件情况，详述变化		
	网络安全补丁	列明网络安全更新部分的补丁情况		
	安全软件	明确本次申报软件情况，详述变化		
实现过程	风险管理	提供网络安全更新部分的风险分析报告、风险管理报告		
	需求规范	提供网络安全更新部分需求规范文档		
	验证与确认	提供网络安全更新部分的测试计划和报告		
	可追溯性分析	提供网络安全更新部分的可追溯性分析报告		
	维护计划	提供用户告知计划	提供用户告知计划、网络安全事件应急响应总结报告	

漏洞评估	明确本次申报软件已知漏洞总数和剩余漏洞数	提供本次申报软件的网络安全自评报告，按照漏洞等级明确已知漏洞总数、已知剩余漏洞情况	提供本次申报软件的网络安全自评报告、网络安全评估机构出具的网络安全漏洞评估报告，明确已知剩余漏洞的维护方案
结论	概述网络安全更新实现过程的规范性和网络安全漏洞评估结果，判定网络安全更新是否满足要求		

考虑到网络安全更新具有累积效应，网络安全更新研究报告需涵盖医疗器械软件自前次注册（延续注册除外）以来网络安全更新的全部内容。

（三）现成软件网络安全研究资料

1. 现成软件组件网络安全研究资料

（1）部分使用方式

对于部分使用方式，即医疗器械软件同时使用自研软件和现成软件组件，无需单独提交网络安全研究报告，基于医疗器械软件的安全性级别，在自研软件网络安全研究报告适用条款中说明现成软件组件的情况。

适用条款包括软件信息、数据架构、网络安全能力、网络安全补丁、风险管理、需求规范、验证与确认、可追溯性分析、维护计划、漏洞评估、结论。

此时若现成软件组件发生网络安全更新，网络安全功能更

新在自研软件网络安全功能更新研究报告的基础上，说明现成软件组件的变化情况，不适用条款说明理由；网络安全补丁更新要求与自研软件相同。

（2）全部使用方式

对于全部使用方式，即医疗器械软件全部为现成软件组件，需要单独提交现成软件组件网络安全研究报告，其内容与自研软件研究报告相同，但需基于现成软件组件（此时即医疗器械软件）的安全性级别予以说明。

此时若现成软件组件发生网络安全更新，网络安全功能更新在现成软件组件网络安全功能更新研究报告的基础上，说明现成软件组件的变化情况，不适用条款说明理由；网络安全补丁更新要求与自研软件相同。

2. 外部软件环境网络安全评估资料

外部软件环境网络安全评估作为外部软件环境评估的重要组成部分，其网络安全及其更新的研究资料要求与外部软件环境评估报告相同，具体要求详见医疗器械软件指导原则第八章。

考虑到医疗器械软件指导原则已明确外部软件环境评估报告要求，同时自研软件网络安全研究资料亦含有外部软件环境的网络安全补丁、漏洞评估等要求，故无需单独提交外部软件环境网络安全评估资料。

七、注册申报资料补充说明[9]

注册申报资料在符合医疗器械注册申报资料要求等文件要

[9]产品技术要求关于网络安全的要求详见医疗器械软件指导原则。

求基础上，满足医疗器械软件等相关指导原则要求，同时重点关注以下要求。

（一）产品注册

1.软件研究资料

在软件研究资料中单独提交自研软件网络安全研究报告。

若使用现成软件组件，根据其使用方式提交相应研究资料。相关研究资料的具体要求详见第六章。

2.说明书

说明书提供网络安全说明和使用指导，明确用户访问控制机制、电子接口（含网络接口、电子数据交换接口）及其数据类型和技术特征、网络安全特征配置、数据备份与灾难恢复、运行环境（含硬件配置、外部软件环境、网络环境，若适用）、安全软件兼容性列表（若适用）、外部软件环境与安全软件更新（若适用）、现成软件清单（SBOM，若适用）等要求。

（二）变更注册

1.软件研究资料

医疗器械变更注册应根据网络安全更新情况，提交变化部分对产品安全性与有效性影响的研究资料：

（1）涉及网络安全功能更新：适用于自研软件发生网络安全功能更新，或合并网络安全补丁更新的情形，此时单独提交一份自研软件网络安全功能更新研究报告（或自研软件网络安全研究报告）；

（2）仅发生网络安全补丁更新：适用于自研软件（含必备

软件、外部软件环境）仅发生网络安全补丁更新的情形，此时单独提交一份自研软件网络安全补丁更新研究报告；

（3）未发生网络安全更新：出具真实性声明，明确对此承担法律责任。

若使用现成软件组件，根据其使用方式提交相应研究资料。相关研究资料的具体要求详见第六章。

2.说明书

若适用，提交说明书关于网络安全内容的变更对比表。

（三）延续注册

延续注册通常无需提交网络安全相关研究资料。若适用，根据注册证“备注”所载明的要求提交相应网络安全研究资料。

产品技术要求“产品型号/规格及其划分说明”所述软件版本命名规则应涵盖网络安全更新情况，区分重大网络安全更新和轻微网络安全更新。若原注册产品标准（或原产品技术要求）及其变更对比表未体现软件相关信息，需在符合性声明中予以明确，其中软件版本命名规则需涵盖网络安全更新情况。

八、参考文献

[1] 全国人大. 中华人民共和国网络安全法[Z]，2016.11

[2] 全国人大. 中华人民共和国数据安全法[Z]，2021.6

[3] 全国人大. 中华人民共和国个人信息保护法[Z]，2021.8

[4] 国务院. 中华人民共和国人类遗传资源管理条例（国令第 717 号）[Z]，2019.5

[5] 中央网信办. 国家网络安全事件应急预案[Z]，2017.1

[6] 国家网信办. 个人信息出境安全评估办法（征求意见稿）[Z]，2019.6

[7] 国家网信办. 数据出境安全评估办法(征求意见稿)[Z]，2021.10

[8] 国家网信办. 网络安全审查办法[Z]，2021.11

[9] 原国家食品药品监督管理总局.医疗器械说明书和标签管理规定（总局令第6号）[Z]，2014.7

[10] 原国家食品药品监督管理总局.医疗器械召回管理办法（总局令第29号）[Z]，2017.1

[11] 国家市场监督管理总局. 医疗器械不良事件监测和再评价管理办法（总局令第1号）[Z]，2018.8

[12] 国家市场监督管理总局.医疗器械注册与备案管理办法（总局令第47号）[Z]，2021.8

[13] 原国家食品药品监督管理总局.医疗器械生产质量管理规范（2014年第64号公告）[Z]，2014.12

[14] 国家市场监督管理总局.医疗器械注册申报资料要求和批准证明文件格式（2021年第121号公告）[Z]，2021.9

[15] 原国家食品药品监督管理总局.医疗器械网络安全注册技术审查指导原则（2017年第13号通告）[Z]，2017.1

[16] 国家药品监督管理局.医疗器械生产质量管理规范附录独立软件（2019年第43号通告）[Z]，2019.7

[17] 国家药品监督管理局.医疗器械生产质量管理规范独立软件现场检查指导原则(药监综械管〔2020〕57号)[Z]，2020.5

[18] 国家药品监督管理局医疗器械技术审评中心. 医疗器械软件技术审查指导原则（第二版）（征求意见稿）[Z]，2020.5

[19] 北京市药品监督管理局. 医疗器械网络安全注册审查指导原则实施指南[Z]，2019.12

[20]国家卫生健康委员会. 国家健康医疗大数据标准、安全和服务管理办法（试行）（国卫规划发〔2018〕23号）[Z]，2018.7

[21] GB9706.1-2020 医用电气设备 第1部分：基本安全和基本性能的通用要求[S]

[22] GB/T 20985.1-2017 信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理[S]

[23] GB/T 22080-2016 信息技术安全技术信息安全管理体系要求[S]

[24] GB/T 22081-2016 信息技术安全技术信息安全管理实用规则[S]

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

[26] GB/T 25000.51-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则[S]

[27] 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[S]

[28] GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求[S]

[29] GB/T 29246-2017 信息技术安全技术信息安全管理体系概述和词汇[S]

[30] GB/T 30276-2020 信息安全技术 网络安全漏洞管理规范[S]

[31] GB/T 31167-2014 信息安全技术 云计算服务安全指南[S]

[32] GB/T 31168-2014 信息安全技术 云计算服务安全能力要求[S]

[33] GB/T 31722-2015 信息技术 安全技术 信息安全风险管理[S]

[34] GB/T 35273-2020 信息安全技术 个人信息安全规范[S]

[35] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求[S]

[36] GB/T 35278-2017 信息安全技术 移动终端安全保护技术要求[S]

[37] GB/T 37964-2019 信息安全技术 个人信息去标识化指南[S]

[38] GB/T 37973-2019 信息安全技术 大数据安全管理指南[S]

[39] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型[S]

[40] GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南[S]

[41] GB/T 39725-2020 信息安全技术 健康医疗数据安全指南[S]

[42] GB/T 信息安全技术 数据出境安全评估指南（征求意见稿）[S]，2017.8

[43] GB/T 信息安全技术 重要数据识别指南（征求意见稿）[S]，2022.1

[44] YY/T 0287-2017 医疗器械 质量管理体系 用于法规的要求[S]

[45] YY/T 0316-2016 医疗器械 风险管理对医疗器械的应用[S]

[46] YY/T 0664-2020 医疗器械软件 软件生存周期过程[S]

[47] YY/T 1406.1-2016 医疗器械软件 第 1 部分:YY/T 0316 应用于医疗器械软件的指南[S]

[48] YY/T 1708.1-2020 医用诊断 X 射线影像设备连通性符合性基本要求 第 1 部分：通用要求[S]

[49] YY/T 1708.2-2020 医用诊断 X 射线影像设备连通性符合性基本要求 第 2 部分：X 射线计算机体层摄影设备[S]

[50] YY/T 1708.3-2021 医用诊断 X 射线影像设备连通性符合性基本要求 第 3 部分：数字化摄影 X 射线机（DR）[S]

[51] YY/T 1708.4-2021 医用 X 射线影像设备连通性符合性基本要求 第 4 部分：数字减影血管造影 X 射线机（DSA）[S]

[52] YY/T 1708.5-2021 医用诊断 X 射线影像设备连通性符合性基本要求 第 5 部分：乳腺 X 射线机[S]

[53] YY/T 1708.6-2021 医用诊断X射线影像设备连通性符合性基本要求 第6部分：口腔X射线机[S]

[54] YY/T 医用电气设备网络安全基本要求（报批稿）[S]，2020.12

[55] IMDRF/SaMD WG/N12 FINAL: 2014, SaMD:Possible Framework for Risk Categorization and Corresponding Considerations[Z], 2014.9

[56] IMDRF/SaMD WG/N23 FINAL:2015,SaMD:Application of Quality Management System[Z], 2015.10

[57] IMDRF/CYBER WG/N60FINAL:2020, Principles and Practices for Medical Device Cybersecurity[Z], 2020.4

[58] FDA, Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software[Z], 2005.1

[59] FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices[Z], 2014.10

[60] FDA, Postmarket Management of Cybersecurity in Medical Devices[Z], 2016.12

[61] FDA, Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices[Z], 2017.9

[62] FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices(Draft Guidance)[Z], 2018.10

[63] FDA, Best Practices for Communicating Cybersecurity Vulnerabilities to Patients[Z], 2021.10

[64] FDA, Playbook for Threat Modeling Medical Devices[Z], 2021.11

[65] MDCG 2019-16 Rev.1, Guidance on Cybersecurity for medical devices[Z], 2020.7

[66] BSI. Cybersecurity of medical devices:Addressing patient safety and the security of patient health information[Z], 2017.3

[67] AAMI TIR57:2016/(R)2019, Principles for medical device security - Risk management[S]

[68] AAMI TIR97:2019, Principles for medical device security - Postmarket risk management for device manufacturers[S]

[69] IEC TR 60601-4-5:2021, Medical electrical equipment - Part 4-5:Guidance and interpretation - Safety-related technical security specifications[S]

[70] IEC80001-1:2021, Application of risk management for IT-networks incorporating medical devices - Part 1:Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software[S]

[71] IECTR 80001-2-1:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-1: Step-by-step risk management of medical IT-networks - Practical applications and examples[S]

[72] IECTR 80001-2-2:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance

for the disclosure and communication of medical device security needs, risks and controls[S]

[73] IECTR 80001-2-3:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-3: Guidance for wireless networks[S]

[74] IECTR 80001-2-4:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-4: Application guidance - General implementation guidance for healthcare delivery organizations[S]

[75] IECTR 80001-2-5:2014, Application of risk management for IT-networks incorporating medical devices - Part 2-5: Application guidance - Guidance on distributed alarm systems[S]

[76] ISOTR 80001-2-6:2014, Application of risk management for IT-networks incorporating medical devices -Part 2-6: Application guidance - Guidance for responsibility agreements[S]

[77] ISOTR 80001-2-7:2015, Application of risk management for IT-networks incorporating medical devices -Application guidance -Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1[S]

[78] IECTR 80001-2-8:2016, Application of risk management for IT-networks incorporating medical devices - Part 2-8: Application guidance - Guidance on standards for establishing the

security capabilities identified in IEC/TR 80001-2-2[S]

[79] IECTR 80001-2-9:2017, Application of risk management for IT-networks incorporating medical devices - Part 2-9: Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities[S]

[80] IEC 80001-5-1:2021,Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle[S]

[81] ISO 81001-1:2021, Health software and health IT systems safety, effectiveness and security - Part 1: Principles and concepts[S]

[82] ISO TS 81001-2-1, Health software and health IT systems safety,effectiveness and security - Part 2-1:Coordination - Guidance for the use of assurance cases for safety and security[S]

[83] ISO/IEC 27035-1:2016, Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management[S]

[84] ISO/IEC 27035-2:2016, Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response[S]

[85] ISO/IEC 29147:2018, Information Technology - Security Techniques - Vulnerability Disclosure[S]

[86] ISO/IEC 30111:2013, Information Technology - Security Techniques - Vulnerability Handling Processes[S]

[87] ISO 27799:2016, Health informatics - Information security management in health using ISO/IEC 27002[S]

[88] NEMA CSP 1-2016, Cybersecurity for Medical Imaging[S]

[89] NEMA HN 1-2019, Manufacturer Disclosure Statement for Medical Device Security[S]

[90] UL 2900-1:2020, Standard for Software Cybersecurity for Network Connectable Products - Part 1: General Requirements[S]

[91] UL 2900-2-1:2018, Software Cybersecurity for Network Connectable Products - Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems[S]

[92] 全国信息安全标准化技术委员会[Z]，https://www.tc260.org.cn

[93] IMDRF CYBER WG[Z]， https://www.imdrf.org/workitems/wi-mdc-guide.asp