附件1

**医疗器械网络安全注册技术指导原则**

**（征求意见稿）**

本指导原则旨在指导制造商提交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。

本指导原则是对医疗器械网络安全的一般性要求，制造商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。制造商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。

本指导原则是在现行法规和标准体系以及当前认知水平下、并参考了国外法规与指南、国际标准与技术报告制定的。随着法规和标准的不断完善，以及认知水平和技术能力的不断提高，相关内容也将适时进行修订。

本指导原则是对制造商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。

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》相关要求进行使用。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、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，其中网络包括无线、有线网络，电子数据交换包括单向、双向数据传输，远程控制包括实时、非实时控制。

同时，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。

二、基本原则

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。

医疗器械网络安全是指保持医疗器械相关数据的保密性（confidentiality）、完整性（integrity）和可得性（availability）（改自GB/T 29246-2012《信息技术 安全技术 信息安全管理体系 概述和词汇》）：

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。

此外，医疗器械网络安全特性还包括真实性（authenticity）、可核查性（accountability）、抗抵赖（non-repudiation）和可靠性（reliability）等特性，相应定义详见GB/T 29246-2012。

制造商应当结合医疗器械产品的预期用途、使用环境和核心功能以及相连设备或系统（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，并采用基于风险管理的方法来保证医疗器械产品的网络安全：识别资产（asset，对个人或组织有价值的任何东西）、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产品和患者的影响以及被利用的可能性，确定风险水平并采取适宜的风险缓解措施，基于风险接受准则评估剩余风险。

制造商应当在医疗器械产品整个生命周期过程中持续关注网络安全问题，包括医疗器械产品的设计开发、生产、分销、部署和维护。同时，制造商应当结合自身质量管理体系的要求和医疗器械产品特点来保证医疗器械产品的网络安全，包括上市前和上市后的相关要求，如风险管理、设计开发、网络安全维护及用户告知等要求。此外，制造商可采用信息安全领域的良好工程实践来完善医疗器械产品的网络安全管理，保证医疗器械产品的安全性和有效性。

制造商应当持续跟踪与网络安全相关的国家法律法规以及有关部门（如公安部、卫生计生委、工信部）的规章，医疗器械的网络安全应当符合相应法律法规和部门规章的要求。

医疗器械产品在使用过程中常与非制造商预期的设备或系统相连接，这就使得制造商难以控制和保证医疗器械产品的网络安全。因此，医疗器械的网络安全需要制造商、用户和信息技术服务商的共同努力和通力合作才能得以保障。制造商应当保证医疗器械产品自身的网络安全，并明确与其预期相连设备或系统的接口要求，从而保证医疗器械产品的安全性和有效性。

鉴于医疗器械网络安全具有影响因素多、涉及面广、扩散性强和突发性高等特点，单独考虑医疗器械产品的软件安全性级别不足以保证其网络安全，因此医疗器械网络安全注册申报资料统一进行要求。

三、网络安全考量

（一）数据考量

医疗器械相关数据从内容上可分为以下两种类型：

1. 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；

2. 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。

医疗器械相关数据的交换方式可分为以下两种情况：

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，需要明确网络相关要求（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），远程控制需考虑是否为实时控制；

2. 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）。

制造商应当基于医疗器械相关数据的类型、功能、用途、交换方式及要求，并结合医疗器械产品特性考虑其网络安全问题。

对于健康数据，制造商应当遵循患者隐私保护的相关规定。

（二）技术考量

用户访问控制机制应当与医疗器械产品特性相适应，包括但不限于用户身份鉴别方法（如用户名、口令等）、用户类型及权限（如系统管理员、普通用户、设备维护人员等）、口令强度设置、软件更新授权等。

医疗器械相关数据在网络传输或数据交换过程中应当保证保密性和完整性，同时平衡可得性的要求，特别是具有远程控制功能的医疗器械。制造商可采用加密、数字签名、标准协议、校验等技术来保证医疗器械的网络安全。

医疗器械对于网络安全威胁的探测、响应和恢复能力应当与医疗器械的产品特性相适应。制造商可采用防火墙、入侵检测和恶意代码防护等技术来保证医疗器械的网络安全。

医疗器械网络安全能力建设可参照相关的国际、国家标准和技术报告，如IEC/TR 80001-2-2规范了十九项网络安全能力：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（RDMP）、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）和传输完整性（TXIG），制造商可根据医疗器械的产品特性考虑其网络安全能力要求的适用性。

（三）现成软件

医疗器械使用现成软件的情况日益普遍，特别是系统软件和支持软件。因此，制造商同样需要关注现成软件的网络安全问题，应当根据质量管理体系要求建立网络安全维护流程，并将医疗器械网络安全信息及时通知用户。

对于应用软件，制造商需要重点关注其网络安全问题对医疗器械临床应用的影响。而对于系统软件和支持软件，制造商需要重点关注其安全补丁更新对医疗器械的影响，安全补丁更新属于设计变更，需要进行验证与确认，但通常情况下可视为轻微软件更新，除非影响到医疗器械的安全性和有效性。

四、网络安全文档

（一）基本考量

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：

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。

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（注册变更和延续注册）时提交相应注册申报资料。

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。

医疗器械产品注册或发生重大网络安全更新时应单独提交一份网络安全描述文档，发生轻微网络安全更新时单独提交一份常规安全补丁描述文档即可。医疗器械同时发生重大和轻微网络安全更新，依据风险从高原则应提交一份网络安全描述文档。

（二）网络安全描述文档

1. 基本信息

描述医疗器械产品的相关信息：

（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），还应提交无线电发射设备核准证书；

（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、完整版本和供应商；

（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。

（三）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、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）。

五、注册申报资料要求

（一）产品注册

1. 软件研究资料

制造商应单独提交一份网络安全描述文档，具体要求详见第四节。

2. 产品技术要求

制造商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。

3. 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、运行环境与安全软件更新的相关要求。

（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：

（1）涉及重大网络安全更新：单独提交一份网络安全描述文档，具体要求详见第四节；

（2）仅发生轻微网络安全更新：单独提交一份常规安全补丁描述文档，具体要求详见第四节；

（3）未发生网络安全更新：出具真实性声明。

2. 产品技术要求

如适用，产品技术要求应体现关于网络安全的变更情况。

3. 说明书

如适用，说明书应体现关于网络安全的变更内容。

（三）延续注册

如适用，医疗器械延续注册产品分析报告第（六）项应单独提交一份常规安全补丁描述文档，具体要求详见第四节。

六、参考文献

[1]《中华人民共和国网络安全法（草案）》（全国人民代表大会常务委员会，2015.6）

[2]国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见（国办发〔2016〕47号）

[3]《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）

[4]《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）

[5]国家食品药品监督管理总局关于公布医疗器械注册申报资料要求和批准证明文件格式的公告（2014年第43号）

[6]国家食品药品监督管理总局关于发布医疗器械软件注册技术审查指导原则的通告（2015年第50号）

[7]《医疗器械召回管理办法（试行）》（卫生部令第82号）

[8]《人口健康信息管理办法（试行）》（国卫规划发〔2014〕24号）

[9]国家卫生计生委关于推进医疗机构远程医疗服务的意见（国卫医发〔2014〕51号）

[10] GB/T 20271-2006《信息安全技术 信息系统通用安全技术要求》

[11] GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

[12] GB/T 22080-2008《信息技术 安全技术 信息安全管理体系 要求》

[13] GB/T 22081-2008《信息技术 安全技术 信息安全管理实用规则》

[14] GB/T 29246-2012《信息技术 安全技术 信息安全管理体系 概述和词汇》

[15] GB/Z 24364-2009《信息安全技术 信息安全风险管理指南》

[16] YY/T 0287-2003《医疗器械 质量管理体系 用于法规的要求》

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

[18] YY/T 0664-2008《医疗器械软件 软件生存周期过程》

[19] YY/T 1474-2016 《医疗器械 可用性工程对医疗器械的应用》

[20] FDA, Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software, 2005-1-14

[21] FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, 2014-10-2

[22] FDA, Radio Frequency Wireless Technology in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, 2013-8-14

[23] FDA, Postmarket Management of Cybersecurity in Medical Devices - Draft Guidance for Industry and Food and Drug Administration Staff, 2016-1-22

[24] FDA, Design Considerations and Pre-market Submission

Recommendations for Interoperable Medical Devices - Draft Guidance for Industry and Food and Drug Administration Staff, 2016-1-26

[25] IEC 60601-1 Edition 3.1:2012, Medical electrical equipment - Part 1: General requirements for basic safety and essential performance

[26] IEC 82304-1, Health Software - Part 1: General requirements for product safety

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

[28] 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

[29] 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

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

[31] 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

[32] 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

[33] 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

[34] 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

[35] 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

[36] 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

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

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

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

[40] IMDRF/SaMD WG/N12 FINAL:2014, Software as a Medical Device(SaMD): Possible Framework for Risk Categorization and Corresponding Considerations, 2014-9-18

**编制说明**

一、编写目的和依据

本指导原则旨在指导制造商提交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。

本指导原则是在现行法规和标准体系以及当前认知水平下、并参考了国外法规与指南、国际标准与技术报告而制定的。本指导原则是对《医疗器械软件注册技术审查指导原则》的补充。

二、有关内容说明

美国和欧盟涉及医疗器械信息安全的指南和标准名称多使用网络安全这一用语，而在信息安全领域，网络安全属于信息安全的子集。为了与国际医疗器械监管用语相统一，并与信息安全领域用语相协调，本指导原则名称也将信息安全改为网络安全。

美国医疗器械网络安全指南适用于全部医疗器械软件，欧盟医疗器械网络安全标准和技术报告适用于医疗信息技术网络（Medical IT-network），本指导原则适用于具有电子数据交换（经网络、存储媒介）、远程控制功能（经网络）的医疗器械，适用范围介于美国和欧盟之间。

医疗器械网络安全防护层级可分为产品级和系统级，保证措施包括管理措施、物理措施和技术措施，本指导原则以医疗器械数据安全为核心主要关注产品级的技术保证措施。

在信息安全领域，信息安全的三个基本特性为保密性（[confidentiality](C:/Program%20Files/Youdao/Dict/6.3.69.5012/resultui/frame/javascript:void(0);)）、完整性（[integrity](C:/Program%20Files/Youdao/Dict/6.3.69.5012/resultui/frame/javascript:void(0);)）和可用性（[availability](C:/Program%20Files/Youdao/Dict/6.3.69.5012/resultui/frame/javascript:void(0);)）。鉴于可用性在医疗器械领域已有定义，即[usability](C:/Program%20Files/Youdao/Dict/6.3.69.5012/resultui/frame/javascript:void(0);)的译文，为了避免引起歧义，本指导原则将[availability](C:/Program%20Files/Youdao/Dict/6.3.69.5012/resultui/frame/javascript:void(0);)译为可得性。

在信息安全领域，IEC 27000系列标准规范了信息安全管理体系（ISMS）的认证要求，而ISO/DIS 27799规范了医疗领域的信息安全管理体系要求，我国已对IEC 27000系列标准的部分标准进行了等同转化。本指导原则不要求制造商进行信息安全管理体系认证，但建议制造商参考相关标准要求以保证医疗器械的网络安全，并鼓励有条件的制造商开展相关认证工作。

IEC/TR 80001-2-2、IEC 60601-1、IEC 82304-1等国际标准和技术报告规范了医疗器械网络安全的相关要求。鉴于国际标准转化工作不属于指导原则范畴，本指导原则未对相关国际标准的要求进行翻译，而是建议制造商遵循相关国际标准的要求。

制造商应当在医疗器械产品整个生命周期过程中持续关注网络安全问题，并结合自身质量管理体系的要求和医疗器械产品的特点来保证医疗器械产品的网络安全，包括上市前和上市后的相关要求。

医疗器械使用现成软件日益普遍，特别是系统软件和支持软件。制造商同样要考虑现成软件的网络安全问题，对于应用软件需要重点关注其网络安全问题对医疗器械临床应用的影响，而对于系统软件和支持软件需要重点关注安全补丁更新对医疗器械的影响。

医疗器械网络安全需要制造商、用户和信息技术服务商的共同努力和通力合作才能得以保障。制造商自身难以控制和保证医疗器械的网络安全，但这并不意味着制造商可以免除医疗器械网络安全的相关责任，相反制造商应当保证医疗器械产品自身的网络安全，并明确与预期相连设备或系统的接口要求，从而保证医疗器械产品的安全性和有效性。

医疗器械网络安全相关法规虽然尚未出台，但医疗器械的网络安全应当符合国家相应法律法规和部门规章的要求，包括正在制订的《中华人民共和国网络安全法》以及国家有关部委的相关规定，如《人口健康信息管理办法（试行）》规定各级各类医疗卫生计生服务机构（含中医药服务机构）不得将人口健康信息在境外服务器中存储，不得托管、租赁境外服务器；《国家卫生计生委关于推进医疗机构远程医疗服务的意见》规定非医疗机构不得开展远程医疗服务。

鉴于医疗器械网络安全具有影响因素多、涉及面广、扩散性强和突发性高等特点，单独考虑医疗器械产品的软件安全性级别不足以保证其网络安全。同时考虑到我国医疗器械网络安全监管工作尚处于起步阶段，注册申报资料要求不宜过于复杂。因此，本指导原则未基于软件安全性级别区分注册申报资料的要求，而是统一进行要求。今后，本指导原则将综合考虑国际医疗器械网络安全的监管趋势和国内行业发展的整体水平，在适当时机下开展修订工作。

三、起草单位

国家食品药品监督管理总局医疗器械技术审评中心