医疗器械网络安全注册技术审查指导原则解读

国家食药监总局医疗器械技术审评中心

审评一部 彭亮

成都 2017.11

内容摘要

- 背景介绍
- 主要内容
- 实施要求

制定背景

- 医疗器械行业发展趋势
- 中国网络安全国家战略
- 国际医疗器械网络安全监管要求

制定背景

- 医疗器械具备网络连接功能日益普遍，在提高医疗服务质量和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、使用者伤害或死亡
- 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，风险相对较高，因此需要加强监管工作

制定原则

- 定位
  - 网络安全是安全有效性的重要组成部分
  - 网络安全指导原则作为软件指导原则的补充，适用范围略小于软件指导原则
- 基本原则
  - 风险管理、质量管理和信息安全工程相结合
  - 技术能力与法规要求相结合
  - 国际接轨与中国国情相结合

主要内容

- 指导原则目录
- 适用范围
- 关注重点
- 医疗器械网络安全
- 医疗器械数据
- 医疗器械网络安全能力
- 现成软件网络安全
- 医疗器械网络安全更新

指导原则目录

适用范围

- 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注册申报
  - 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
- 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
- 产品包括境内、进口产品，注册方式包括产品注册、许可事项变更、延续注册

关注重点

- 防护层级
  - 产品级：医疗器械产品自身
  - 系统级：医疗信息技术网络
- 保证措施
  - 管理措施：如使用规范等
  - 物理措施：如防盗措施等
  - 技术措施：如加密技术等
- 关注重点
  - 以医疗器械数据安全为核心关注产品级的技术保证措施

医疗器械网络安全

- 医疗器械网络安全是指保持医疗器械相关数据的保密性、完整性和可得性
  - 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
  - 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
  - 可得性（可用性）：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

医疗器械网络安全

- 注意事项
  - 保密性、完整性、可得性相互制约
  - 应结合预期用途、使用环境、核心功能以及相连设备的情况来确定医疗器械产品的网络安全特性
  - 其它特性：真实性、可核查性、抗抵赖、可靠性

医疗器械数据

- 健康数据
  - 标明生理、心理健康状况的私人数据（又称个人数据或敏感数据，指可用于人员身份识别的相关信息）
  - 健康数据涉及患者隐私信息，应遵循患者隐私保护相关法律法规的规定
- 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
  - 设备数据本身不涉及患者隐私信息，应保证其与健康数据的有效隔离

医疗器械数据交换方式

- 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
  - 考虑网络（如接口、带宽、无线电管理）、数据传输协议（是否为标准协议）、远程控制（是否为实时控制）等要求
- 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
  - 考虑数据储存格式（是否为标准格式）等要求

医疗器械网络安全能力

- 识别、防护
  - 用户访问控制机制
  - 可采用加密、数字签名、标准协议、校验等技术
- 探测、响应、恢复
  - 可采用防火墙、入侵检测和恶意代码防护等技术
- 网络安全能力建设
  - 医疗器械对于网络安全威胁应具备必要的识别、保护能力和适当的探测、响应、恢复能力
  - 可参考IEC/TR 80001-2-2等标准和技术报告

医疗器械网络安全能力

- 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）
- 传输完整性（TXIG）

医疗器械网络安全能力

- 自动注销
  - 未授权用户不能在无人值守的工作节点上访问**健康数据**
- 审核控制
  - 记录和追踪**健康数据**的访问、修改、删除情况
- 授权
  - 避免未授权访问数据和功能，保证网络安全和预期用途
- 安全特性配置
  - 本地IT管理员能够选择是否使用产品的网络安全能力

医疗器械网络安全能力

- 网络安全产品升级
  - 根据法规要求尽快安装第三方安全补丁
- 健康数据身份信息去除
  - 产品能够去除**健康数据**的患者身份信息
- 数据备份与灾难恢复
  - 保证健康数据在系统发生故障后能够恢复使用
- 紧急访问
  - 临床用户在紧急情况下能够无需认证而访问**健康数据**

医疗器械网络安全能力

- 健康数据完整性与真实性
  - 保证健康数据未经创建人许可而被篡改
- 恶意软件探测与防护
  - 能够探测已知恶意软件和未经授权即与产品互动的软件
- 网络节点鉴别
  - 能够识别设备帐号，保护**健康数据**的访问
- 人员鉴别
  - 基于访问控制机制创建用户独有帐号和角色，控制和监控网络访问和活动

医疗器械网络安全能力

- 物理锁
  - 保证存储于产品或者媒介的**健康数据的**安全，且安全程度与数据的敏感性和体量相匹配
- 第三方组件维护计划
  - 供应商应在产品生命周期中对系统进行维护/支持
- 系统与应用软件硬化
  - 调整安全控制措施，在实现预期用途的同时保证安全的最大化和维护的最小化
- 安全指导
  - 不同用户均应有相应操作指南，以明确职责和操作方法

医疗器械网络安全能力

- 健康数据存储保密性
  - 采用加密技术保证存储于产品或媒介的**健康数据**的安全
- 传输保密性
  - 在经认证的节点之间传输**健康数据**
- 传输完整性
  - 保证传输过程维系**健康数据**的完整性

现成软件网络安全

- 现成软件类型
  - 应用软件：成品软件、遗留软件、外包软件
  - 系统软件、支持软件
- 关注重点
  - 应用软件：重点关注其网络安全问题对医疗器械临床应用的影响
  - 系统软件、支持软件：重点关注安全补丁更新对医疗器械的影响

医疗器械网络安全更新

- 更新类型
  - 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，如常规安全补丁（属于设计变更）
- 监管要求
  - 重大网络安全更新：许可事项变更
  - 轻微网络安全更新：通过质量管理体系进行控制，无需进行许可事项变更，待到下次注册（许可事项变更、延续注册）时提交相应注册申报资料

医疗器械网络安全更新

- 注意事项
  - 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
  - 软件版本命名规则应考虑网络安全更新的情况

实施要求

- 实施过渡期
- 注册申报要求
- 网络安全文档
- 制造商实施要求

实施过渡期

- 过渡期
  - 网络安全指导原则于2017.1.20发布，将于2018年1月1日正式施行
- 申报要求
  - 过渡期：制造商应当结合网络安全指导原则的要求做好相应准备工作，同时可以自主决定是否按照网络安全指导原则的要求提交相应注册申报资料
  - 正式实施：制造商应当按照网络安全指导原则的要求提交相应注册申报资料

注册申报要求

- 产品注册
- 许可事项变更
- 延续注册

产品注册

- 软件研究资料
  - 单独提交网络安全描述文档
- 产品技术要求
  - 数据接口：传输协议/存储格式
  - 用户访问控制：用户身份鉴别方法、用户类型及权限
- 说明书
  - 运行环境：硬件配置、软件环境、网络条件
  - 安全软件：杀毒软件、防火墙，更新要求
  - 数据与设备（系统）接口
  - 用户访问控制机制

许可事项变更

- 软件研究资料
  - 涉及重大网络安全更新：单独提交网络安全描述文档
  - 仅发生轻微网络安全更新：单独提交常规安全补丁描述文档
  - 未发生网络安全更新：出具真实性声明
- 产品技术要求
  - 如适用体现网络安全的变更内容
- 说明书
  - 如适用体现网络安全的变更内容

延续注册

- 产品分析报告第（六）项
  - 如适用单独提交一份常规安全补丁描述文档

网络安全文档

- 网络安全描述文档
  - 内容包括基本信息、风险管理、验证与确认、维护计划
  - 适用于首次注册、重大网络安全更新
- 常规安全补丁描述文档
  - 内容包括情况说明、测试计划与报告、新增已知剩余缺陷情况说明
  - 适用于轻微网络安全更新

网络安全描述文档

- 基本信息
  - 类型：健康数据、设备数据
  - 功能：电子数据交换、远程控制
  - 用途：如临床应用、设备维护等
  - 交换方式：网络及要求，存储媒介及要求；对于专用无线设备，应提交符合无线电管理规定的证明材料
  - 安全软件：描述安全软件的名称、型号规格、完整版本、供应商、运行环境要求
  - 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

网络安全描述文档

- 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

网络安全描述文档

- 验证与确认
  - 提供网络安全测试计划和报告、网络安全可追溯性分析报告
  - 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，提供标准符合性证明材料；对于自定义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

网络安全描述文档

- 维护计划
  - 提供软件（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

常规安全补丁描述文档

- 软件（含现成软件）常规安全补丁情况说明
  - 补丁描述、影响分析、用户告知计划
- 回归测试计划与报告
- 新增已知剩余缺陷情况说明
  - 证明新增风险均是可接受的

制造商责任

- 制造商应当在医疗器械全生命周期过程（包括设计开发、生产、分销、部署、维护）中保证医疗器械产品自身的网络安全
- 制造商应当在医疗器械产品注册申请中提交相应网络安全注册申报资料，以证明医疗器械产品的安全性和有效性

制造商实施要求

- 制造商应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其网络安全，包括上市前和上市后的要求。制造商还可采用信息安全领域良好工程实践来完善医疗器械产品的网络安全管理
- 制造商应结合医疗器械产品的预期用途、使用环境、核心功能以及相连设备（系统）的情况来确定其网络安全特性，并采用基于风险管理的方法保证其网络安全

制造商实施要求

- 制造商应结合医疗器械数据的类型、功能、用途、交换方式及要求来考虑医疗器械产品网络安全问题。对于健康数据，制造商应当遵循患者隐私保护相关法律法规的规定；对于设备数据，制造商应当保证其与健康数据的有效隔离
- 制造商应根据医疗器械的产品特性考虑其网络安全能力的要求，保证医疗器械产品对于网络安全威胁具备必要的识别、保护能力和适当的探测、响应、恢复能力

制造商实施要求

- 制造商应重视现成软件的网络安全问题，结合质量管理体系的要求和现成软件的类型，采用基于风险管理的方法保证现成软件的网络安全
- 制造商应区分医疗器械网络安全更新的类型，根据网络安全更新对于医疗器械产品的影响程度，结合质量管理体系的要求开展相应质量保证工作，并按网络安全指导原则要求提交相应注册申报资料

制造商实施要求

- 制造商应遵循网络安全相关国家法律法规和部门规章的有关规定
  - 公安部、国家网信办、卫生计生委、工业和信息化部等
  - 《中华人民共和国网络安全法》、《人口健康信息管理办法（试行）》、《国家卫生计生委关于推进医疗机构远程医疗服务的意见》等

制造商实施要求

- 制造商可参考与网络安全相关的国际标准及技术报告的要求来保证医疗器械产品的网络安全，完善质量管理体系关于网络安全体系的要求
  - IEC 80001系列标准及技术报告、IEC 60601-1第三版、IEC 82304-1等
  - IEC 27000系列标准及技术报告、ISO/DIS 27799等

谢谢静听!

Q&A


医课汇
公众号
专业医疗器械资讯平台
WECHAT OF
HLONGMED
hlongmed.com
医疗器械咨询服务
MEDICAL DEVICE
CONSULTING
SERVICES
医课培训平台
医疗器械任职培训
WEB TRAINING
CENTER
医械宝
医疗器械知识平台
KNOWLEDG
ECENTEROF
MEDICAL DEVICE
MDCPP.COM
医械云专业平台
KNOWLEDG
ECENTEROF MEDICAL
DEVICE