国家药品监督管理局医疗器械技术审评中心
CENTER FOR MEDICAL DEVICE EVALUATION , NMPA

医疗器械网络安全、移动医疗器械审评指导原则解读

国家药监局器审中心 彭亮

2019.8 北京

内容摘要

- 医疗器械网络安全指导原则
- 移动医疗器械指导原则

网络安全指导原则目录

- 前言
- 适用范围
- 基本原则
  - 数据考量
  - 技术考量
  - 现成软件
- 网络安全文档
  - 网络安全更新类型
  - 网络安全描述文档
  - 常规安全补丁描述文档
- 注册申报资料要求
- 参考文献

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
  - 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

基本原则

- 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
- 基本考量
  - 基于风险：资产、威胁、脆弱性
  - 全生命周期：质量体系、工程实践
  - 责任共享：制造商、用户、IT服务商
  - 法规关注：国家法律法规、部委规章

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：医疗器械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：医疗器械数据是准确和完整的，未被篡改
  - 可得性：医疗器械数据能以预期方式适时访问和使用
- 补充说明
  - 基于预期用途、使用场景、核心功能
  - 保密性、完整性、可得性相互制约，需平衡兼顾
  - 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、心理健康状况的个人数据
  - 涉及患者隐私信息，遵循患者隐私保护相关规定
- 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
  - 本身不涉及患者隐私信息，保证与健康数据的有效隔离

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
  - 建议参考IEC/TR 80001-2-2、HIMSS/NEMA HN-1开展风险管理、验证与确认工作

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）
- 远程访问

医疗器械网络安全能力

- 自动注销
  - 自动注销、自动锁定、密码屏保
- 审核控制
  - 记录和追踪用户操作行为
- 授权
  - 用户账号与密码
- 安全特性配置
  - 网络安全特性可配置
- 网络安全产品升级
  - 网络安全补丁安装

医疗器械网络安全能力

- 健康数据身份信息去除
  - 去除患者身份信息、匿名化
- 数据备份与灾难恢复
  - 数据备份、数据恢复
- 紧急访问
  - 用户紧急情况可无需认证即可访问数据，但需记录
- 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
  - 安全软件兼容性

医疗器械网络安全能力

- 网络节点鉴别
  - 网络节点认证
- 人员鉴别
  - 设备鉴别用户的能力
- 物理锁
  - 物理访问限制措施
- 第三方组件维护计划
  - 产品生命周期对于第三方组件的维护要求
- 系统与应用软件硬化
  - 网络端口禁用、未授权软硬件安装限制

医疗器械网络安全能力

- 安全指导
  - 不同用户均应有相应操作指南
- 健康数据存储保密性
  - 数据加密
- 传输保密性
  - 点对点传输、数据加密
- 传输完整性
  - 数据加密、校验码
- 远程访问
  - 远程访问、远程维护

现成软件网络安全

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

网络安全更新

- 更新类型
  - 重大网络安全更新
  - 轻微网络安全更新，如常规安全补丁
- 监管原则
  - 重大网络安全更新：许可事项变更
  - 轻微网络安全更新：无需注册变更，待下次注册时提交
  - 遵循风险从高原则
  - 软件版本命名规则应考虑网络安全更新的情况

申报要求

- 注册形式
  - 产品注册
  - 许可事项变更
  - 延续注册
- 文档形式
  - 网络安全描述文档
  - 常规安全补丁描述文档

- 软件研究资料
  - 单独一份提交网络安全描述文档
  - 软件版本命名规则应当涵盖网络安全的情况
- 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

- 变更情况声明
  - 软件版本命名规则应当涵盖网络安全的情况
- 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
- 产品技术要求与说明书
  - 如适用体现网络安全的变更内容

延续注册

- 产品未变化声明
  - 软件版本命名规则应当涵盖网络安全的情况
- 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
- 无需提交网络安全描述文档

文档形式

- 网络安全描述文档
  - 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
  - 情况说明、测试计划与报告、新增剩余缺陷情况说明
  - 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
- 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；安全软件提供兼容性测试报告；标准传输协议提供符合性证明材料，自定义传输协议提供完整性测试总结报告；实时远程控制提供完整性和可得性测试报告
- 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

- 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
- 新增剩余缺陷情况说明
  - 证明新增风险均是可接受的

常见问题

- 首次许可事项变更需提交网络安全描述文档
- 基本信息未围绕数据进行描述
- 风险管理、验证与确认未与网络安全能力建立关系
- 对部分网络安全能力理解有误
- 验证与确认未含可追溯性分析报告
- 维护计划未含网络安全事件应急响应预案
- 软件版本命名规则未涵盖网络安全情况

移动器械指导原则目录

- 前言
- 适用范围
- 移动医疗器械
- 基本原则
- 技术考量
- 注册申报资料要求
- 参考文献

适用范围与基本原则

- 适用范围
  - 适用于移动医疗器械的注册申报，包括第二、三类医疗器械
- 基本原则
  - 移动医疗器械 = 医疗器械 + 移动计算技术
  - 综合考虑等效传统医疗器械、移动计算技术的风险
  - 移动计算技术风险包括但不限于显示屏尺寸小、分辨率低、亮度低，受环境光影响大，电池容量小，数据传输失真等

移动医疗器械

- 定义
  - 采用无创“移动计算终端”实现一项或多项医疗用途的设备和/或软件
  - 移动计算终端：供个人使用的移动计算技术产品终端，包括通用（商业现成）终端和专用（自制医用）终端
  - 使用形式：手持式、穿戴式、混合式
- 补充说明
  - 移动医疗器械含有医疗器械软件（移动App）
  - 植入和侵入医疗器械如采用移动计算终端参考使用

移动医疗器械类型

- 移动医疗设备
  - 采用通用或专用移动计算终端实现一项或多项医疗用途的设备，即**移动App+传感器**
- 移动独立软件
  - 采用通用移动计算终端（含外观改装）实现一项或多项医疗用途的独立软件，即**移动App**
- 移动医疗附件
  - 采用通用或专用移动计算终端控制医疗器械运行（即控制型）或与医疗器械进行电子数据交换（即数据型）的设备或软件，即**移动App+医疗器械**

移动医疗器械判定原则

- 基本原则
  - 凡符合医疗器械定义的移动计算设备或软件属于移动医疗器械，必要时申请分类界定
- 判定要素
  - 预期用途：健康管理、疾病管理
  - 目标人群：健康人群、医护人员、患者
  - 核心功能：健康信息记录统计、医疗器械控制驱动、医疗数据处理分析监测

技术考量

- 网络安全能力
  - 自动清除、加密技术，需性能验证
- 显示屏限制
  - 屏幕尺寸、分辨率、亮度，需性能验证、临床评价
- 环境光影响
  - 环境光检测、亮度矫正，需性能验证、临床评价
- 电池容量限制
  - 电池续航能力、剩余电量提示，需性能验证

技术考量

- 注册信息用户确认
  - 患者使用（特别是在家庭环境使用）的移动医疗器械若有用户界面应具备产品注册信息用户确认功能
- 开机自检
  - 采用通用终端的移动医疗器械（特别是移动独立软件）应具备运行环境开机自检功能
- 专用终端
  - 若为无线设备应符合无线电管理的相关规定
- 穿戴计算技术
  - 除移动计算技术风险之外还应考虑可用性、可靠性

云计算服务

- 云计算服务
  - 服务模式：软件即服务、平台即服务、基础设施即服务
  - 部署模式：私有云、公有云、社区云、混合云
- 监管原则
  - 云计算服务视为现成软件
  - 云服务商视为医疗器械供应商
- 自建云计算平台
  - 制造商应遵循云服务商的规定
  - 申报资料参照自主开发独立软件和云计算服务的要求

云计算服务申报资料

- 基本信息
  - 云计算的名称和配置，云服务商的名称、住所和资质
- 技术要求
  - 服务与部署模式、核心功能、数据接口、网络安全能力
- 风险管理
- 验证与确认
- 维护计划
- 云计算服务协议
  - 网络安全保证、患者数据与隐私保护、数据残留处理

移动医疗设备申报要求

- 参照移动器械指导原则、软件指导原则、网络安全指导原则、等效传统医疗器械指导原则（如有）
- 风险管理应当综合考虑等效传统医疗器械的风险以及移动计算终端的风险
- 产品技术要求应当包含等效传统医疗器械适用的性能指标、移动计算终端的性能指标
- 临床评价可选取等效传统医疗器械进行实质等同对比
- 说明书应当明确移动计算终端的性能指标和使用方法
- 若采用云计算服务提交响应注册申报资料

移动独立软件申报要求

- 参照移动器械指导原则、软件指导原则、网络安全指导原则、传统独立软件指导原则（如有）
- 若采用云计算服务提交响应注册申报资料

移动医疗附件申报要求

- 控制型移动医疗附件
  - 随医疗器械产品整体注册
  - 根据移动器械指导原则的适用要求，补充性能指标并提供验证资料
- 数据型移动医疗附件
  - 随医疗器械产品整体注册则参照控制型移动医疗附件
  - 单独注册则参照移动医疗设备或移动独立软件

常见问题

- 对移动医疗器械的理解有误
- 未结合预期用途、使用场景、核心功能来识别移动计算技术的风险
- 对云计算服务的理解有误

国家药品监督管理局医疗器械技术审评中心
CENTER FOR MEDICAL DEVICE EVALUATION , NMPA

中国器审

谢谢！

WWW.CMDE.ORG.CN

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