附件 1:

医疗器械网络安全技术审查指导原则（第二版）征求意见稿

目录

（三）远程维护

（四）陈旧设备

六、网络安全研究资料

（一）自研软件网络安全研究报告

（二）自研软件网络安全更新研究报告

（三）现成软件网络安全研究资料

七、注册申报资料说明

（一）产品注册

（二）许可事项变更

（三）延续注册

八、参考文献

医疗器械网络安全技术审查指导原则
(第二版)

本指导原则旨在指导注册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，为医疗器械软件和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性要求，注册人应根据医疗器械产品特性提交网络安全注册申报资料，判断指导原则中的具体内容是否适用，不适用内容详述理由。注册人也可采用其他满足法规要求的替代方法，但应提供详尽的研究资料。

本指导原则基于当前认知水平和技术能力，在现行法规体系下参考国外法规与指南、国际标准与技术报告予以制定。随着认知水平和技术能力的不断提高以及法规体系的不断完善，相关内容也将适时修订。

本指导原则作为注册人、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。

本指导原则作为《医疗器械软件技术审查指导原则》（以下简称软件指导原则）的补充，应结合软件指导原则相关要求使用。

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、远程控制或用户访问功能的第二、三类独立软件和含有软件组件的医疗器械。

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，远程控制包括基于网络的实时、非实时控制，用户访问包括基于软件用户界面（含独立软件、软件组件）、电子接口（含网络接口、电子数据交换接口）的人机交互方式。

二、网络安全基础

（一）网络安全基本概念

1.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均处于可接受水平。

其中，保密性是指信息不被未授权实体（含个人、组织）获

[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。

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是相互制约的关系，某一特性的能力提升会使得另一特性或多个特性的能力下降，例如可得性的提升通常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。注册人应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。

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，但是本指导原则从医疗

器械软件角度出发不做严格区分，统一采用网络安全进行描述，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。

2.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。

（1）医疗数据是指医疗器械所使用的、产生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，反之即为非敏感医疗数据。个人信息是指能够单独或与其他信息结合识别特定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。敏感医疗数据属于健康数据，健康数据是指标明生理、心理健康状况的私人数据，涵盖医疗领域、健康领域。

（2）设备数据是指描述医疗器械运行状况的数据，用于监视、控制医疗器械运行或用于医疗器械的维护维修，不应含有个人信息。

注册人应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数据安全要求。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。

3.电子接口

医疗器械电子接口包括网络接口、电子数据交换接口。

（1）网络接口：是指医疗器械通过网络进行电子数据交换或远程控制，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）、物理接口（如电口、光口）、数据接口（标准协议、私有协议）、远程控制方式（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）、无线电、射频、红外等形式，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，需考虑定制化功能的兼容性问题。远程控制包括系统软件所提供的运程桌面功能。

（2）电子数据交换接口：是指医疗器械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）或存储媒介（如光盘、移动硬盘、U 盘）进行电子数据交换。

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、文件储存格式（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，需考虑文件格式完整性问题。

注册人应结合医疗器械电子接口（含内部接口、外部接口）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。

（二）网络安全能力

根据医疗器械网络安全相关标准和技术报告的定义，本指导原则所述医疗器械网络安全能力包括:

1.自动注销: 产品在使用闲置期间阻止非授权用户访问和使用的能力。

2.审核: 产品提供用户活动可被审核的能力。

3.授权: 产品确定用户已获授权的能力。

4.网络安全特征配置: 产品根据用户需求配置网络安全特征的能力。

5.网络安全补丁升级: 授权用户或服务人员安装/升级网络安全补丁的能力。

6.数据去标识化: 产品直接去除或匿名化数据所含个人信息的能力。

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

8.紧急访问: 产品在预期紧急情况下允许用户访问和使用的能力。

9.数据完整性与真实性: 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。

10.恶意软件探测与防护: 产品有效探测、阻止恶意软件的

能力。

11.节点鉴别：产品鉴别网络节点的能力。

12.人员鉴别：产品鉴别授权用户的能力。

13.物理防护：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。

14.现成软件维护：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。

15.系统固化：产品通过固化措施对网络攻击和恶意软件的抵御能力。

16.网络安全指导：产品为用户提供网络安全指导的能力。

17.存储保密性与完整性：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。

18.传输保密性与完整性：产品确保数据传输保密性和完整性的能力。

19.远程访问与控制：产品确保用户远程访问与控制的网络安全的能力。

20.抗拒绝服务攻击：产品具有抗拒绝服务攻击的能力。

注册人应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，并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设置或采用动

态口令，亦可采用生物识别技术，一般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，明确不适用理由并予以记录。

（三）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，注册人应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。

注册人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。

注册人应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，结合风险管理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。造成严重后果或影响的事件应向药监部门报告，适用时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。

（四）网络安全更新

1.基本概念

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。根据其对医疗器械的影响程度可分为以下两类:

（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，应申请许可事项变更。

（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，无需申请许可事项变更，待下次许可事项变更时提交相应注册申报资料。考虑到网络安全更新亦具有累积效应，注册申报资料应涵盖自前次注册以来的全部网络安全更新内容。

此外，涉及召回的网络安全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。

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

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：产品所处网络环境发生改变，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；电子接口发生改变，如接口形式由网口变为 USB 口、接口数量由少变多、接口功能由电子数据交换扩至远程控制等。

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一般视为轻微网络安全更新：网络环境、电子接口的数据传输效率单纯提高，电子接口原有功能单纯优化；医疗器械软件、必备软件（医疗器械软件正常运行所必需的其他医疗器械软件、医用中间件）、外部软件环境（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）的网络安全补丁更新。

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。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。注册人应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，基于国家互联网应急中心（CNCERT/CC）、国家信息安全漏洞共享平台（CNVD）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人、用户（含医疗机构、个人）、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，但这不意味注册人可以免除医疗器械网络安全相关责任。注册人应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之一，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。注册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。

（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，其风险级别一般情况下可参照软件安全性级别，即医疗器械网络安全的风险级别与所属医疗器械软件的安全性级别相同。在特殊情况下，网络安全的风险级别可低于软件风险级别，此时应详述理由并按新软件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应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，因此对于适用于多个使用场景的医疗器械，注册人应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剩余风险。注册人可结合医疗器械风险管理和网络安全风险管理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。

（三）全生命周期管理

与软件类似，注册人应在医疗器械全生命周期中持续关注网络安全问题，包括但不限于设计开发、生产、分销、部署、更新维护、上市后监测等。

医疗器械上市前应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，及时将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[2]来完善医疗器械网络安全管理工作，以保证医疗器械的安全有效性。

四、网络安全生存周期过程

网络安全生存周期过程作为软件生存周期过程的重要组成部分，应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，具体要求详见软件指导原则第六章以及《医疗器械生

[2]在信息安全领域，IEC 27000 系列标准明确信息安全管理体系（ISMS）认证要求，本指导原则不要求注册人进行 ISMS 认证，但建议参考相关标准要求。

产质量管理规范附录独立软件》、《医疗器械生产质量管理规范独立软件现场检查指导原则》。

注册人可参考信息安全领域相关标准、技术报告，完善网络安全生存周期过程质控要求。

五、技术考量

（一）现成软件

现成软件同样存在网络安全问题，注册人应根据质量管理体系要求建立现成软件网络安全更新维护过程，及时将现成软件网络安全相关信息以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。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；需要说明的是，网络安全补丁属于设计变更，需要进行验证、确认。

（二）医疗数据出境

根据《中华人民共和国网络安全法》相关规定，在中国境内收集和产生的个人信息和重要数据应当在中国境内存储，因业务需要确需向境外提供的，应当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。《人口健康信息管理办法（试行）》

亦规定，不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。

医疗数据属于重要数据，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个人信息、重要数据出境安全评估办法的相关规定。

（三）远程维护

具有远程维护功能的医疗器械可以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。同时，远程维护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。此外，医疗器械在远程维护过程中若无人值守，则可能存在医疗器械非授权访问和使用的风险。

因此，注册人应明确远程维护的实现方法、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、维护过程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。

（四）陈旧设备

本指导原则所述陈旧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。陈旧设备由于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，因此应尽快停运退市。

医疗器械实际使用情况极为复杂，一般情况下可结合医疗器械停售、停止售后服务两个时间点判定其是否属于陈旧设备：在售的医疗器械均非陈旧设备；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陈旧设备，反之不属于陈旧设备；停止售后服务的医疗器械均为陈旧设备。

对于陈旧设备，注册人应按照质量管理体系关于软件停运/软件退市的要求开展相应工作，详见《医疗器械生产质量管理规范附录独立软件》。

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，按陈旧设备处理。

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，并申请许可事项变更。

六、网络安全研究资料

（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，每项条款的具体要求若不适用应说明理由，详见表 1。

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。

若网络安全的风险级别低于软件风险级别，详述理由并按新软件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）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（敏感与非敏感医疗数据、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口接口、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 20 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，若适用详述网络安全能力的实现方法，反之说明不适用的理由。

（4）网络安全补丁

提供申报医疗器械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。

（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（含远程维护）的风险分析报告、风险管理报告，另附原文。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（含远程维护）需求规范文档，另附原文。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（含远程维护）测试计划和报

告，另附原文。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，出具真实性声明即可；对于私有传输协议或存储格式，提供完整性测试总结报告。对于实时远程控制功能，提供完整性和可得性测试报告。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（含远程维护）可追溯性分析报告，即追溯网络安全能力、网络安全需求规范、网络安全设计规范、网络安全测试报告、网络安全风险分析报告的关系表。

（5）更新维护计划

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，全部级别均应提供远程维护的流程图，并依据图示描述相关活动。

3. 漏洞评估

轻微级别：按照通用漏洞评分系统（CVSS）所定义的漏洞

等级，明确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，按照 CVSS 漏洞等级明确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、影响、风险，确保风险均可接受。或提供第三方网络安全漏洞评估报告。

严重级别：提供境内第三方网络安全评估机构出具的网络安全漏洞评估报告，以及已知剩余漏洞的维护方案。

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。

表 1：自研软件网络安全研究报告框架

条款		轻微	中等	严重
基本信息	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		
	网络安全能力	逐项分析 20 项网络安全能力的适用情况		
	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		
	更新维护计划	提供网络安全更新、远程维护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或第三方网络安全漏洞评估报告，按照	提供境内第三方网络安全评估机构出具的网络安全漏洞评估报告，以及已

		漏洞等级明确已知漏洞总数和剩余漏洞情况	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、网络安全补丁更新研究报告。

网络安全功能更新研究报告适用于重大、轻微网络安全功能更新，或合并网络安全补丁更新，内容详见表 2，不再赘述。

网络安全补丁更新研究报告仅适用于医疗器械软件、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、更新维护计划、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

条款		**轻微**	**中等**	**严重**
基本信息	软件信息	明确申报版本软件情况，详述变化。		
	数据架构	明确申报版本软件情况，详述变化。		
	网络安全能力	明确申报版本软件情况，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	明确申报版本软件情况，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		
	更新维护计划	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		明确申报版本软件已知漏洞总数和剩余漏洞数	提供申报版本软件的网络安全自评报告，明确已知漏洞总数和剩余	提供申报版本软件的境内第三方网络安全评估机构出具的网络安全漏洞评

		漏洞情况	估报告
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		

（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，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、更新维护计划、漏洞评估、结论。

此时若现成软件发生网络安全更新，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，说明现成软件的变化情况，不适用条款说明理由；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，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（此时即医疗器械软件）的安全性级别予以说明。

此时若现成软件发生网络安全更新，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，说明现成软件的变化情况，不适用条款说明理由；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，具体要求详见软件指导原则第八章。

七、注册申报资料说明[3]

（一）产品注册

1.软件研究资料

注册人应在软件研究资料中提交自研软件网络安全研究报告、外部软件环境评估报告。

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

说明书应提供网络安全说明，明确用户访问控制机制、电子接口（含网口接口、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）、安全软件兼容性、外部软件环境与安全软件更新等要求。

（二）许可事项变更

1.软件研究资料

医疗器械许可事项变更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：

[3] 产品技术要求关于网络安全的要求详见医疗器械软件技术审查指导原则（第二版）。

（1）涉及网络安全功能更新：适用于发生功能更新或合并补丁更新的情形，此时提交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）、外部软件环境评估报告；

（2）仅发生网络安全补丁更新：提交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。

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，说明书应体现网络安全的变更内容。

（三）延续注册

延续注册无需提交网络安全相关研究资料。

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，应在产品未变化声明中予以明确，其中软件版本命名规则涵盖网络安全更新情况。

八、参考文献

[1]《中华人民共和国网络安全法》（中华人民共和国主席令第五十三号，2016.11）

[2]《中华人民共和国数据安全法（草案）》（全国人大，

2020.7）

[3]《国家网络安全事件应急预案》（中央网信办，2017.10）

[4]《个人信息出境安全评估办法（征求意见稿）》（国家互联网信息办公室，2019.6）

[5]《人口健康信息管理办法（试行）》（国卫规划发〔2014〕24 号）

[6]《医疗器械注册管理办法》（国家食品药品监督管理总局令第 4 号）

[7]《医疗器械说明书和标签管理规定》（国家食品药品监督管理总局令第 6 号）

[8]《医疗器械召回管理办法》（国家食品药品监督管理总局令第 29 号）

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

[10]《医疗器械注册申报资料要求和批准证明文件格式》（征求意见稿）

[11]《医疗器械软件注册技术审查指导原则》（国家食品药品监管总局通告 2015 年第 50 号）

[12]《医疗器械软件技术审查指导原则（第二版）》（征求意见稿）

[13]《医疗器械网络安全注册技术审查指导原则》（国家食

品药品监督管理总局通告2017年第13号）

[14]《医疗器械生产质量管理规范附录独立软件》（国家药品监督管理局通告2019年第43号）

[15]《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）

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

[17] 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》

[18] GB/T 22080-2016《信息技术 安全技术 信息安全管理体系要求》

[19] GB/T 22081-2016《信息技术 安全技术 信息安全管理实用规则》

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

[21] 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》

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

[23] 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》

[24] GB/T 31722-2015《信息技术 安全技术 信息安全风险管理》

[25] GB/T 35273-2020《信息安全技术 个人信息安全规范》

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

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

[28] YY/T 0316-2016《医疗器械 风险管理对医疗器械的应用》

[29] YY/T 0664-2020《医疗器械软件 软件生存周期过程》（报批稿）

[30] 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》

[31]YY/T 1708.2《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》

[32]YY/T 1708.3《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）》

[33]YY/T 1708.4《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）》

[34]YY/T 1708.5《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》

[35] YY/T 1708.6《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》

[36] YY/T《医用电气设备网络安全基本要求》（讨论稿）

[37] DB32/T 3769-2020《医疗器械网络连接通用技术规范》

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

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

[40] IMDRF/CYBER WG/N60 FINAL:2020, Principles and Practices for Medical Device Cybersecurity, 2020.4

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

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

[43] FDA, Radio Frequency Wireless Technology in Medical Devices, 2013.8

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

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

[46] FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Draft, 2018.10

[47] MDCG, Guidance on Cybersecurity for medical devices, 2019.12

[48] AAMI TIR57:2016, Principles for medical device security - Risk management

[49] AAMI TIR 97:2019, Principles for medical device security - Postmarket risk management for device manufacturers

[50] HIMSS/NEMA HN 1-2013, Manufacturer Disclosure Statement for Medical Device Security

[51] IEC 60601-1 AMD1:2012, Medical electrical equipment - Part 1: General requirements for basic safety and essential performance

[52] IEC/TR 60601-4-5, Medical electrical equipment - Part 4-5. Safety related technical security specifications for medical devices

[53] IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices - Part 1: Roles,responsibilities and activities

[54] IEC/TR 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

[55] IEC/TR 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

[56] IEC/TR 80001-2-3:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-3: Guidance for wireless networks

[57] IEC/TR 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

[58] IEC/TR 80001-2-5:2014, Application of risk management for IT-networks incorporating medical devices - Part 2-5: Application guidance - Guidance on distributed alarm systems

[59] ISO/TR 80001-2-6:2014, Application of risk management for IT-networks incorporating medical devices -Part 2-6: Application guidance - Guidance for responsibility agreements

[60] ISO/TR 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

[61] IEC/TR 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

[62] IEC/TR 80001-2-9, 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

[63] ISO/IEC 80001-5-1, Application of Risk Management for IT networks incorporating medical device - Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software - Part 5-1: Activities in the product life-cycle

[64] ISO 81001-1, Health software and health IT systems safety, effectiveness and security - Foundational principles, concepts and terms

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

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

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

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

[69] ISO 27799 Health informatics - Information security management in health using ISO/IEC 27002

[70] NEMA/MITA CSP 1-2016, Cybersecurity for Medical Imaging

[71] UL 2900-1:2017, Standard for Software Cybersecurity for Network Connectable Products - Part 1: General Requirements

[72] UL 2900-2-1:2017, Software Cybersecurity for Network Connectable Products - Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems

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

[74] 国家互联网应急中心，https://www.cert.org.cn

[75] 国家信息安全漏洞共享平台，https://www.cnvd.org.cn