MS-002.30W009

MS-002

网络安全维护计划

编制/日期： XXX/2023.xx.xx

审核/日期： 洪洁/2023.xx.xx

批准/日期： 张巍/2023.xx.xx

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 | 2023.xx.xx | 文件新编 | XXX |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目录**

[1. 目的 1](#_Toc19314)

[2. 参考资料 1](#_Toc7783)

[3. 职责 1](#_Toc13977)

[4. 网络安全更新 1](#_Toc20739)

[5. 网络安全更新的维护流程 2](#_Toc22067)

[6. 网络安全事件应急响应 4](#_Toc4361)

# 目的

本文档为MS-002的网络安全维护计划，描述了网络安全更新的维护流程，包括更新确认和用户告知，并针对网络安全事件制定应急响应措施，以保证MS-002系统的安全有效性并保护患者隐私。

# 参考资料

医疗器械网络安全注册技术审查指导原则（2022年修订版）（2022年第7号）

ST-ZD-40 《网络安全保证规范》  
ST-ZD-47 《网络安全应急响应管理办法》

《MS-002软件维护计划摘要》

# 职责

|  |  |
| --- | --- |
| **角色** | **职责和权限** |
| 网络安全小组 | 由技术负责人/研发总监为组长，组织软件组、测试组、信息部、质量部等相关人员，必要时，及时上报管理者代表与总经理。  负责统一领导网络与信息安全的应急工作，全面负责信息网络可能出现的各种突发事件处置工作。发生网络与信息安全突发事件时，组织确定并启动预案，组织应急处置。 |
| 网络安全员 | 负责网络和信息安全的日常工作和组织协调。 |

# 网络安全更新

医疗器械网络安全更新从内容上可分为功能更新、补丁更新，类似于增强类软件更新、纠正类软件更新。根据其对医疗器械安全性和有效性的影响程度分为以下两类：

1. 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，即重大网络安全功能更新。

网络安全功能更新若影响到医疗器械的预期用途、使用场景或核心功能原则上均属于重大网络安全更新，包括但不限于：产品预期运行的网络环境发生改变，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；产品预期使用的电子接口发生改变，如接口形式由网口变为USB口、接口类型由少变多、接口功能由电子数据交换扩至远程控制；产品网络安全能力发生实质性改变，如自动注销能力由操作系统自带功能实现改为产品自身功能实现、物理防护能力由有变无等。

此外，涉及召回的网络安全更新，无论功能更新还是补丁更新均属于重大网络安全更新。

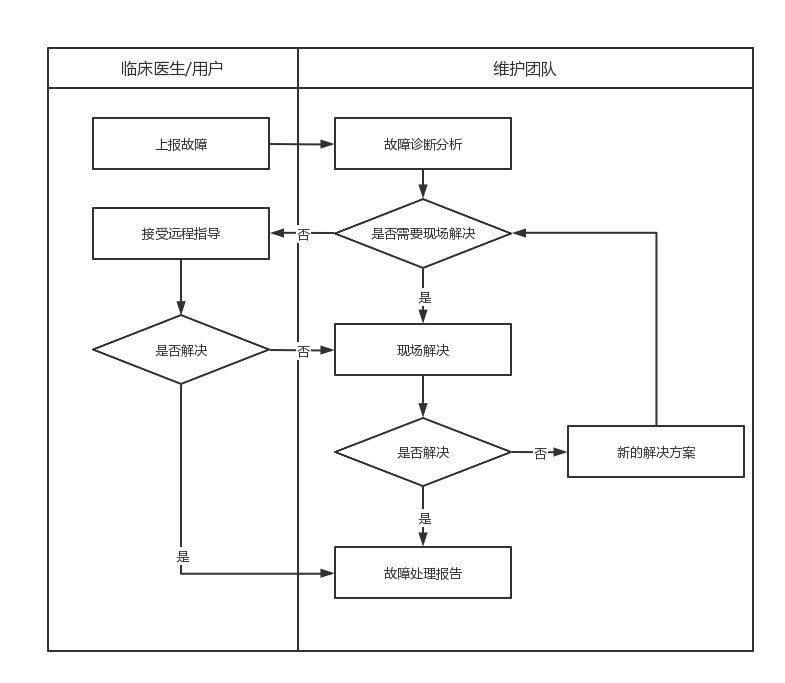
网络安全更新同样遵循风险从高原则，即同时发生重大和轻微网络安全更新按重大网络安全更新处理。

（2）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。

除非影响到医疗器械的安全性或有效性，以下网络安全功能更新和网络安全补丁更新通常视为轻微网络安全更新：产品预期运行的网络环境数据传输效率单纯提高，预期使用的电子接口原有功能单纯优化、传输效率单纯提高，产品网络安全能力发生非实质性改变；医疗器械软件、必备软件、外部软件环境的网络安全补丁更新。

# 网络安全更新的维护流程

软件网络安全更新的维护流程如下：



流程说明：

* 更新确认：

临床医生/用户提出维护申请。

维护团队需要对故障进行分析核实，并确认是否需要现场维护。

如果不需要现场维护的情况下，维护团队远程指导临床医生/用户进行维护，如果需要现场维护的情况则派遣维护团队到实地进行现场维护。现场如果未解决故障，维护团队分析并提出新的解决方案，并对可能产生的风险进行分析评价，必要时提出风险控制措施。

如有需要，对系统进行数据备份。

* 用户告知：

维护团队按照方案进行修改操作。完成维护后，通知用户进行了维护以及维护主要内容。

# 网络安全事件应急响应

公司基于相关标准和技术报告建立网络安全事件应急响应机制，保证医疗器械的安全有效性并保护患者隐私。

一旦发生网络安全事件，第一时间成立网络安全小组，结合产品、软件的特性，应制定相应的应急响应措施，包括但不仅限于如下列举的措施方式：

（1）升级网络安全防护；

（2）升级运行环境；

（3）更新访问权限；

（4）软件更新与替换；

（5）软件卸载与销毁；

（6）数据备份与恢复。

必要时提供网络安全事件应急响应预案文档。

具体按照ST-ZD-47《网络安全应急响应管理办法》实施。