新版《医疗器械网络安全注册技术审查指导原则》解读

傅赛珍 | Cindy
Email: fsz@cirs-group.com

Protecting your health and beautifying your life

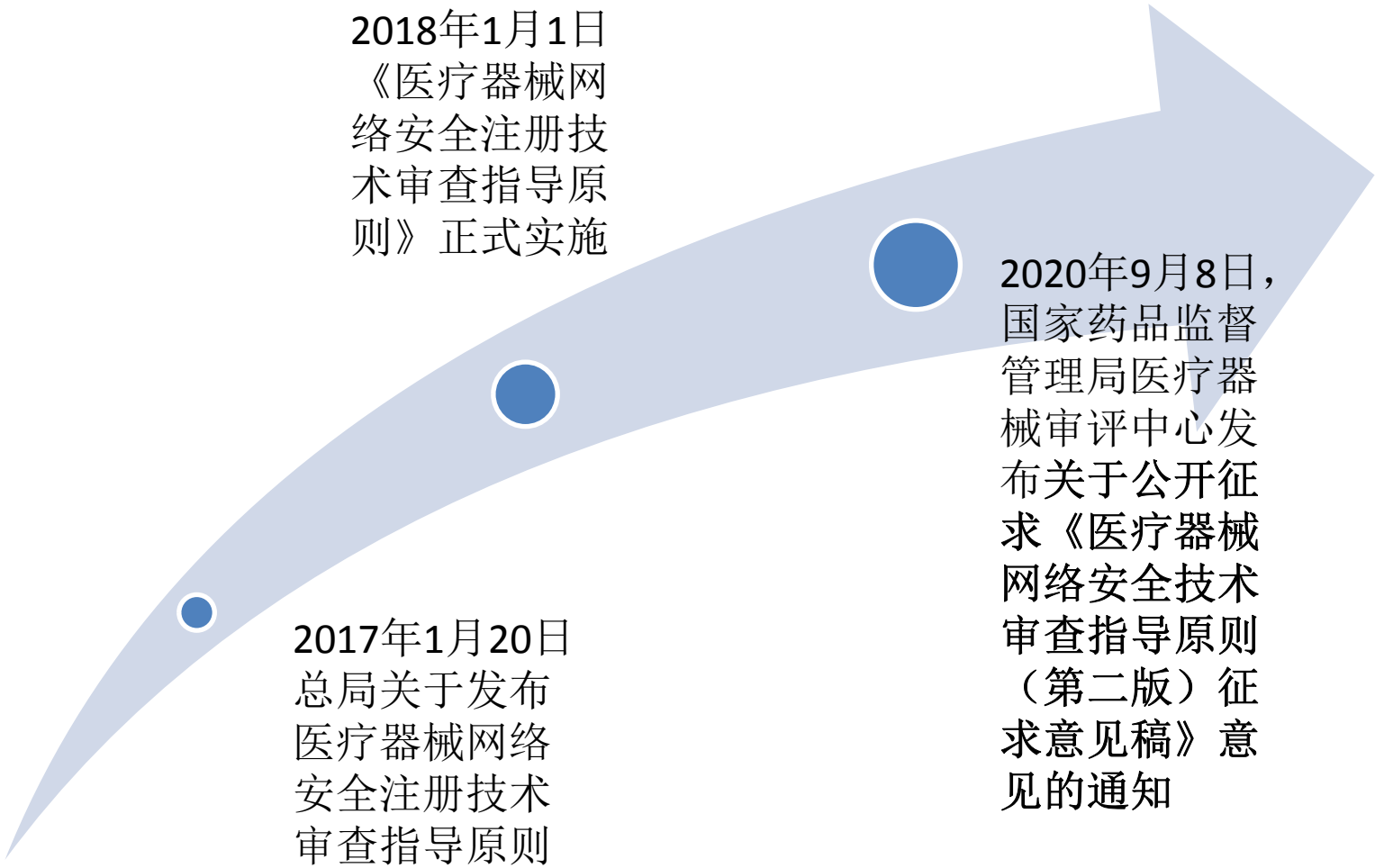
CIRS Group

目录

- 指导原则（征求意见稿）简介及与现行版的对比
- 医疗器械网络安全的要求
- 医疗器械企业应对方案
- 网络安全注册资料要求

1.指导原则简介

1.1网络安全法规发展路径



2017年1月20日
总局关于发布
医疗器械网络
安全注册技术
审查指导原则
的通告（2017
年第13号）

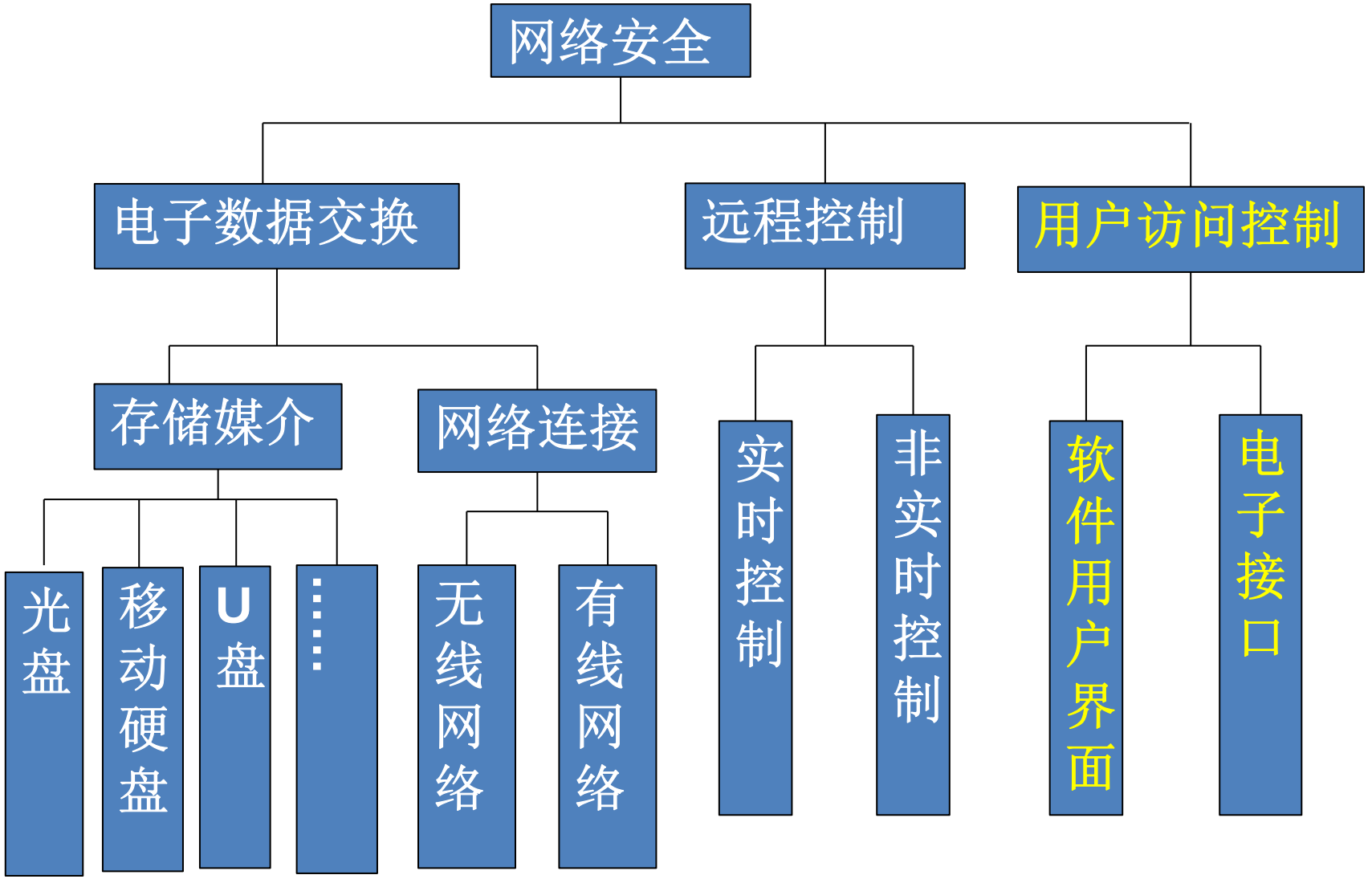
2018年1月1日
《医疗器械网
络安全注册技
术审查指导原
则》正式实施

2020年9月8日，
国家药品监督
管理局医疗器
械审评中心发
布关于公开征
求《医疗器械
网络安全技术
审查指导原则
（第二版）征
求意见稿》意
见的通知

1.2适用范围对比

第一版	第二版
具有网络连接功能以进行电子数据交换或远程控制、以及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。 网络：无线、有线网络， 电子数据交换：单向、双向数据传输， 远程控制：实时、非实时控制。 存储媒介：包括但不限于光盘、移动硬盘和U盘。	具备电子数据交换、远程控制或用户访问功能的第二、三类独立软件和含有软件组件的医疗器械。 网络：无线、有线网络， 电子数据交换：基于网络、存储媒介的单向、双向数据传输， 远程控制：基于网络的实时、非实时控制， 用户访问：基于软件用户界面（含独立软件、软件组件）、电子接口（含网络接口、电子数据交换接口）的人机交互方式。

1.3网络安全涉及的范围



2.医疗器械网络安全的要求

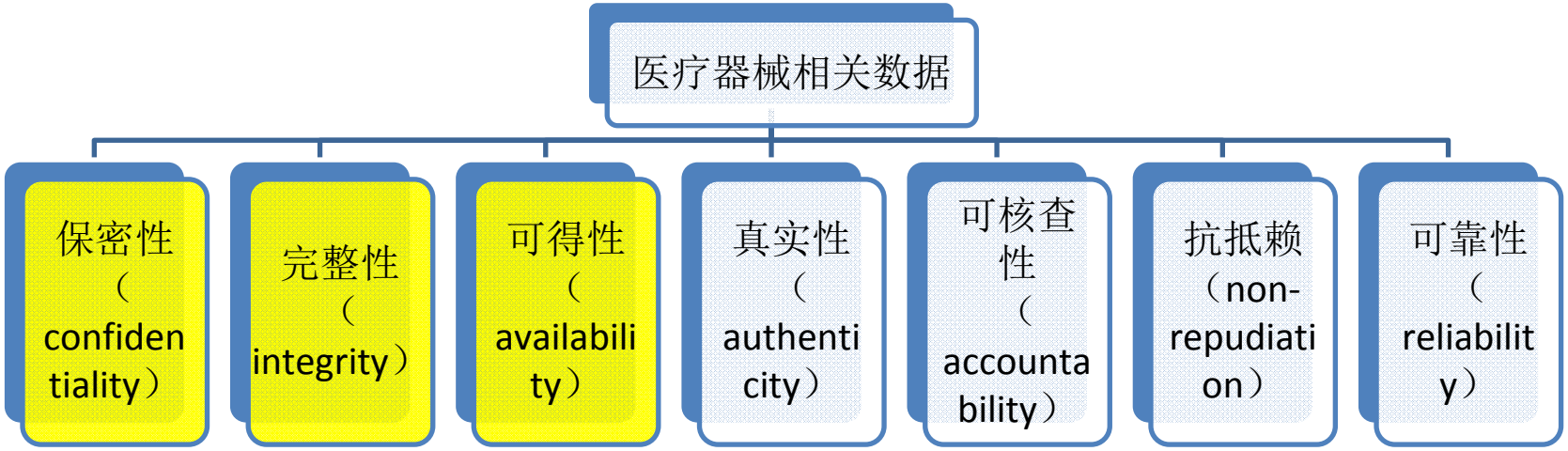
2.1网络安全法规依据
2.2网络安全基本概念
2.3网络安全能力
2.4网络安全事件应急响应
2.5网络安全更新
2.6网络安全风险
2.7网络安全技术考量

2.1实施网络安全管理的法规依据

序号	法规名称	备注
1	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）	
2	**中华人民共和国数据安全法（草案）（全国人大，2020.7）**	
3	**国家网络安全事件应急预案（中央网信办，2017.10）**	
4	个人信息出境安全评估办法（征求意见稿）（国家互联网信息办公室，2019.6）	
5	人口健康信息管理办法（试行）（国卫规划发〔2014〕24号）	
6	**DB32/T 3769-2020《医疗器械网络连接通用技术规范》**	江苏省地标

2.2网络安全基本概念

2.2.1医疗器械网络安全



保密性

•指~~数据~~信息不能被未授权的~~个人、~~实体（含个人、组织）~~利用~~获得或知悉的特性，即医疗器械产品自身和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和使用。

完整性

•指信息的创建、传输、存储、显示未以非授权方式进行更改（含删除、添加）的特性，~~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）~~

•指信息可根据授权~~个人、~~实体的要求可访问和使用的特性，即医疗器械产品自身和相关数据能以预期方式适时进行访问和使用。

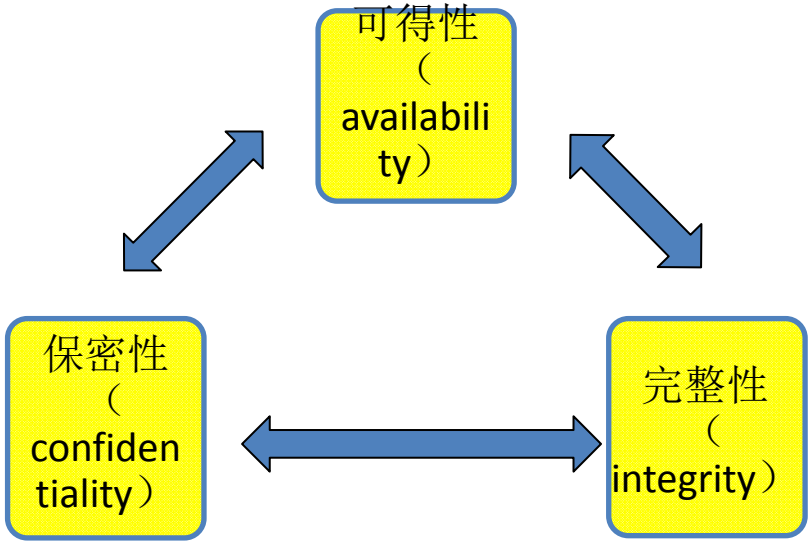
2.2.1医疗器械网络安全

真实性
- 是指实体符合其所声称的特性，

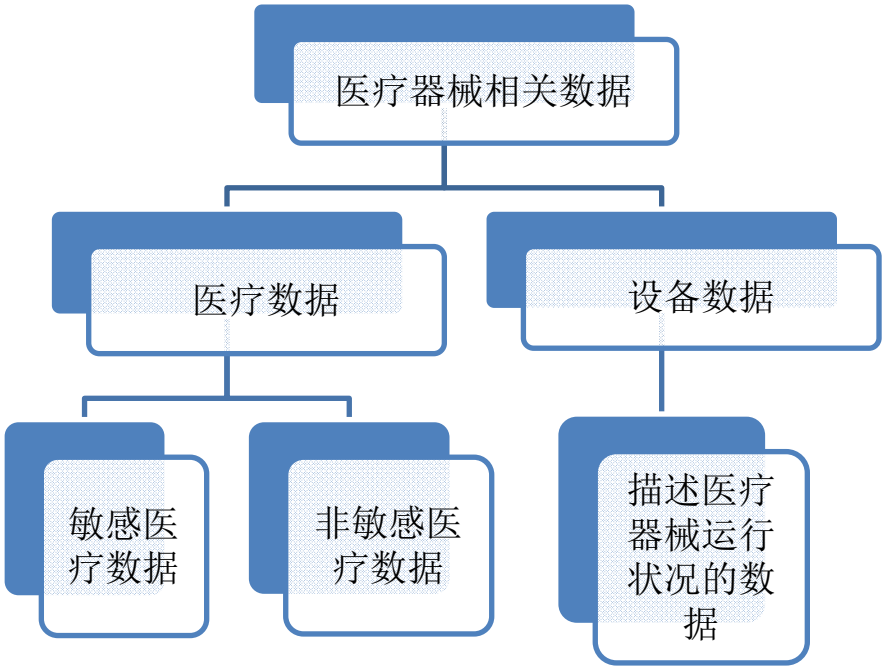
抗抵赖性
- 是指实体可证明所声称事件或活动的发生及其发起实体的特性，

可核查性
- 是指实体的活动及结果可被追溯的特性，

可靠性
- 是指实体的活动及结果与预期保持一致的特性。



2.2.2医疗器械相关数据



注册人应基于医疗器械相关数据的类型、功能、用途，结合网络安全特性考虑医疗器械数据安全要求。同时，保证敏感医疗数据所含个人信息免于泄露、滥用和篡改，以及医疗数据和设备数据的有效隔离。

敏感医疗数据/非敏感医疗数据

- 是指含有个人信息的医疗数据，反之即为非敏感医疗数据。

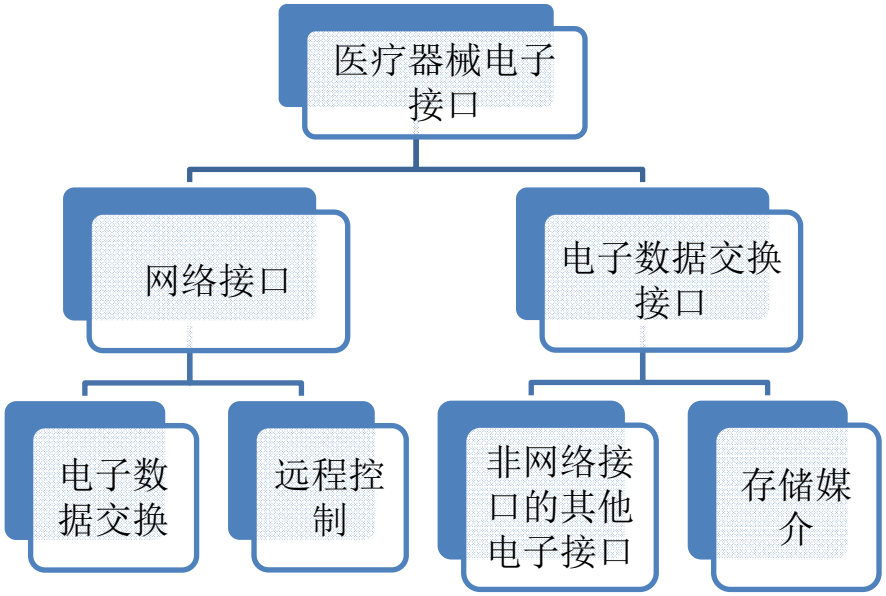
个人信息

- 是指能够单独或与其他信息结合识别特定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

- 是指描述医疗器械运行状况的数据，用于监视、控制医疗器械运行或用于医疗器械的维护维修，不应含有个人信息。

2.2.3电子接口



网络接口

- 是指医疗器械通过网络进行电子数据交换或远程控制，包括但不限于网络形式（有线、无线）、物理接口（如电口、光口）、数据接口（标准协议、私有协议）、远程控制方式（实时、非实时）、性能指标（如端口、传输速率、带宽）等。无线网络包括Wi-Fi（IEEE 802.11）、蓝牙（IEEE 802.15）、无线电、射频、红外等形式，
- 远程控制包括系统软件所提供的运程桌面功能。

电子数据交换接口

- 是指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）或存储媒介（如光盘、移动硬盘、U盘）

数据存储的技术特征要求

- 包括但不限于存储媒介形式、文件储存格式（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。

2.3网络安全能力

- **自动注销 :**产品在使用闲置期间阻止非授权用户访问和使用的能力。
- **审核控制:**产品提供用户活动可被审核的能力。
- **授权 :**产品确定用户已获授权的能力。
- **网络安全特性配置 :**产品根据用户需求配置网络安全特征的能力。
- **网络安全补丁升级：**授权用户或服务人员安装/升级网络安全补丁的能力。
- **数据去标识化 ：**产品直接去除或匿名化数据所含个人信息的能力。
- **数据备份与灾难恢复 ：**产品的数据、硬件或软件受到损坏或破坏后恢复的能力。
- **紧急访问：**产品在预期紧急情况下允许用户访问和使用的能力。
- **数据完整性与真实性：**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。

2. 3网络安全能力

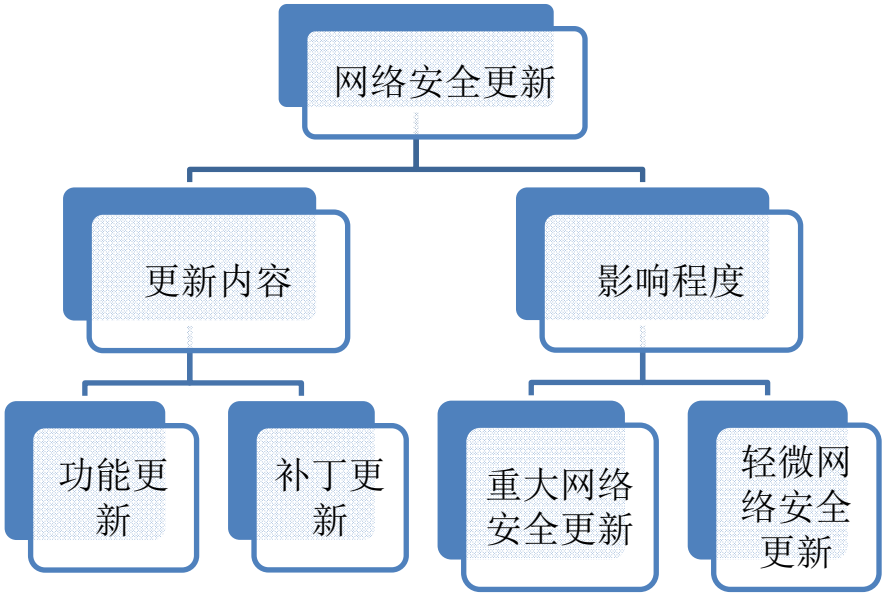
- **恶意软件探测与防护：**产品有效探测、阻止恶意软件的能力。
- **节点鉴别：**产品鉴别网络节点的能力。
- **人员鉴别：**产品鉴别授权用户的能力。
- **物理防护：**产品提供防止非授权用户访问和使用的物理防护措施的能力。
- **现成软件维护：**产品在全生命周期中对现成软件提供网络安全维护的能力。
- **系统固化：**产品通过固化措施对网络攻击和恶意软件的抵御能力。
- **网络安全指导：**产品为用户提供网络安全指导的能力。
- **存储数据存储保密性：**产品确保数据传输保密性和完整性的能力。
- **远程访问与控制：**产品确保用户远程访问与控制的网络安全的能力。
- **抗拒绝服务攻击：**产品具有抗拒绝服务攻击的能力。

注册人应根据医疗器械的产品特性分析上述网络安全能力的适用性。

2. 4网络安全事件应急响应

- **网络安全事件应急响应预案要求：**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。
- 根据网络安全事件的严重程度、紧迫程度、广泛程度等因素进行分类分级管理，结合风险管理开展应急响应措施的验证工作并予以记录，在事件发生期间及时告知用户应对措施。
- 造成严重后果或影响的事件应向药监部门报告，适用时按照医疗器械不良事件、召回相关法规要求处理，必要时向国家网络安全主管部门报告。

2. 5网络安全更新



涉及召回的网络安全更新均属于重大网络安全更新。

网络安全更新同样遵循风险从高原则。同时，软件版本命名规则应涵盖网络安全更新情况，区分重大和轻微网络安全更新。

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

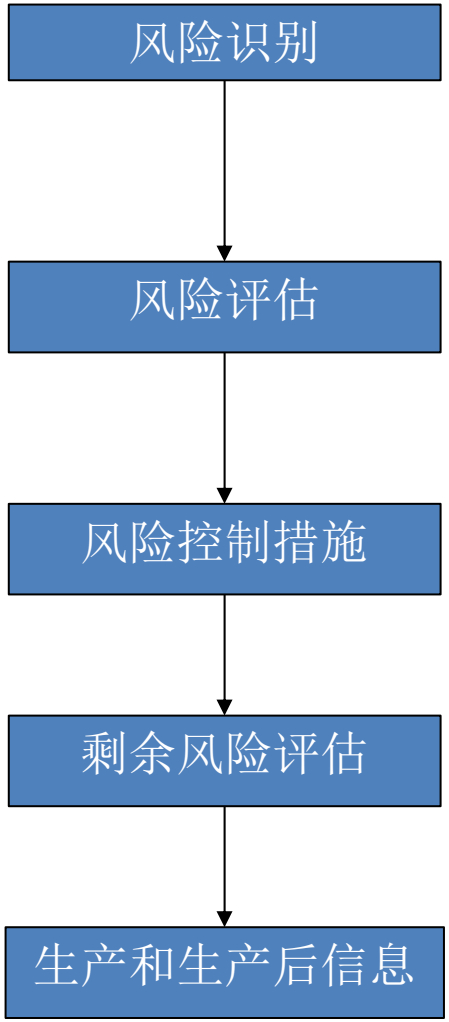
包括但不限于：产品所处网络环境发生改变，如由封闭网络环境变为开放网络环境、局域网变为广域网、有线网络变为无线网络；电子接口发生改变，如接口形式由网口变为USB口、接口数量由少变多、接口功能由电子数据交换扩至远程控制等。

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。

网络环境、电子接口的数据传输效率单纯提高，电子接口原有功能单纯优化；医疗器械软件、必备软件（医疗器械软件正常运行所必需的其他医疗器械软件、医用中间件）、外部软件环境（医疗器械软件正常运行所必需的系统软件、通用应用软件、通用中间件、支持软件）的网络安全补丁更新。

2. 6网络安全风险管理



- **资产Asset：** 对个人或组织有价值的物理和数字实体
- **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
- **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和患者的影响以及被利用的可能性，确定风险水平

采取充分、有效、适宜的风险控制措施，以减低原有风险对产品安全有效性的影响

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

2.7网络安全技术考量

2. 7.1现成软件

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

注册人工作

注册人应根据质量管理体系要求建立现成软件网络安全更新维护过程，及时将现成软件网络安全相关信息以及应对措施告知用户。

2. 7.2医疗数据出境

1.在中国境内收集和产生的个人信息和重要数据应当在中国境内存储，因业务需要确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

2.不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。

2. 7.3远程维护

1. 远程维护功能：远程访问和使用设备数据，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。

2.远程维护所用电子接口：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。

3.医疗器械在远程维护过程中若无人值守，则可能存在医疗器械非授权访问和使用的风险。

注册人工作

注册人应明确远程维护的实现方法、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、维护过程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。

2. 7.4陈旧设备

1.陈旧设备：指不能通过补丁更新、补偿控制等合理风险控制措施抵御当前网络安全威胁的医疗器械。

2.陈旧设备应尽快停运退市。

3.陈旧设备判定：医疗器械停售、停止售后服务。

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陈旧设备，反之不属于陈旧设备；停止售后服务的医疗器械均为陈旧设备。

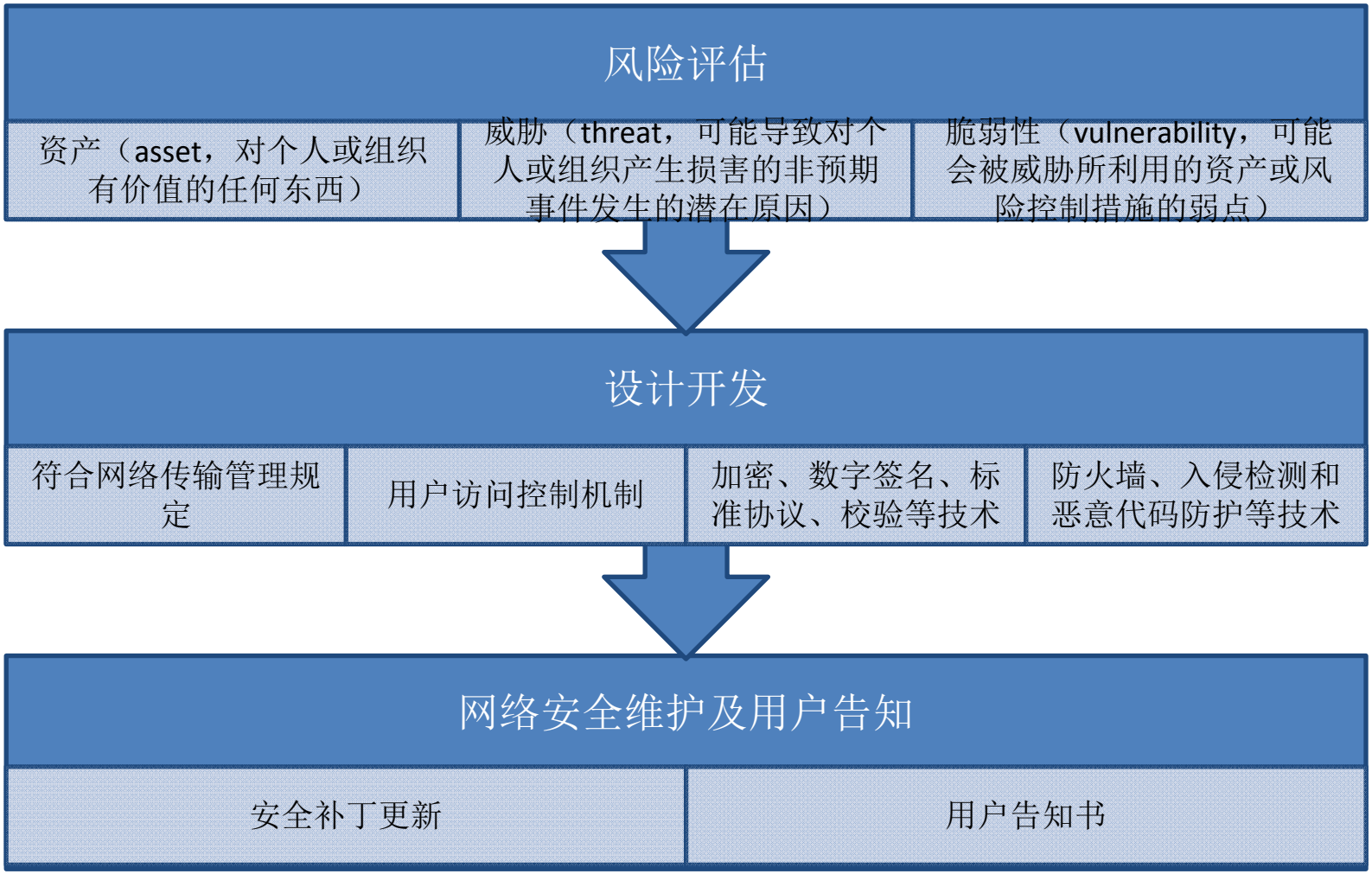
注册人工作

注册人应按照质量管理体系关于软件停运/软件退市的要求开展相应工作。

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。

3.医疗器械企业应对方案

3.1医疗器械网络安全应对总则



3.2技术规范

序号	标准名称	备注
1	GB/T 20271-2006《信息安全技术信息系统通用安全技术要求》	
2	GB/T 20984-2007 《信息安全技术信息安全风险评估规范》	
3	GB/T 22080-2016《信息技术安全技术信息安全管理体系要求》	
4	GB/T 22081-2016《信息技术安全技术信息安全管理实用规则》	
5	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》	
6	GB/Z 24364-2009《信息安全技术信息安全风险管理指南》	
7	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	
8	YY/T 1474-2016 《医疗器械可用性工程对医疗器械的应用》	

3.3设计开发关注重点

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

*来源：CMDE培训资料

3.4网络安全能力建设重点

•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

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

3.5网络安全能力确认

- 自动注销
- 审核控制
- 授权
- 网络安全特性配置
- 网络安全补丁升级
- 数据去标识化
- 数据备份与灾难恢复
- 紧急访问
- 数据完整性与真实性
- 恶意软件探测与防护
- 节点鉴别
- 人员鉴别
- 物理防护
- 现成软件维护
- 系统固化
- 网络安全指导
- 存储数据存储保密性
- 远程访问与控制
- 抗拒绝服务攻击

3.6漏洞评估

轻微级别：按照通用漏洞评分系统（CVSS）所定义的漏洞等级，明确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，按照CVSS漏洞等级明确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、影响、风险，确保风险均可接受。或提供第三方网络安全漏洞评估报告。

严重级别：提供境内第三方网络安全评估机构出具的网络安全漏洞评估报告，以及已知剩余漏洞的维护方案。

4.网络安全注册资料要求

4.1注册资料要求-首次注册

资料编号	资料名称	资料内容
5.1	产品性能研究	增加网络安全保障的相关研究资料
5.7	软件研究资料	自研/现成软件网络安全研究报告 外部软件环境评估报告
8	风险管理资料	增加网络安全相关的风险评估和控制工作
9	产品技术要求	要求见软件注册审查指导原则（第二版）征求意见稿
11.1	说明书	网络安全的相关说明： 1.明确用户访问控制机制 2.电子接口（含网口接口、电子数据交换接口）及其数据类型和技术特征 3.网络安全特征配置 4.数据备份与灾难恢复 5.运行环境（含硬件配置、外部软件环境、网络环境） 6.安全软件兼容性 7.外部软件环境与安全软件更新等要求。

4.2注册资料要求-许可事项变更

资料编号	资料名称	资料内容
1	软件研究资料	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）涉及网络安全功能更新：发生功能更新或合并补丁更新，提交自研/现成软件网络安全功能更新研究报告（或自研/现成软件网络安全研究报告）、外部软件环境评估报告； （2）仅发生网络安全补丁更新：提交自研软件网络安全补丁更新研究报告 （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。

4.3注册资料要求-延续注册

资料编号	资料名称	资料内容
延续注册无需提交网络安全相关研究资料。		
7	其他	若原注册产品标准（或原产品技术要求）及其变更对比表未体现软件相关信息，应在产品未变化声明中予以明确，其中软件版本命名规则涵盖网络安全更新情况。

4.4自研软件网络安全研究报告框架

条款		轻微	中等	严重
基本信息	软件信息	明确软件的基本情况和安全性级别		
	数据架构	提供每个使用场景的网络环境和数据流图，描述医疗器械相关数据和电子接口的基本情况		
	网络安全能力	逐项分析20项网络安全能力的适用情况		
	网络安全补丁	列明网络安全补丁的基本情况		
	安全软件	明确安全软件的基本情况		
实现过程	风险管理	提供网络安全的风险分析报告、风险管理报告		
	需求规范	提供网络安全需求规范文档		
	验证与确认	提供网络安全的测试计划和报告		
	可追溯性分析	提供网络安全可追溯性分析报告		
	更新维护计划	提供网络安全更新、远程维护的流程图及活动描述	提供网络安全更新、网络安全事件应急响应、远程维护的流程图及活动描述	
漏洞评估		按照漏洞等级明确已知漏洞总数和剩余漏洞数。	提供网络安全漏洞自评报告或第三方网络安全漏洞评估报告，按照漏洞等级明确已知漏洞总数和剩余漏洞情况	提供境内第三方网络安全评估机构出具的网络安全漏洞评估报告，以及已知剩余漏洞的维护方案。
结论		概述网络安全实现过程的规范性和网络安全漏洞评估结果，判定网络安全是否满足要求		

4.5自研软件网络安全更新研究报告

条款		轻微	中等	严重
基本信息	软件信息	明确申报版本软件情况，详述变化。		
	数据架构	明确申报版本软件情况，详述变化。		
	网络安全能力	明确申报版本软件情况，详述变化。		
	网络安全补丁	列明网络安全更新部分的补丁情况		
	安全软件	明确申报版本软件情况，详述变化。		
实现过程	风险管理	提供网络安全更新部分的风险分析报告、风险管理报告		
	需求规范	提供网络安全更新部分需求规范文档		
	验证与确认	提供网络安全更新部分的测试计划和报告		
	可追溯性分析	提供网络安全更新部分的可追溯性分析报告		
	更新维护计划	提供用户告知计划	提供用户告知计划、网络安全事件应急响应总结报告	
漏洞评估		明确申报版本软件已知漏洞总数和剩余漏洞数	提供申报版本软件的网络安全自评报告，明确已知漏洞总数和剩余漏洞情况	提供申报版本软件的境内第三方网络安全评估机构出具的网络安全漏洞评估报告
结论		概述网络安全更新实现过程的规范性和网络安全漏洞评估结果，判定网络安全更新是否满足要求		

4.6现成软件网络安全研究资料

使用方式	资料要求	资料内容
部分使用方式	对于部分使用方式，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、更新维护计划、漏洞评估、结论。
部分现成软件发生网络安全更新	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，说明现成软件的变化情况，不适用条款说明理由；	补丁更新要求与自研软件相同。
全部使用方式	需要单独提交现成软件组件网络安全研究报告	内容与自研软件研究报告相同。 但需基于现成软件（此时即医疗器械软件）的安全性级别予以说明。
全部现成软件发生网络安全更新	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，说明现成软件的变化情况，不适用条款说明理由	补丁更新要求与自研软件相同。

Thank You!

CIRS 瑞旭技术

地址：杭州市滨江区秋溢路288号东冠高新科技园1号楼11层
邮编：310052
邮箱：fsz@cirs-group.com