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。（法规要求）*

公司的体系文件规定了风险管理过程，按照YY/T 0316-2008 idt ISO14971:2007《医疗器械 风险管理对医疗器械的应用》与相关的控制程序，在产品和软件风险分析的基础上，根据《医疗器械网络安全注册技术审查指导原则》的要求，对网络安全进行风险管理评审。

风险管理报告见申报材料8 风险管理报告。

3.验证与确认

1. *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。*
2. *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。（法规要求）*

示例：1.网络安全测试

本公司对记录仪进行了网络安全测试，证实医疗器械产品的网络安全需求（保密性、完整性、可得性等特性）均已得到满足。具体见附件《记录仪网络安全测试报告》。

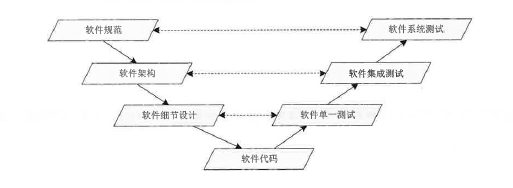
2.网络安全可追溯性分析

将网络安全设计规范和风险联系起来的可追踪性矩阵：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 网络安全风险序号 | 产品需求规范 | 网络安全设计规范 | 验证报告编号 | 方案编号 | 测试结果报告编号 |
|  |  |  |  |  |  |

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。（法规要求）*

示例：我司提供了网络安全风险更新的维护流程如下：

简述更新确认、用户告知。

5.网络安全事件应急响应预案

基于产品的特性，以及通过对十九项网络安全能力进行分析，传输数据为\*\*\*\*\*。

控制软件在现有的功能下，不会由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响，因此不涉及中华人民共和国互联网信息办公室发布的中网办发文〔2017〕4号《国家网络安全事件应急预案》相关内容。