序号与项目	旧版	新版
1 指导原则的地位	本指导原则作为《医疗器械软件注册技术审查指导原则》的补充，应结合《医疗器械软件注册技术审查指导原则》的相关要求使用。	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
2.范围	本指导原则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、第三类医疗器械产品的注册申报。本指导原则也适用于采用存储媒介以进行电子数据交换的第二类、第三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。	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。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。
3.主要概念	健康数据：标明生理、心理健康状况的私人数据（“Private Data”，又称个人数据“Personal Data”、敏感数据“Sensitive Data”，指可用于人员身份识别的相关信息），涉及患者隐私信息；	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[1]，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：描述设备运行状况的数据，用于监视、控制设备运行或用于设备的维护保养，本身不涉及患者隐私信息。	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。
	/	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：通过网络（包括无线网络、有线网络）进行电子数据交换或远程控制，需要考虑网络相关要求（如接口、带宽等），数据传输协议需考虑是否为标准协议（即业内公认标准所规范的协议），远程控制需考虑是	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。

	否为实时控制；	
	/	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。
	存储媒介：通过存储媒介（如光盘、移动硬盘、U 盘等）进行电子数据交换，数据储存格式需考虑是否为标准格式（即业内公认标准所规范的格式）。	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。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。
4.网络安全能力	19 项网络安全能力：自动注销（ALOF）、审核控制（AUDT）、授权（AUTH）、安全特性配置（CNFS）、网络安全产品升级（CSUP）、健康数据身份信息去除（DIDT）、数据备份与灾难恢复（DTBK）、紧急访问（EMRG）、健康数据完整性与真实性（IGAU）、恶意软件探测与防护（MLDP）、网络节点鉴别（NAUT）、人员鉴别（PAUT）、物理锁（PLOK）、第三方组件维护计划（RDM	22 项网络安全能力：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

	P）、系统与应用软件硬化（SAHD）、安全指导（SGUD）、健康数据存储保密性（STCF）、传输保密性（TXCF）传输完整性（TXIG）	（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。
5.网络安全事件应急响应	/	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。
6.医疗器械网络安全更新	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；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，如常规安全补丁。	（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。
7.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；

判定原则		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。
8.医疗器械网络安全的安全性级别	/	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。
9.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[2]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。
10 医疗器械网络安全生存周期过程	/	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。
11.医疗数据出境	/	《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[3]，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。
12.远程维护与升级	/	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。
13.遗留设备	/	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。
14.自研软件网络安全研究报告	1.基本信息（1）类型：健康数据、设备数据；（2）功能：电子数据交换（单向、双向）、远程控制（实时、非实时）；（3）用途：如临床应用、设备维护等；（4）交换方式：网络（无线网络、有线网络）及要求（如传输协议（标准、自定义）、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（标准、自定义）、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；（5）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	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.（3）网络安全能力 22 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、

	商、运行环境要求；（6）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。 2.风险管理提供医疗器械网络安全风险管理的分析报告和总结报告，确保全部剩余风险均是可接受的。 3.验证与确认提供网络安全测试计划和报告，证明医疗器械产品的网络安全需求（如保密性、完整性、可得性等特性）均已得到满足。同时还应提供网络安全可追溯性分析报告，即追溯网络安全需求规范、设计规范、测试、风险管理的关系表。对于安全软件，应提供兼容性测试报告。对于标准传输协议或存储格式，应提供标准符合性证明材料，而对于自定义传输协议或存储格式，应提供完整性测试总结报告。对于实时远程控制功能，应提供完整性和可得性测试报告。 4.维护计划描述软件（含现成软件）网络安全更新的维护流程，包括更新确认和用户告知。 / /	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。
15.自研软件网络安全更新研究报告	常规安全补丁描述文档提交软件（含现成软件）常规安全补丁的情况说明（补丁描述、影响分析、用户告知计划）、测试计划与报告、新增已知剩余缺陷情况说明（证明新增风险均是可接受的）。	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 1 基本信息（1）软件信息（2）数据架构（3）网络安全能力（4）网络安全补丁（5）安全软件 2.实现过程（1）风险管理（2）验证与确认（3）可追溯性分析（4）维护计划 3.漏洞评估 4.结论
16.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。（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。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。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。
17．现成软件网络安全更新研究	/	（1）部分使用方式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。

18.说明书	说明书应提供关于网络安全的相关说明，明确运行环境（含硬件配置、软件环境和网络条件）、安全软件（如杀毒软件、防火墙等）、数据与设备（系统）接口、用户访问控制机制、软件环境（含系统软件、支持软件、应用软件）与安全软件更新的相关要求。	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。
19.产品技术要求	注册申请人应在产品技术要求性能指标中明确数据接口、用户访问控制的要求：（1）数据接口：传输协议/存储格式；（2）用户访问控制：用户身份鉴别方法、用户类型及权限。	并入《医疗器械软件注册审查指导原则》

更多资讯，请扫码关注