医疗器械网络安全注册审查指导原则实施指南

发布时间：2021 年 06 月 03 日

医疗器械网络安全注册审查指导原则实施指南

目 录

本指导原则实施指南旨在指导注册申请人提交第二类医疗器械网络安全注册申报资料，同时为第二类医疗器械网络安全的技术审评提供参考。

本指导原则实施指南是对第二类医疗器械网络安全一般性要求的细化和补充，注册申请人应根据医疗器械产品特性提交网络安全注册申报资料，注册申请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和验证资料。

本指导原则实施指南是对注册申请人和审评人员的指导性文件，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，应在遵循相关法规的前提下使用本指导原则实施指南。

本指导原则实施指南依据原国家食品药品监督管理总局发布的《医疗器械软件注册技术审查指导原则》和《医疗器械网络安全注册技术审查指导原则》编写，因而采用时应结合以上注册技术审查指导原则的相关要求使用。

本指导原则实施指南适用于具有网络连接功能以进行电子数据交换或远程控制的第二类医疗器械产品的注册申报，其中网络连接包括无线网络连接和有线网络连接，电子数据交换包括单向数据传输和双向数据传输，远程控制包括实时控制和非实时控制。

同时，本指导原则实施指南也适用于采用存储媒介以进行电子数据交换的第二类医疗器械产品的注册申报，其中存储媒介包括但不限于光盘、移动硬盘和 U 盘。

需要指出的是，本指导原则实施指南中所述的文件应来源于医疗器械的开发过程。注册申请人应将网络安全风险管理与质量管理体系充分融合，在确保医疗器械安全有效性的同时提高医疗器械的网络安全。

一、综述

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，这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，导致患者或使用者受到伤害甚或死亡。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。

同时，对于接入计算机信息系统的医疗器械，注册申请人应考虑医疗器械的使用环境，对预期接入定级系统或非定级系统的医疗器械的网络安全能力进行合理的设计。注册申请人还应考虑国家对于网络安全相关的法律法规和标准要求，特别是计算机信息系统安全保护方面的要求，例如《中华人民共和国计算机信息系统安全保护条例》，《GB/T 22239-2019 信息系统安全等级保护基本要求》，《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》等法规和标准。

二、医疗器械的使用环境

医疗器械根据使用环境可以分为家用医疗器械和医院用医疗器械，以及既可以在家庭使用也可以在医院使用的医疗器械。根据接口的类型可以分为有线网络连接、无线网络连接和连接本地存储媒介。根据所处的网络环境又可分为无网络环境（仅连接本地存储媒介）、受控的网络环境和开放的网络环境。注册申请人应根据不同的使用环境，识别网络安全风险，并采取相应的网络安全措施。

三、 医疗器械的网络安全

（一） 医疗器械网络安全特性

医疗器械网络安全是指保持医疗器械相关数据的保密性、完整性、可得性、真实性、可核查性、抗抵赖性以及可靠性等特性。

1.保密性

指数据不能被未授权的个人、实体利用或知悉的特性，即医疗器械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；

2.完整性

指保护数据准确和完整的特性，即医疗器械相关数据是准确和完整的，且未被篡改；

3.可得性

指根据授权个人、实体的要求可访问和使用的特性，即医疗器械相关数据能以预期方式适时进行访问和使用；

4.真实性

一个实体是其所声称实体的特性，即医疗器械相关数据能够体现其真实的临床状态，例如：生理状态、操作状态、设备状态等；

5.可核查性

实体表征对自己的动作和做出的决定负责的特性，即医疗器械相关数据表征对相关临床动作和决定负责；

6.抗抵赖性

证明所声称事态或行为的发生及其发起实体的能力，以解决有关事态或行为发生与否以及事态中实体是否牵涉的争端，即医疗器械相关数据可证明相关临床事态和行为的发生及其发起的能力；

7.可靠性

与预期行为和结果一致的特性，即医疗器械相关数据与临床的预期行为和结果一致。

（二）网络安全能力

对医疗器械网络安全的保障，是用户、网络设施提供方与注册申请人共同参与的结果。以现有技术水平而言，注册申请人可以参考《IEC TR 80001-2-2-2012 包含医疗器械的 IT 网络的风险管理应用.第 2-2 部分 医疗器械安全》以及《T/ZMDS 20003-2019 医疗器械网络安全风险控制 - 医疗器械网络安全能力信息》等标准，识别医疗器械网络安全能力，进行网络安全风险控制。

需要注意的是，注册申请人对这些网络安全能力进行配置以配合用户进行网络安全风险管理时，应综合考虑具体医疗器械的预期用途与使用场景。医疗器械的预期用途一般是对疾病的预防、诊断与治疗，在权衡医疗器械的安全性、有效性以及数据安全时，需要首先保证医疗器械的安全性、有效性。例如，为了在急救环境下发挥医疗器械的有效性，可能会对保密性的要求予以折衷。综合考虑的结果导致大部分的医疗器械可能并不具备全部的网络安全能力，此时需要注册申请人与用户进行良好的沟通，以实现最终医疗环境下的网络安全。

以下列出了 19 种医疗器械网络安全能力，并依据相关标准，结合医疗器械的产品特点对其主要内容进行了描述，注册申请人可根据医疗器械的产品特性，预期用途和使用方式考虑其网络安全能力要求的适用性。

1.自动登出能力（ALOF）

无人值守的医疗器械终端设备，存在被进行非授权操作、显示信息被非授权人员阅读的风险。此项网络安全能力确保医疗器械在所设时段内若未被用户操作，则自动进入保护状态，从而降低上述风险发生的概率。此项网络安全能力，改善了医疗器械的保密性与完整性，但会降低医疗器械的可得性，对急诊用医疗器械、长期监护用医疗器械、用户无需获得授权的医疗器械等可得性要求较高的医疗器械应结合医疗器械的预期用途与使用场景，决定是否配置以及如何配置。

2.审核控制能力（AUDT）

医疗器械的网络安全与医疗器械的使用方式息息相关，不正确、非授权的使用会导致医疗器械存在网络安全方面的风险。对医疗器械使用环节的关键信息予以记录，是风险控制措施的一部分。此项能力的配置对网络安全的保密性、完整性、可核查性均有提高，有利于对医疗器械使用记录提供可追溯性检测以及用于事后问责调查和对风险的持续监视，也为风险控制的应急响应提供输入。

3.确定用户权限的能力（AUTH）

医疗器械的非授权使用，会导致多种危险情况，确保医疗器械的使用者、管理者、维护者、拥有者得到合适的授权是重要的风险控制手段。用户权限的管理可以提高保密性、完整性与可核查性，但可能会降低可得性。

4.网络安全配置能力（CNFS）

对医疗器械网络安全的保障是由用户、使用者、网络设施提供方、注册申请人多方共同参与的一项活动。开放网络安全相关的配置有利于网络安全在使用场景中的整体部署，但是另一方面医疗器械在有意、无意情况下的配置错误也可能导致不可接受的风险，此项能力与系统的加固要求（SAHD）相矛盾，应根据医疗器械的预期用途与使用方式综合考虑此项能力的配置。

5.网络安全升级能力（CSUP）

医疗器械以及医疗器械所依赖的软硬件环境，所面临的威胁并不是一成不变的，作为风险控制手段，有必要对医疗器械或医疗器械的运行环境予以修补以抵御新的网络威胁。由于医疗器械、运行环境、所受威胁的状况千差万别，

部分修补可以由用户自行升级完成；而部分修补则可能需要注册申请人的授权人员才能进行。

6.健康数据去标识化能力（DIDT）

在医疗服务过程中产生的健康数据常常具有预防、诊断、治疗之外的其它价值，例如科研、培训、不良事件追溯、设备维护等。健康数据若直接用于非医疗用途，则存在隐私数据保护方面的风险。数据交付之前，去除健康数据所附带的身份信息，是提高保密性的重要手段。但去除标识会降低数据的可追溯性。

7.数据备份与灾难恢复能力（DTBK）

健康数据在处理过程中面临着数据被破坏甚至丢失的风险，保持数据备份与灾难恢复的能力，可以提高数据的完整性与可得性。

8.紧急访问隐私数据的能力（EMRG）

医疗器械是以提供预防、诊断、治疗目的为核心属性，部分情况下医疗器械、数据的可得性受损会导致不可接受的风险。为医疗器械配置被紧急访问的能力以及相应的安全可控的紧急访问流程，对此项风险的控制至关重要。然而，配置被紧急访问的能力，常常会导致可得性之外的其它网络安全特性降低，应根据医疗器械的预期用途与使用方式综合考虑此项能力的配置。

9.数据完整性真实性确认能力（IGAU）

当数据的完整性受损而导致不可接受的风险时，医疗器械具备此项能力可以确保健康数据的来源可靠且未经篡改与破坏。

10.恶意软件的防止、检测与清除能力（MLDP）

恶意软件侵入医疗器械可能会导致不可接受的风险，此项能力可以对已知恶意软件进行探测、报告并防止受其侵害。由于恶意软件的产生难以预知，此项能力需要在医疗器械的使用过程中不断维护，必要时采取紧急措施。

11.通信对象、通信节点的身份验证能力（NAUT）

医疗器械如与未经授权的通信节点进行互操作，可能导致不可接受的风险。此项能力配合用户的网络安全策略可确保数据的发送方与接收方相互识别并被授权进行数据传输。

12.验证合法用户的能力（PAUT）

有一部分医疗器械并非开放给所有的使用者，这部分医疗器械如果被未获授权的用户使用，可能导致不可接受的风险。此项能力配合用户的网络安全策略，可确保医疗器械的使用者是经过授权认证的。

13.物理保护能力（PLOK）

医疗器械在物理上被侵入，会造成保密性与完整性的破坏，可能导致不可接受的风险。可以重点关注敏感信息的存储媒介（可移动媒介除外）是否不借助工具就能被取出。

14.第三方组件管理能力（RDMP）

医疗器械可能用到第三方组件作为整体医疗器械的一部分，例如第三方的操作系统或数据库等。用户若对此类组件不知情，则不利于此类组件未来的网络安全管理，也不利于未来网络安全事件的责任划分，可能导致不可接受的风险。

15.系统与应用加固能力（SAHD）

医疗器械中可能存在着与预期用途无关的配置，例如：某些非医疗预期用途的账号、通信端口、共享文件、服务等。此类配置可能会成为网络攻击者所利用的通道，从而造成不可接受的风险，对这些配置予以关闭有利于降低风险发生的概率。

16.对操作者与管理员提供网络安全指导的能力（SGUD）

医疗器械的不当使用可能在医疗器械网络安全方面造成不可接受的风险，对使用者提供产品说明、提供可索取的披露资料、予以培训等，均有利于降低使用者操作不当的风险。

17.存储保密能力（STCF）

健康数据的明文存储会降低产品的保密性，对数据存储予以加密有利于降低数据泄露相关的风险。国家对商用密码产品的科研、生产、销售、使用等都有相应的管理规定。使用商用密码应遵守相关的法律法规要求。

18.传输保密能力（TXCF）

健康数据的明文传输会降低医疗器械的保密性，对数据传输予以加密有利于降低数据泄露相关的风险。国家对商用密码产品的科研、生产、销售、使用等都有相应的管理规定。使用商用密码应遵守相关的法律法规要求。

19.保障数据传输完整性的能力（TXIG）

健康数据在传输过程中，数据可能受到无意的信道噪声干扰，也有可能受到恶意篡改，这都可能造成不可接受的风险。采用技术手段确保所接受到的数据与所发送出数据具有一致性，可以降低此类风险。

注册申请人可以通过综合考虑上述19项网络安全能力来提高医疗器械的网络安全特性。网络安全能力与网络安全特性之间的关系如下：

自动登出能力（ALOF）	2	2	-1	-
审核控制能力（AUDT）	1	1	-	1
确定用户权限的能力（AUTH）	2	2	-1	1
网络安全配置能力（CNFS）	1	1	1	1
网络安全升级能力（CSUP）	1	1	1	-
数据备份与灾难恢复能力（DTBK）	-	1	2	-
紧急访问隐私数据的能力（EMRG）	-	-	2	-1
健康数据去标识化能力（DIDT）	2	-	-	-
数据完整性真实性确认能力（IGAU）	-	2	-	2
存储保密能力（STCF）	2	-	-	-
恶意软件的防止、检测与清除能力（MLDP）	1	1	1	-
通信对象、通信节点的身份验证能力（NAUT）（）（）（）	1	-	-	1
验证合法用户的能力（PAUT）	1	-	-	2
物理保护能力（PLOK）	1	1	1	-
对操作者与管理员提供网络安全指导的能力（SGUD）	1	1	1	1
系统与应用加固能力（SAHD）	1	1	1	-
第三方组件管理能力（RDMP）	-	-	-	-
传输保密能力（TXDF）	2	-	-	-
保障数据传输完整性的能力（TXIG）	-	2	-	-
网络安全特性 网络安全能力	**保密性**	**完整性**	**可得性**	**可靠性**

注：“2”指可以显著提高此项网络安全特性，“1”指可以提高此项网络安全特性，“-”指基本不对此项网络安全特性产生影响，“-1”指可以降低此项网络安全特性。

（三）网络安全的上市后监管

1.网络安全事件

网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。

网络安全事件可能会造成医疗器械系统不能访问、医疗数据泄露或者篡改，进而导致病人受到严重伤害，死亡或病人的健康数据泄漏。

2.网络安全事件的处置

注册申请人应建立医疗器械上市后的网络安全事件处置流程。网络安全事件发生后，注册申请人应能够及时有效地处理和管理安全事件，一般包括以下措施：

应收集并确认受网络安全事件影响的用户，识别网络安全事件对相关系统带来的风险；

应快速采取应急对策，例如：告知用户断开网络连接，提供临时解决方案恢复系统至正常工作状态等；

应对网络安全事件的做出详细的风险分析和评估；

应提供经过验证和确认的解决措施，并告知用户相关的更新信息。

注册申请人应建立相应的组织以确保网络安全事件处置流程得以实施。

3.网络安全事件上报

当下列网络安全事件发生，注册申请人应及时向相关监管部门报送信息：

——病人受到严重伤害或者死亡；

——注册申请人提供的大量医疗器械系统不能访问；

——大量的病人健康数据泄露。

若涉及到病人受到严重伤害或死亡的网络安全事件，注册申请人应按照医疗器械不良事件的相关规定上报。

4.涉及召回的网络安全事件应按照医疗器械召回的相关法规处理，不属于本指导原则讨论范围。

5.网络安全更新的管理

网络安全更新（包括自主开发软件和现成软件）根据其对医疗器械的影响程度可分为以下两类：

——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；

——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，例如常规安全补丁。

医疗器械产品发生重大网络安全更新，应进行许可事项变更；而发生轻微网络安全更新，注册申请人应通过质量管理体系进行控制，无需进行注册变更，待到下次注册（注册变更或延续注册）时提交相应注册申报资料。医疗器械同时发生重大和轻微网络安全更新，遵循风险从高原则应进行许可事项变更。

涉及召回的网络安全更新应按照医疗器械召回的相关法规处理，不属于本指导原则讨论范围。

软件版本命名规则应考虑网络安全更新的情况。

注册申请人在提交注册申报资料时，应根据医疗器械网络安全的具体情况提交网络安全描述文档或常规安全补丁描述文档。网络安全描述文档适用于医疗器械注册、重大网络安全更新，常规安全补丁描述文档适用于轻微网络安全更新。

四、 网络安全注册资料

注册申请人应结合医疗器械产品的预期用途、使用环境和核心功能以及预期相连设备或系统（例如：其它医疗器械、信息技术设备）的情况来确定医疗器械产品的网络安全特性，提交网络安全描述文档。网络安全描述文档应描述医疗器械的基本信息、风险管理、验证与确认以及维护计划。

（一） 基本信息

应描述医疗器械产品网络安全相关的基本信息，这些信息包括：

1.医疗器械传输，存储和处理信息的总结性描述；

2.以上信息的类型：健康数据、设备数据；

3.以上信息的传输方向：单向、双向；

4.以上信息是否用于实时远程控制：实时、非实时或不用于远程控制；

5.以上信息的用途：如临床应用、设备维护等；

6.以上信息的交换方式：网络（无线网络、有线网络）及要求（如传输协议、接口、带宽等），存储媒介（如光盘、移动硬盘、U盘等）及要求（如存储格式、容量等）；对于专用无线设备（非通用信息技术设备），还应提交符合无线电管理规定的证明材料，如涉及个人敏感数据，应明确个人敏感数据的储存和传输方式；

7.医疗器械包含的安全软件：描述安全软件（如杀毒软件、防火墙等）的名称、型号规格、完整版本、供应商、运行环境要求；

8.医疗器械包含的现成软件：描述现成软件（包括应用软件、系统软件、支持软件）的名称、型号规格、完整版本和供应商。

（二）风险管理

1.网络安全风险管理概述

网络安全风险管理是指注册申请人基于医疗器械产品的预期用途和使用场景进行网络安全风险分析，评价并采取网络安全风险控制手段确保产品的网络安全能力。注册申请人可对网络安全采用医疗器械风险管理的方法（可参照《YY/T 0316-2016 医疗器械 风险管理对医疗器械的应用》）对医疗器械网络安全相关的风险进行分析、评价和控制，也可采用信息安全风险评估的方法（可参照《GB/T20984 信息安全技术 信息安全风险评估规范》）进行评估，并进行风险控制。

如适用，医疗器械网络安全风险管理应考虑对个人敏感信息的保护。对个人信息的处理，应遵循个人信息安全基本原则和相关的法律法规以及标准，如《GB/T 35273-2017 信息安全技术 个人信息安全规范》。如有必要，应对个人信息进行匿名化或去标识化处理。

风险管理除了从网络安全角度来考虑医疗器械的网络安全能力外，还应根据医疗器械的预期用途考虑网络安全风险对医疗器械的安全性和有效性的影响。

医疗器械网络安全风险管理需要考虑整个医疗器械生命周期并适时更新。

2.网络安全风险管理过程

（1）风险分析与评价

注册申请人应对网络安全管理活动进行策划并制定网络安全风险可接受性准则。注册申请人应考虑网络安全损害的严重度和网络安全损害的发生概率并按照接受性准则决定是否需要降低风险。

1） 网络安全损害的严重度，例如：

等级名称	代码	网络安全损害的严重度
轻度	1	轻微伤或者无须处理，少量设备数据泄露...
中度	2	中等人身伤害需要专业医治，有限的设备数据泄露...
严重	3	一人重伤或者死亡，有限的病人数据泄露...
灾难	4	多人重伤或者死亡，大规模病人数据泄露...

2） 网络安全损害的发生概率，例如：

等级名称	代码	网络安全损害的发生概率
很低	1	几乎不可能发生，仅可能在非常罕见和例外的情况下发生
低	2	一般不太可能发生，或没有被证实发生过
中等	3	在某种情况下可能会发生，或被证实曾经发生过或在大多数情况下很有可能会发生，或可以证实多次发生过
高	4	或在大多数情况下很有可能会发生，或可以证实多次发生过
很高	5	在大多数情况下几乎不可避免，或可以证实经常发生过

注：发生概率应和医疗器械具体情况相适应

（2）风险控制

根据风险评价结果需要降低风险时，注册申请人应识别适当的风险控制措施，以把风险降低到可接受的水平。

例如：风险分析、评价和风险控制措施记录表

漏洞		威胁	描述				技术风险				
系统设计、实施或操作和管理中的一系列条件，使其易受影响		有可能造成不良后果的来源。可以是作用物、人、事件或事物，动机可以是有意的或无意的	原因、影响因素、描述风险场景、漏洞和缓解因素（漏洞+可利用性）	初始风险			缓解措施		剩余技术风险		
漏洞编号	漏洞描述	威胁描述	风险状况	可能性	影响	风险	缓解措施	缓解措施编号	可能性	影响	风险

例如：风险评估矩阵模型

注：下表中红色表示不可接受风险，黄色和绿色表示可接受风险。表格中的数字仅作为举例。采取风险控制措施后，剩余风险中不可接受风险数量为0。

1）初始风险分布

概率		严重度			
		4	3	2	1
		灾难	严重	中度	轻度
经常	5	0	0	0	0
有时	4	1	0	2	2
偶尔	3	0	2	4	1
非常少	2	0	0	0	3
极少	1	2	0	2	1

2）采取风险控制措施后风险分布

概率		严重度			
		4	3	2	1
		灾难	严重	中度	轻度
经常	5	0	0	0	0
有时	4	0	0	0	1
偶尔	3	0	1	2	1
非常少	2	0	0	0	3
极少	1	0	0	2	1

（3）风险管理报告

注册申请人应形成网络安全风险管理报告，并完成风险管理过程的评审，确认综合剩余风险是可接受的。

（4）关于上市后的风险

注册申请人要持续关注医疗器械上市后与医疗器械相关的网络安全风险，根据实际情况适时更新风险分析、评价和控制文件，如法规更新、不良事件报告等。

（三）验证与确认

1．总体原则

网络安全验证和确认活动的目的是确定风险管理中采用的网络安全控制手段均已得到正确的实施，确保医疗器械产品的网络安全需求（例如保密性、完整性、可得性等特性）均已得到满足。

对于现成软件，注册申请人应在网络安全风险分析过程中将其作为医疗器械的一部分进行充分的网络安全评估，并在医疗器械的网络安全能力配置中予以综合考虑。

2．验证与确认活动

注册申请人应在医疗器械产品研制过程中进行网络安全的验证与确认活动，通过分析、测试、评估、审查等手段，确保医疗器械产品的网络安全需求得到满足。网络安全验证与确认活动可以参考附录中的 19 项网络安全能力应用参考，应根据医疗器械的预期用途、使用方式和风险评估综合考虑每项网络安全能力的验证。

（1）应确保在医疗器械产品的需求、设计、测试以及风险管理各个阶段考虑并落实网络安全需求，并且保证网络安全需求规范、设计规范、测试以及风险管理的一致性和完整性。

（2）应针对医疗器械产品进行网络安全测试验证，确保所有网络安全风险控制措施都得到正确的实施。

1）应对网络安全测试活动进行合理的策划，包括确定测试的内容（包括医疗器械需求中要求配置的网络安全能力）、测试人员和相应的职责、测试所需的环境、测试的技术和方法（如漏洞测试、恶意软件测试、缺陷输入测试、结构化渗透测试等）、异常处理方式、测试通过的准则、测试所需的资源以及测试进度安排等。

2）应根据测试计划的安排设计测试用例，并按照测试用例的要求执行测试活动，记录原始测试结果，确保测试过程的可追溯性。对于安全软件，注册申请人应针对不同的软件、硬件运行平台，进行兼容性测试；如医疗器械采用标准传输协议或存储格式，应进行审查或测试验证其对相关标准的符合性；如医疗器械采用自定义的传输协议和存储格式，应进行完整性测试验证。

3）应对测试结果进行分析和评价，确保测试活动的有效性，并对测试遗留的问题进行评价。

3．验证与确认记录

注册申请人应将医疗器械网络安全验证与确认活动的结果以文档的方式进行记录，确保网络安全验证与确认活动的可追溯性。

（1）应以文档的形式记录医疗器械网络安全需求规范、设计规范、测试以及风险管理的追溯性关系。

（2）应对网络安全测试策划活动进行记录并形成网络安全测试计划文档。

（3）应对网络安全测试执行过程、测试结果以及测试结果的分析评估进行记录，形成网络安全测试报告。

（4）对于安全软件，注册申请人可将兼容性测试结果进行单独文档记录，并形成兼容性测试报告。

（5）对于采用标准传输协议或存储格式的医疗器械，注册申请人应记录标准符合性审查结果；对于采用自定义的传输协议和存储格式的医疗器械，注册申请人应对完整性测试结果进行记录并形成完整性测试报告。

（6）可以对实时远程控制功能医疗器械中关于远程数据相关的测试进行单独的文档记录，并形成相应的完整性和可得性测试报告。

（四）维护计划

1．维护流程

在医疗器械产品上市后，注册申请人应结合自身质量管理体系要求，制定网络安全维护流程，保证医疗器械的安全性和有效性。

网络安全维护流程涉及到以下方面：

（1）监控网络安全信息源（包括第三方软件组件）以识别和检测网络漏洞；

（2）了解、检测可能发生的漏洞，评估其风险影响；

（3）重点分析与医疗器械的安全和基本性能有关的网络安全问题，特别是网络安全事件相关的问题，针对其风险和影响，制定缓解策略，使得医疗器械及时得到保护和恢复；

（4）用于修补漏洞的软件更新和补丁程序，包括第三方软件组件的漏洞修复（如操作系统，安全软件等），需要进行验证和确认；

（5）尽早地部署软件网络安全更新程序至用户站点，并告知用户相关更新内容。

有关医疗器械产品中网络漏洞的披露和处理，可参阅文献《ISO/IEC 29147-2018 信息技术 安全技术 漏洞公告》和《ISO/IEC 30111-2013 信息技术 安全技术 漏洞处理流程》。

2. 网络安全更新

具备联网功能的医疗器械产品面临的网络问题可能不断变化，注册申请人在医疗器械产品上市前难以解决所有的网络安全问题。注册申请人应对已上市医疗器械产品进行有效、及时并持续地网络安全更新。

对于已发现的漏洞，应分析漏洞的可被利用性，对病人伤害的严重程度以及病人信息泄露的可能性，注册申请人应决定该漏洞的风险是可控还是处于失

控状态，制定相应的解决措施修复该网络漏洞。与网络安全事件相关的网络更新，需要重点分析其风险和影响，及时有效地提供经验证的解决方案。

通常的网络安全更新应包括：

（1）自研软件的漏洞安全更新；

（2）第三方软件（包括操作系统等）的漏洞安全更新；

（3）安全软件（例如杀毒软件等）的病毒扫描引擎的更新。

若在医疗器械产品中新的网络安全设计是不可行的或者不能马上实施，注册申请人应考虑使用网络补偿控制方案来减轻网络漏洞风险。

网络补偿控制是在缺乏有效网络安全设计的前提下，提供补充性网络防护措施。例如注册申请人对医疗器械产品的网络漏洞评估后，认为对设备在未被授权的情况下进行访问极有可能影响设备的安全和基本性能，但是若该设备没有连接到外部网络(例如，医院网络)或者使用路由器对连接进行限定，则医疗器械仍然可以安全有效的工作。

（五）产品技术要求

1.数据接口

对于预期接入网络或与其它医疗器械进行交互的医疗器械，其数据交换方式有两种：网络（包括有线网络和无线网络）或存储媒介（如光盘、移动硬盘、U 盘等）。

对于数据交换的接口，常见的有线接口包括 USB、RS232、RS485、CAN、RJ45 等。近些年，无线通讯被广泛使用，例如蓝牙、WiFi、Zigbee、RFID、各种蜂窝无线网络等。对于有线接口，技术要求中应明确连接接口的规格。有线网络应明确带宽要求。对于无线网络，应描述网络类型、制式、使用频段、数据特性（如上/下行传输速率）等。

注册申请人可以采用已经标准化的医用数据传输协议或存储格式。常见的医疗器械传输协议如 HL7、DICOM 等，医疗器械存储格式如 EDF 等。注册申请人也可以使用通用的网络传输协议如 TCP/IP、UDP、HTTP、HTTPS 等。注册申请人在产品技术要求中，应明确传输协议/存储格式。对于已经标准化的传输协议或存储格式除了说明协议类型之外，还应说明协议的版本，如果用于控制，还应说明是否为实时控制。

对于注册申请人自定义的数据传输协议或存储格式，应在随机文件中描述或在产品技术要求中提供相应的验证方法。

2.用户访问控制

医疗器械在执行用户访问控制之前，应完成对用户身份的鉴别或认证。认证是系统验证希望访问系统的用户身份的过程。基本的认证技术包括数字签名、消息认证、数字摘要等。在产品技术要求中注册申请人应明确医疗器械所采用的用户身份鉴别或认证技术。

用户访问控制策略对医疗器械的保密性、完整性起直接的作用，是对越权使用资源的防御措施，是网络安全的重要组成部分。医疗器械的使用者应依据访问控制策略来限制对数据和系统功能的访问。用户访问控制的种类早期分为自主访问控制（DAC）和强制访问控制（MAC），但随着计算机和网络技术的发展，又出现了基于角色的访问控制（RBAC）、基于任务的访问控制（TBAC）、以及基于属性、上下文、信誉等的访问控制模型。随着系统的复杂度变高，一个系统中也可以融合多种访问控制策略。在产品技术要求中，注册申请人应明确医疗器械执行的用户访问控制的方法、用户类型及权限。

（六）说明书

预期接入计算机网络或与其它医疗器械进行交互的医疗器械具有复杂的运行环境与技术生态系统。例如：复杂的信息基础设施（如硬件、软件、网络、其他系统和数据接口等），参与开发、实施、临床使用所涉及的众多的人员、组织和机构。医疗器械生命周期不仅包含设计、开发、也包括实施和临床使用，其中包含医疗器械的采购、安装、配置、数据集成或迁移、工作流实现与优化、培训、使用与维护、退市等环节。

一般情况下，注册申请人只涉及医疗器械的设计与开发过程，而后期的实施与临床使用等环节的网络安全可能由另外的组织和机构来负责。注册申请人但应在说明书或其他文档中提供在实施与临床使用环节中所需要的必要信息，如运行环境、接口与访问控制、安全软件及软件更新等，以保证在实施与临床使用环节的网络安全。

1.运行环境

如适用，注册申请人在说明书中应明确医疗器械的运行环境，包括硬件配置、软件环境和网络条件。硬件配置应明确医疗器械安全运行所需要的最低硬件资源配置要求，如 CPU、内存、存储与显示要求等。软件环境应明确要求医疗器械运行所需要的操作系统等。网络条件应明确医疗器械运行所需要的网络类型、带宽等。

2.接口与访问控制

如适用，注册申请人在说明书中应描述接口与访问控制，以满足医疗器械实施与临床使用过程中的要求。对于接口的描述，应能够满足医疗器械与网络、或其它设备的安全连接。对于访问控制的描述，应能指导使用者安全使用系统提供的访问控制策略并集成到工作流程中。

3.安全软件

在资源允许的情况下，医疗器械可使用一些安全软件来提高医疗器械的网络安全特性。这些安全软件包括但不限于防火墙、杀毒软件、反流氓软件、工具软件等。如适用，注册申请人应在说明书中明确这些软件的名称、版本等信息。

4.软件更新

如适用，注册申请人应在说明书中明确软件环境与安全软件的更新需求，更新的来源、执行的步骤等。

附录

19 项网络安全能力应用参考

1.自动登出能力（ALOF）

注册申请人应考虑，未授权的用户不能在无人值守的工作区访问健康数据，授权用户会话在预先设置的一段时间后自动终止或锁定；自动注销能够清除所有显示器上的健康数据；本地授权的管理员能够禁用该功能并设置过期时间(包括屏幕保护程序)；当短时间内(例如 15 秒到几分钟)没有按下键时，此功能被调用以清除显示的健康数据；临床用户不会因自动下线而丢失未提交的工作。

2.审核控制能力（AUDT）

注册申请人应考虑，通过在设备上创建审计跟踪来跟踪系统和健康数据的访问、修改或删除，从而记录和检查系统活动。将日志记录信息作为独立的存储库(在其自己的文件系统中记录审计文件)使用。使用适当的审计审查工具支持审计创建和维护，确保审核资料的安全(特别是在这些资料本身含有个人资料的情况下)，并确保无法编辑或删除审计数据。审计数据可能包含个人数据和/或健康数据，所有处理(例如存取、储存和转移)都应该有适当的控制。

3.确定用户权限的能力（AUTH）

注册申请人应考虑适当的授权功能允许每个用户仅访问已批准的数据，并执行已批准的功能。医疗器械一般支持基于许可的系统，提供对角色(基于角色的访问控制)适当的系统功能和数据访问。例如：

（1）操作者可使用所有适当的设备功能(例如监察或扫描病人)执行指定的工作；

（2）质量保证人员(如医学物理学家)可以从事所有适当的质量和保证测试活动；

（3）服务人员可以以支持预防性维护、问题调查和问题消除活动的方式访问系统；

4.网络安全配置能力（CNFS）

注册申请人应考虑，经过授权的本地管理员能够选择使用医疗器械安全功能还是不使用医疗器械安全功能。

5.网络安全升级能力（CSUP）

注册申请人应考虑，尽快在医疗产品上安装第三方安全补丁。 根据客观的、权威的、文档化的漏洞风险评估，优先考虑解决高风险漏洞的补丁。应进行充分的测试，以发现对医疗器械(性能或功能)可能危及患者的任何意外副作用。注册申请人需要主动提供关于评估/验证补丁的信息。

6.健康数据去标识化能力（DIDT）

注册申请人应考虑，临床用户、服务工程师和营销人员能够在不需要患者身份的信息的情况下去识别敏感数据。

7.数据备份与灾难恢复能力（DTBK）

注册申请人应保证在系统故障或损坏后，可以恢复存储在医疗器械上的持久保存的系统设置和敏感数据，以便业务能够继续进行。这一要求可以不适用于较小的低成本设备。

8.紧急访问隐私数据的能力（EMRG）

注册申请人应考虑，在紧急情况下，临床用户需要能够在没有个人用户 ID 和身份验证的情况下访问敏感数据（break-glass 功能）。应检测、记录和报告紧急通道。理想情况下，包括以某种方式立即通知系统管理员或医务人员（除了审计记录之外）。注册申请人可以使用特定用户帐户或系统功能的方法以满足紧急访问在输入时要求并记录自认证用户标识（无需身份验证）的要求。管理员能够启用/禁用依赖于技术或过程控制的医疗器械提供的紧急访问功能。

9.数据完整性真实性确认能力（IGAU）

注册申请人应考虑，通过使用包括固定媒介和可移动媒介，来确保健康数据是可靠的，不会被篡改。

10.恶意软件的防止、检测与清除能力（MLDP）

注册申请人应考虑，相关法规和用户需求，以确保可以有效预防、检测和删除恶意软件。对防止恶意软件的应用程序及恶意软件模式数据文件及时进行软件更新，及时对当前操作环境、系统、数据文件和应用程序进行补丁更新。并对设备更新后进行验证测试。

11.通信对象、通信节点的身份验证能力（NAUT）

注册申请人应考虑管理跨节点的账户的访问，以保护健康数据。可以支持独立管理或集中管理。支持根据行业标准进行节点认证。检测和防止实体伪造（提供不可抵赖性）。

12.验证合法用户的能力（PAUT）

注册申请人应考虑管理账户以保护健康数据的能力。提供基于角色的访问控制（RBAC）。用户可以将个人首选项与用户账户关联。可以支持独立或集中管理。单一账号登录所有工作地点且密码相同。控制对设备、网络资源和健康数据的访问并生成不可否认的审计跟踪。发现和防止人员造假（提供不可抵赖性）。

13.物理保护能力（PLOK）

注册申请人应根据数据的敏感程度和数据量保证其存储安全性。合理地避免了可能危及完整性、保密性或可用性的篡改或组件删除。确保篡改（包括设备移除）是可以检测到的。

14.第三方组件管理能力（RDMP）

注册申请人应对医疗器械提供明确的预期寿命说明，并对提供第三方组件的服务商对其医疗器械生命周期内维护或支持相应的系统进行要求。当平台组件过时的情况下，需要及时进行更新和升级。在存储设备退役（丢弃、重用、转售或回收）之前，服务提供商需不可逆地擦除健康数据。这些活动应该被记录和审计。销售和服务人员应了解对每个医疗器械在其生命周期中提供的安全支持。

15.系统与应用加固能力（SAHD）

注册申请人应给用户提供一个稳定的系统，并且只提供那些根据其预期用途而指定和需要的服务，同时进行最少的维护活动。并且要求连接到它们的网络的系统在交付时是安全的以加强对误用和攻击的抵御能力。注册申请人应将用户反馈的用户设备中可疑的安全漏洞和察觉到的弱点以报告的形式记录。并通过风险分析和管理进行漏洞的修复，并及时更新交付。

16.对操作者与管理员提供网络安全指导的能力（SGUD）

注册申请人应让操作人员清楚地了解自己的职责和安全的系统工作方式。管理员需要关于管理、定制和监视系统的信息（即访问控制列表、审计日志等）。管理员需要清楚地了解安全功能，以便根据适当的法规要求进行健康数据风险评估。销售和服务应包括系统的安全能力和安全工作方式的信息。用户应知道如何以及何时将用户设备中可能存在的安全漏洞和察觉到的弱点通知注册申请人。

17.存储保密能力（STCF）

注册申请人应合理保证储存在医疗器械或媒介上的健康数据的安全。基于风险分析，考虑对存储在医疗器械上的健康数据进行加密。对于临床用户、提供服务和收集临床数据的应用程序工程师使用的存储在可移动媒介上的健康数

据，加密可以保护其机密性/完整性。应考虑使用正常使用、服务访问、紧急访问一致的加密密钥管理机制。加密方法和强度应考虑数据量和敏感性。

18.传输保密能力（TXCF）

注册申请人应考虑在经过身份验证的节点之间传输健康数据的机密性。

19.保障数据传输完整性的能力（TXIG）

注册申请人应考虑在相对开放的网络或环境中传输健康数据，需保证健康数据的完整性。

参考文献：

1）《医疗器械软件注册技术审查指导原则》（原国家食品药品监督管理总局 2015 年第 50 号通告）

2）《医疗器械网络安全注册技术审查指导原则》（原国家食品药品监督管理总局 2017 年第 13 号通告）

3）《中华人民共和国计算机信息系统安全保护条例》（中华人民共和国国务院令第 147 号）

4）中华人民共和国互联网信息办公室《国家网络安全事件应急预案》（中网办发文〔2017〕4 号）

5）GB/T 29246-2012 信息安全技术 信息安全管理体系概述和词汇

6）GB/T 20984-2015 信息安全技术 信息安全风险评估规范

7）GB/T 22239-2019 信息系统安全等级保护基本要求

8）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

9）GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

10) GB 17859-1999 计算机信息系统 安全保护等级划分准则

11）YY/T 0316-2016 医疗器械 风险管理对医疗器械的应用

12）IEC TR 80001-2-2-2012 包含医疗器械的 IT 网络的风险管理应用.第 2-2 部分 医疗器械安全

13）T/ZMDS 20001-2016 风险管理在 IT 网络引入医疗器械时的应用 第 1 部分：角色、责任与活动

14）T/ZMDS 20003-2019 医疗器械网络安全风险控制 – 医疗器械网络安全能力信息

15）ISO/IEC 27035-2011 Information technology - Security techniques - Information security incident management

16）ISO/IEC 27035-1:2016 Part 1: Principles of incident management

17）ISO/IEC 27035-2:2016 Part 2: Guidelines to plan and prepare for incident response

18）ISO/IEC 27043:2015 Information technology - Security techniques - Incident investigation principles and processes

19）ISO 27799:2016 Health informatics—Information security management in health using ISO/IEC 27002

20）ISO/IEC 29147:2014 Information technology - Security techniques - Vulnerability disclosure

21）ISO/IEC 30111:2013 Information technology - Security techniques - Vulnerability handling processes

22）ISO/IEC TS 33052:2016 Information technology - Process reference model (PRM) for information security management

22）ISO/IEC 80001 Application of risk management for IT-networks incorporating medical devices

23) IEC/TR 80001-2-3:2012: Part 2-3: Application of risk management for IT-networks incorporating medical devices - Guidance for wireless networks

24）IEC/TR 80001-2-8:2016 Part 2-8: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

25）IEC/TR 80002-3:2014 Part 3: Process reference model of medical device software life cycle processes (IEC 62304)

26）HIMSS/NEMA Manufacturer Disclosure Statement for Medical Device Security