文件号：MS001.01.102TR.1.0

**MS-001**

**网络安全风险管理报告**

|  |  |
| --- | --- |
| 编制/时间: | 郭宏瑞/2021.04.20 |
| 审核/时间: | 童睿/2021.04.20 |
| 批准/时间: | 陈汉清/2021.04.20 |

杭州三坛医疗科技有限公司

文档更改履历

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 发布/实施日期 | 更改内容概述 | 更改者 |
| V1.0 | 2021.04.20 | 文件新编 | 郭宏瑞 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 引言

风险管理报告的目的是，根据风险管理计划总结医疗器械产品开发过程中进行的风险管理活动，提供对产品整体风险的评估和风险管理过程的结果报告。

# 术语和定义

伤 害――对人体的损伤或对人体健康的损害，或对财产或环境的损害。

危险(源) ――可能导致伤害的潜在根源。

危险情况――人员、财产或环境暴露于一个或多个危险(源)中的情形。

安 全――免除了不可接受的风险的状态。

严 重 度――危险(源)可能后果的度量。

风 险――伤害发生的概率和该伤害严重度的组合。

剩余风险――实施风险控制措施后还存在的风险。

风险分析――系统地运用现有信息确定危险(源)和估计风险的过程。

风险评定――包括风险分析和风险评价的全过程。

风险估计――用于对伤害发生的概率和该伤害严重度赋值的过程。

风险控制――作出决策并实施措施，以便降低风险或把风险维持在规定水平的过程。

风险评价――将估计的风险和给定的风险准则进行比较，以决定风险可接受性的过程。

风险管理――用于风险分析、评价、控制和监视工作的管理方针、程序及其实践的系统运用。

合理可遇见误用――产品或系统的使用方式不按照制造商的说明进行，而是由易于预测的人类行为引起的。

# 参考文件

YY/T 0316-2016 医疗器械 风险管理对医疗器械的应用

YY/T 0664-2020 医疗器械软件 软件生存周期过程

医疗器械网络安全注册技术审查指导原则

《MS-001 技术需求规格书》

《规划软件概要设计说明书》

《导引软件概要设计说明书》

# 产品描述

1. **产品名称：**

|  |  |  |
| --- | --- | --- |
| **序号** | **主体** | **描述** |
| 1 | 专有名称 | 模块化手术导引系统 |
| 2 | 型号 | MS-001 |

1. **预期用途：**

MS-001是一款需与C型臂X光机配合使用，用于骨组织手术中体内规划目标的定位与导引，为手术提供辅助参考的产品。

1. **软件运行环境：**

|  |  |  |
| --- | --- | --- |
| 硬件要求 | CPU | Intel(R) Core(TM) i3-10100 CPU @3.60GHz 3.60GHz |
| 内存 | 8GB |
| 显卡 | Intel(R) UHD Graphics 630 |
| 硬盘 | 500GB |
| 显示器 | 分辨率：1920 \* 1080 |
| 软件要求 | 操作系统 | Windows10 64位 |

# 风险管理团队

## 5.1 职责和权限

| **职位** | **名字** | **职责** | **权限** |
| --- | --- | --- | --- |
| 管理者代表（风险评审小组组长） | 卢明 | * 负责书面制定本公司的风险可接受性准则的方针； * 为风险管理活动配备充分的资源和有资格能胜任的人员； * 规定风险管理的职责和权限，组建风险评审小组，授权研发中心确定风险管理小组成员； * 定期审查公司风险管理过程； * 授权风险管理评审小组组长批准《风险管理报告》。 | 审核  批准 |
| 研发中心总监 | 陈汉清 | * 负责指定各产品和项目的风险管理小组组长； * 负责批准《风险管理计划》和《风险评估和控制记录》； * 负责组织协调风险管理活动； * 负责跟踪检查风险管理活动实施情况。 | 审核  批准 |
| 产品经理  （风险管理小组组长） | 郭宏瑞 | * 负责制定《风险管理计划》，协调风险管理活动； * 组织风险管理小组实施风险管理活动，编写《风险管理报告》； * 识别和监督行动，审查所采取行动的有效性； * 将风险管理活动的影响和产品生命周期的各个阶段关联； * 负责协调行业技术水平的调研和应用； * 负责竞争产品的对比输入； * 跟踪相关活动，包括生产和生产后信息； * 对涉及重大风险的，可直接向最高管理者汇报； * 整理风险管理文档，确保风险管理文档的完整性和可追溯性。 | 编制  审核 |
| 质量 | 詹佳丹 | * 对整个风险管理过程进行监控； * 确保风险管理活动的有效性； * 关于内部质量偏差的输入； * 将风险管理活动的影响和质量管理体系关联； * 执行内部审核或审计。 | 编制  审核 |
| 临床 | 方华磊 | * 参与风险管理活动； * 实施行动，审查有效性； * 风险评估时，从临床角度对伤害的严重度和可能性以及理由提供参考； * 风险受益分析时，从临床角度作出判断结论。 | 编制  审核 |
| 生产 | 王玉帆 | * 参与风险管理活动； * 实施行动，审查有效性； * 关于工艺更改或生产制造过程的风险评估的输入。 | 编制  审核 |
| 采购 | 戚利华 | * 参与风险管理活动； * 实施行动，审查有效性； * 关于供应商、采购不符合品等风险评估的输入。 | 编制  审核 |
| 注册 | 焦晓黎 | * 参与风险管理活动； * 实施行动，审查有效性； * 从注册角度审查风险评估的输入。 | 编制  审核 |

# 风险管理过程总结

所有风险管理活动都按照风险管理计划的要求实施行动和交付成果物。

## 风险管理过程示意图



图1 风险管理过程

## 风险分析和评价

在正常使用，非正常使用和故障模式条件下，识别已知或可预见的危险(源)、危险情况和伤害。使用风险管理计划中定义的标准，对每种危险情况的风险进行估计，包括潜在的伤害严重度等级和伤害的总体概率。还利用风险管理计划中定义的“风险可接受性准则”对每个估计的风险进行了风险可接受性评估。

风险分析和评估结果见《风险评估和控制记录》。

## 风险控制措施和实施

需要降低风险时，应按照以下方式进行风险控制活动，并在实施控制措施后评估剩余风险。

风险控制措施，应按照以下顺序，使用一种或多种方式。

1） 设计固有的安全性；

2） 医疗器械本身或制造过程中的保护措施；

3） 安全信息。

通过设计验证测试和必要的验证研究，以确认风险控制措施的实施和有效性。

有关采取风险控制措施前/后风险分析和评估结果，和可追溯性均记录在《风险评估和控制记录》。

## 剩余风险评价

实施风险控制措施后，应当按照与风险评价时相同的标准进行剩余风险评估。

* 风险控制措施前

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **发**  **生**  **概**  **率**  **等**  **级** | **严重程度等级** | | | | | |
|  | 可忽略（S1） | 轻度（S2） | 严重（S3） | 危重的（S4） | 灾难性的（S5） |
| 经常（P5） |  |  |  |  |  |
| 有时（P4） |  |  |  |  |  |
| 偶然（P3） |  | H6、H18 |  |  |  |
| 很少（P2） | H1、H7、H9、H10、H11、H13、H20、H22、H23、H24 | H2、H3、H4、H8、H12、H14、H16、H19、H21、H25 | H5、H17 |  |  |
| 非常少（P1） |  |  |  |  |  |

* 风险控制措施后

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **发**  **生**  **概**  **率**  **等**  **级** | **严重程度等级** | | | | | |
|  | 可忽略（S1） | 轻度（S2） | 严重（S3） | 危重的（S4） | 灾难性的（S5） |
| 经常（P5） |  |  |  |  |  |
| 有时（P4） |  |  |  |  |  |
| 偶然（P3） |  |  |  |  |  |
| 很少（P2） |  |  |  |  |  |
| 非常少（P1） | H1、H7、H8、H9、H10、H11、H12、H13、H20、H21、H22、H23、H24、H25 | H2、H3、H4、H5、H6、H14、H15、H16、H17、H18、H19 |  |  |  |

## 风险/受益分析

从 6.4 我们知道，所有剩余风险都是可以接受的。因此，风险/受益分析是没有必要的。

## 风险控制完整性

已考虑所有相关风险，风险评估过程确认完整，不再采取进一步行动。

# 综合剩余风险评价

在所有风险控制措施实施和验证后，风险管理团队认为医疗器械产品的总体剩余风险是可以接受的。

且，未发现存在互相矛盾的风险控制措施。所有风险叠加后的影响处于可接受水平。

# 风险管理的结论

风险管理活动遵循风险控制程序和适用的风险管理标准进行。制定了风险管理计划，并按计划实施。已识别风险，并在需要降低风险时进行风险控制活动。所有风险控制措施均已实施和核实，并记录在风险评估和控制文件中。综合剩余风险被评估为可接受。所有风险管理文件都包含在设计历史文件中。

# 附录：产品安全特征问题清单

参考《医疗器械网络安全注册技术审查指导原则》

规划软件：

| **网络安全能力** | **考虑因素** | **适用**  **与否** | **产品能力评估** | **可能的危险（源）** | **危险源标识** |
| --- | --- | --- | --- | --- | --- |
| 自动注销（ALOF） | 考虑：  无人值守的医疗器械终端设备，存在被进行非授权操作、显示信息被非授权人员阅读的风险。 | 适用 | 用户登录进入软件之后一定时间内不操作会自动进入锁屏界面，解锁需要输入账户对应密码 | 使用错误危险 | H1 |
| 审核控制（AUDT） | 考虑：  产品提供信息审核的能力。 | 适用 | 日志记录关键操作及关键结果 | 功能危险 | H2 |
| 授权（AUTH） | 考虑：  产品授权管理，不同使用者的权限不同。 | 适用 | 不同账户拥有不同权限 | 使用错误危险 | H3 |
| 安全特性配置（CNFS） | 考虑：  产品管理员可以选择使用产品的不同的网络安全功能。 | 不适用 | 不连接网络 | / | / |
| 网络安全产品升级（CSUP） | 考虑：  授权用户安装/升级产品网络安全补丁的能力。 | 不适用 | 不连接网络 | / | / |
| 健康数据身份信息去除（DIDT） | 考虑：  产品去除健康数据所附带的身份信息的能力。 | 不适用 | 导出数据不含敏感信息 | / | / |
| 数据备份与灾难恢复（DTBK） | 考虑：  产品出现故障或受到破坏后，可以恢复存储在产品上的健康数据，从而可以继续开展业务。 | 适用 | 数据管理，点下一步按钮，首次导入的数据将被写入数据库，同时更新到数据列表首行 | 使用错误危险 | H4 |
| 紧急访问（EMRG） | 考虑：  紧急情况下，用户需要能够访问健康数据，而无需个人用户ID和身份验证。紧急访问要能被检测，记录和报告。 | 不适用 | 不提供紧急访问功能 | / | / |
| 健康数据完整性与真实性（IGAU） | 考虑：  产品要确保健康数据的来源可靠且未经篡改与破坏，比如用硬盘、U盘保存数据。 | 适用 | 数据管理，点击导入按钮，识别U盘，并加载显示数据列表 | 使用错误危险 | H5 |
| 恶意软件探测与防护（MLDP） | 考虑：  产品需要在使用过程中探测恶意软件的侵入，并且可以不断维护，必要时采取紧急措施。 | 适用 | Windows Defender实时开启防护，防止恶意软件探测 | 功能危险 | H6 |
| 网络节点鉴别（NAUT） | 考虑：  产品在与其他设备通信时进行数据节点的认证，保证数据不被篡改。 | 适用 | 规划台车通过网线物理连接可信的设备（导引台车）；规划软件与导引软件的通讯遵循内部通信协议 | 功能危险 | H7 |
| 人员鉴别（PAUT） | 考虑：  产品为用户创建和使用唯一帐户，需要身份验证才能登录。 | 适用 | 用户拥有唯一账户，需要身份验证才能登陆 | 使用错误危险 | H8 |
| 物理锁（PLOK） | 考虑：  产品采用物理的方式，防止系统被损坏。主要是防止存储敏感信息的媒介被轻松取出，这里不包括移动的存储媒介。 | 适用 | 硬盘在主机内，外部有主机外壳，硬盘不会被轻松取出 | 使用错误危险 | H9 |
| 第三方组件维护计划（RDMP） | 考虑:  医疗器械是否用到第三方组件进行管理，比如包括操作系统，数据库系统，报告生成器。 | 不适用 | 不连接网络 | / | / |
| 系统与应用软件硬化（SAHD） | 考虑：  产品存在着与预期用途无关的配置，例如：某些非医疗预期用途的账号、通信端口、共享文件、服务等。 | 不适用 | 不连接网络 | / | / |
| 安全指导（SGUD） | 考虑：  产品为用户提供网络安全方面资料的能力。 | 适用 | 加强人员培训 | 使用错误危险 | H10 |
| 健康数据存储保密性（STCF） | 考虑：  产品确保所存数据保密性和完整性的能力。 | 适用 | 所有用户都无法进入windows桌面，无法访问保存健康数据的硬盘 | 使用错误危险 | H11 |
| 传输保密性（TXCF） | 考虑：  产品确保数据传输保密性的能力。 | 适用 | 网络通讯功能遵循内部加密协议 | 使用错误危险 | H12 |
| 传输完整性（TXIG） | 考虑：  产品确保数据传输完整性的能力。 | 适用 | 网络通讯功能遵循内部加密协议 | 功能危险 | H13 |

导引模块：

| **网络安全能力** | **考虑因素** | **适用**  **与否** | **产品能力评估** | **可能的危险（源）** | **危险源标识** |
| --- | --- | --- | --- | --- | --- |
| 自动注销（ALOF） | 考虑：  无人值守的医疗器械终端设备，存在被进行非授权操作、显示信息被非授权人员阅读的风险。 | 适用 | 用户登录进入软件之后一定时间内不操作会自动进入锁屏界面，解锁需要输入账户对应密码 | 使用错误危险 | H14 |
| 审核控制（AUDT） | 考虑：  产品提供信息审核的能力。 | 适用 | 日志记录关键操作及关键结果 | 功能危险 | H15 |
| 授权（AUTH） | 考虑：  产品授权管理，不同使用者的权限不同。 | 适用 | 不同账户拥有不同权限 | 使用错误危险 | H16 |
| 安全特性配置（CNFS） | 考虑：  产品管理员可以选择使用产品的不同的网络安全功能。 | 不适用 | 不连接网络 | / | / |
| 网络安全产品升级（CSUP） | 考虑：  授权用户安装/升级产品网络安全补丁的能力。 | 不适用 | 不连接网络 | / | / |
| 健康数据身份信息去除（DIDT） | 考虑：  产品去除健康数据所附带的身份信息的能力。 | 不适用 | 导出数据不含敏感信息 | / | / |
| 数据备份与灾难恢复（DTBK） | 考虑：  产品出现故障或受到破坏后，可以恢复存储在产品上的健康数据，从而可以继续开展业务。 | 适用 | 在关键操作后自动对数据进行保存 | 使用错误危险 | H17 |
| 紧急访问（EMRG） | 考虑：  紧急情况下，用户需要能够访问健康数据，而无需个人用户ID和身份验证。紧急访问要能被检测，记录和报告。 | 不适用 | 不提供紧急访问功能 | / | / |
| 健康数据完整性与真实性（IGAU） | 考虑：  产品要确保健康数据的来源可靠且未经篡改与破坏，比如用硬盘、U盘保存数据。 | 不适用 | 导引软件不存储健康数据 | / | / |
| 恶意软件探测与防护（MLDP） | 考虑：  产品需要在使用过程中探测恶意软件的侵入，并且可以不断维护，必要时采取紧急措施。 | 适用 | Windows Defender实时开启防护，防止恶意软件探测 | 功能危险 | H18 |
| 网络节点鉴别（NAUT） | 考虑：  产品在与其他设备通信时进行数据节点的认证，保证数据不被篡改。 | 适用 | C臂机AEtitle设置 | 功能危险 | H19 |
| 人员鉴别（PAUT） | 考虑：  产品为用户创建和使用唯一帐户，需要身份验证才能登录。 | 适用 | 用户拥有唯一账户，需要身份验证才能登陆 | 使用错误危险 | H20 |
| 物理锁（PLOK） | 考虑：  产品采用物理的方式，防止系统被损坏。主要是防止存储敏感信息的媒介被轻松取出，这里不包括移动的存储媒介。 | 适用 | 硬盘在主机内，外部有主机外壳，硬盘不会被轻松取出 | 使用错误危险 | H21 |
| 第三方组件维护计划（RDMP） | 考虑:  医疗器械是否用到第三方组件进行管理，比如包括操作系统，数据库系统，报告生成器。 | 不适用 | 不连接网络 | / | / |
| 系统与应用软件硬化（SAHD） | 考虑：  产品存在着与预期用途无关的配置，例如：某些非医疗预期用途的账号、通信端口、共享文件、服务等。 | 不适用 | 不连接网络 | / | / |
| 安全指导（SGUD） | 考虑：  产品为用户提供网络安全方面资料的能力。 | 适用 | 加强人员培训 | 使用错误危险 | H22 |
| 健康数据存储保密性（STCF） | 考虑：  产品确保所存数据保密性和完整性的能力。 | 不适用 | 导引软件不存储健康数据 | / | / |
| 传输保密性（TXCF） | 考虑：  产品确保数据传输保密性的能力。 | 适用 | 网络通讯功能遵循内部加密协议 | 使用错误危险 | H23 |
| 传输完整性（TXIG） | 考虑：  产品确保数据传输完整性的能力。 | 适用 | 网络通讯功能遵循内部加密协议 | 功能危险 | H24 |

**注1：H表示危险源“Hazard”，H后的序号为危险源序号，该序号是起始为1的顺位自然数（顺位无空挡）。**