医疗器械软件安全文档编制要点

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、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，也是国家网络安全的组成部分之一。

根据《医疗器械网络安全注册技术审查指导原则》，《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（包括境内、进口）的注册申报，适用的注册方式包括产品注册、许可事项变更、延续注册。注册人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，从而保证其安全性和有效性。注册人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。

医疗器械网络安全能力包括对网络安全威胁的识别、防护、探测、响应、恢复的能力。医疗器械对网络安全威胁应当具备相应识别、防护能力，而由于预期用途、使用环境的限制，医疗器械对网络安全威胁的探测、响应、恢复能力应当与其产品特性相适应。

对于属于应用软件的现成软件，应当重点关注其网络安全问题对医疗器械临床应用的影响。对于属于系统软件或支持软件的现成软件，应当重点关注安全补丁更新对医疗器械的影响。

医疗器械网络安全文档包括网络安全描述文档、常规安全补丁描述文档。

1.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，适用于产品注册、重大网络安全更新；

2.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。

注册人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，如 IEC80001 系列标准及技术报告、IEC 60601-1 第三版、IEC 82304-1、IEC 27000 系列标准及技术报告、ISO/DIS 27799 等。

下面为文件的具体模板：

目录

1.基本信息

1.1 类型

说明软件包含的数据类型。

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。

1.2 功能

软件进行电子数据交换的方式（单向、双向）、是否进行远程控制，控制的类型（实时、非实时）。

1.3 用途

医疗器械软件的用途，如：临床应用、设备维护等。

1.4 数据交换方式

l 交换方式：网络（无线网络、有线网络）产品通过存储媒介进行数据交换，这些存储媒介包括光盘、U 盘、移动硬盘等通用外接存储设备。

l 传输协议：传输的数据格式、容量等如：数据格式为 DICOM，外接存储设备容量不喧嚣与 4G。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；

1.5 安全软件

软件支持通用的安全软件（如 360 安全卫士、360 杀毒、qq 电脑管家、金山杀毒等），安全软件应是能够保证计算机系统安全的有效版本。产品运行环境如下：

目录

1.6 现成软件

软件名称	规格型号	完整版本	供应商	运行环境要求
Windows 7			微软	通用计算机
极速 PDF 阅读器			极速 PDF 阅读器	Win2000/WinXP/Win2003/Vista/Win7/Win8/Win10

2.风险管理

医疗器械网络安全风险分析报告见《风险分析报告》。

3.验证与确认

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。详见附件《网络安全测试报告》。

4.维护计划

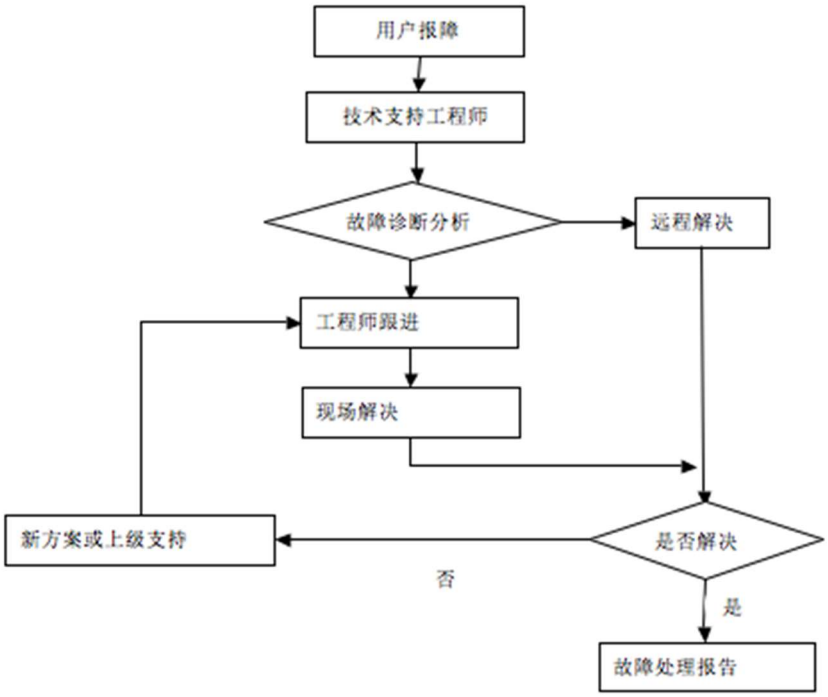
4.1 维护流程

由于软件的复杂性，一个看似很小地方的修正可能对全局系统产生重大影响。每当软件修正后，验证分析不仅要对此修正进行验证，还要确认此修正对整个软件系统的影响程度。同时涉及到该软件的修改，评审、验证和风险分析，软件修改前后的差别对比，新软件版本号，这

些都将形成文字记录。

公司制定《软件维护计划》、《BUG 管理规定》、《软件版本管理规定》对软件维护进行管理和控制，并按照《风险控制程序》对软件维护可能产生的风险进行分析和控制，以确保软件维护可能造成的风险可接受。

软件网络安全更新的维护流程如下：



流程说明

更新确认：

使用者因为各种原因需要对已经产生的数据进行修改，提出维护申请。维护范围只包括错误数据修正。

提出申请部门负责人需要对情况进行核实，并确认。

维护工程师（一般由软件开发组专人负责）接收到确认后的维护请求，分析并提出修改方案，并对软件更新可能产生的风险进行分析评价，必要时提出风险控制措施。

研发部负责人对方案进行审核，确保方案的安全性和正确性，并对可能产生的风险进行分析，必要时进行风险控制。根据维护所涉及产品的安全性和有效性的影响程度确定维护类型，确定软件维护符合法规要求。

如需要，对系统进行备份。（具体操作由方案确定）

如需要，对维护操作进行模拟验证。（具体操作由方案确定）

用户告知：

维护工程师（一般指方案提出者本人）按照方案进行修改操作。完成维护后，如果需要对用户软件需要更新，应通知用户软件进行了维护以及维护的主要内容。

维护申请提出用户对维护结果进行反馈和评价。

放射治疗轮廓勾画软件通过硬件设备进行数据交换，这些硬件设备包括 U 盘、光盘、移动硬盘等任意存储设备，软件不需要联网使用，产品安装在普通计算机上运行，软件通过计算机自带的硬件接口导入数据。