附件

医疗器械网络安全注册技术审查指导原则

本指导原则旨在指导注册申请人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，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，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。

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，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，导致患者或使用者受到伤害或死亡。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[1]（availability）（改自GB/T 29246-2012《信息技术安全技术信息安全管理体系

[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。

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。

注册申请人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预期相连设备或系统（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控制措施，基于风险接受准则评估剩余风险。

注册申请人应当在医疗器械产品全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，注册申请人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，注册申请人可采用信息安全领域的良好工程[2]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。

注册申请人应当持续跟踪与网络安全相关的国家法律法规（如《中华人民共和国网络安全法》）以及有关部门（如公安部、国家网信办、卫生计生委、工业和信息化部）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注册申请人预期的设备或系统相连接，这就使得注册申请人自身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注册申请人、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。但是这并不意味着注册申请人可以免除医疗器械网络安全的相关责任，注册申请人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。

[2]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）认证要求，本指导原则不要求制造商进行 ISMS 认证，但建议制造商参考相关标准要求。

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。

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，因此对于与医疗器械网络安全有关的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）。

注册申请人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，注册申请人应当遵循患者隐私保护的相关规定。对于无线设备，注册申请人应当遵循无线电管理的相关规定。

（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。注册申请人可采用加密、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。

鉴于预期用途、使用环境的限制，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。注册申请人可采用防火墙、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[3]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），注册申请人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）现成软件考量

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，注册申请人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，注册申请人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，注册申请人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

[3] 详见 IEC/TR 80001-2-2:2012Application 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

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。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产品注册、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。

（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。

（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（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）。

五、注册申报资料要求

（一）产品注册

1.软件研究资料

注册申请人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

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。

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、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。

（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

（一）《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）

（二）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）

（三）《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）

（四）《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）

（五）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（国家食品药品监管总局公告 2014 年第 43 号）

（六）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（国家食品药品监管总局通告 2015 年第 50 号）

（七）《医疗器械召回管理办法（试行）》（原卫生部令第 82 号）

（八）《人口健康信息管理办法（试行）》（国卫规划发〔2014〕24号）

（九）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）

（十）GB/T 20271-2006《信息安全技术信息系统通用安全技术要求》

（十一）GB/T 20984-2007 《信息安全技术信息安全风险评估规范》

（十二）GB/T 22080-2016《信息技术安全技术信息安全管理体系要求》

（十三）GB/T 22081-2016《信息技术安全技术信息安全管理实用规则》

（十四）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》

（十五）GB/Z 24364-2009《信息安全技术信息安全风险管理指南》

（十六）YY/T 0287-2003《医疗器械质量管理体系用于法规的要求》

（十七）YY/T 0316-2016《医疗器械风险管理对医疗器械的应用》

（十八）YY/T 0664-2008《医疗器械软件软件生存周期过程》

（十九）YY/T 1474-2016 《医疗器械可用性工程对医疗器械的应用》

（二十）FDA, Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software, 2005-1-14

（二十一）FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, 2014-10-2

（二十二）FDA, Radio Frequency Wireless Technology in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, 2013-8-14

（二十三）FDA, Postmarket Management ofCybersecurity in Medical Devices – Draft Guidance for Industry and Food and Drug Administration Staff, 2016-1-22

（二十四）FDA, Design Considerations and Pre-market SubmissionRecommendations for InteroperableMedical Devices – Draft Guidance for Industry and Food and Drug Administration Staff, 2016-1-26

（二十五）IEC 60601-1Edition3.1:2012, Medical electrical equipment - Part 1: General requirements for basic safety and essential performance

（二十六）IEC 82304-1, Health Software - Part 1: General

requirements for product safety

（二十七）IEC80001-1:2010, Application of risk management for IT-networks incorporating medical devices - Part 1: Roles,responsibilities and activities

（二十八）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

（二十九）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

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

（三十一）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

（三十二）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

（三十三）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

（三十四）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

（三十五）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

（三十六）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

（三十七）ISO/DIS 27799Health informatics - Information security management in health using ISO/IEC 27002

（三十八）HIMSS/NEMA HN 1-2013, Manufacturer Disclosure Statement for Medical Device Security

（三十九）NEMA/MITA CSP 1-2016, Cybersecurity for Medical Imaging

（四十）IMDRF/SaMD WG/N12FINAL:2014, Software as a Medical Device (SaMD): Possible Framework for Risk Categorization and Corresponding Considerations, 2014-9-18