动态心电分析软件

网络安全测试计划

通心络科（河北）科技有限公司

目录

[**1** **目的** 1](#_Toc522193940)

[**2** **范围** 1](#_Toc522193941)

[**3** **背景** 1](#_Toc522193942)

[**4** **参考文件** 1](#_Toc522193945)

[**5** **术语或缩写词** 1](#_Toc522193946)

[**6** **文件的更新要求** 1](#_Toc522193947)

[**7** **人员职责** 2](#_Toc522193948)

[**8** **测试设备** 2](#_Toc522193950)

[**9** **环境要求** 2](#_Toc522193952)

[**10** **测试项目、接受标准和测试方法** 2](#_Toc522193954)

[**11** **结论** 8](#_Toc522193999)

[**12** **附录** 9](#_Toc522194000)

1. **目的**

按照《医疗器械网络安全注册技术审查指导原则》中的规定要求进行测试，确保产品的网络安全，保证产品的安全和有效。

1. **范围**

适用通心络科（河北）科技有限公司生产的动态心电分析软件进行网络安全相关测试。

1. **背景**

动态心电分析软件传输设备数据，包括：心电数据、用户数据、分析报告、分析参数传输等。本产品通过互联网进行电子数据传输，数据由服务器传输给动态心电分析软件，或者由动态心电分析软件传输给服务器。

对通心络科（河北）科技有限公司的产品动态心电分析软件进行验证，确保产品符合指导原则的要求。

1. **参考文件**
   1. 《动态心电分析软件需求规范》
   2. 《动态心电分析软件技术要求》
   3. 《医疗器械网络安全注册技术审查指导原则》2017年第13号
2. **术语或缩写词**
   1. 保密性：指数据不能被未授权的个人、实体利用或知悉的特性，即医疗器械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；
   2. 完整性：指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；
   3. 可得性：指根据授权个人、实体的要求可访问和使用的特性，即医疗器械相关数据能以预期方式适时进行访问和使用。
3. **文件的更新要求**

## 包括但不限于触发以下事件时，应考虑更新文件：

* 当《动态心电分析软件需求规范》变化时需考虑本文件;
* 当《动态心电分析软件技术要求》变化时需考虑本文件;
* 测试过程、结果与方案发生较大偏差时需考虑本文件；
* 法律法规更新时需考虑本文件；
* 测试方式，方法变化时需考虑本文件。

## 本文件更新时应考虑对包括但不限于以下文件的影响：

* 《动态心电分析软件网络安全测试报告》；
* 《动态心电分析软件风险管理文档》。

1. **人员职责**

|  |  |  |  |
| --- | --- | --- | --- |
| **人员** | **部门** | **职位** | **职责** |
| 张乔 | 品质注册部 | 质量工程师 | 编制《测试计划》和《测试报告》，并组织进行相应实施 |
| 孟祥思 | 品质注册部 | QC工程师 | 按照方案内容进行测试，并形成、汇总检验记录，协助编制《测试报告》。 |
| 马军 | 品质注册部 | 品质注册总监 | 审核和批准《测试计划》和《测试报告》。 |

1. **测试设备**

详见测试方法。

1. **环境要求**

TXLK/AS 6.4-01按《环境管理制度》要求，常温区环境要求。

1. **测试项目、接受标准和测试方法**
   1. 产品确认
      1. 数据考量确认

相关数据从内容上可分为以下两种类型：

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。

根据动态心电分析软件产品特性，确动态心电分析软件数据方式。

* + 1. 相关数据的交换方式确认

医疗器械相关数据的交换方式可分为以下两种情况：

1.网络：通过网络（包括无线网络、有线网络）进行电子数据交换或远程控制，需要考虑网络相关要求（如接口、带宽等），数据传输协议需考虑是否为标准协议（即业内公认标准所规范的协议），远程控制需考虑是否为实时控制；

2.存储媒介：通过存储媒介（如光盘、移动硬盘、U盘等）进行电子数据交换，数据储存格式需考虑是否为标准格式（即业内公认标准所规范的格式）

根据动态心电分析软件产品特性，确认动态心电分析软件数据方式。

* 1. 产品网络安全特性确认

|  |  |  |
| --- | --- | --- |
| 条款要求 | 判断 | 说明 |
| 自动注销（ALOF） | × | 此条款目的是：减少无人值守工作节点的非授权用户访问健康数据的风险，如果系统或节点在一段时间闲置后，防止其他用户的误操作。  本产品：软件在登录条件下，才可以分析心电数据。因此不存在非授权用户访问健康数据的风险，以及误操作，因此不需要自动注销。 |
| 审核控制（AUDT） | × | 此条款目的是：定义协调一致的方法，以可靠地审计对健康数据所做的操作。允许医疗机构的IT使用公共的框架来监控谁正在做何种操作。  本产品：软件下载数据副本，进行数据分析，不能修改原始文件，不能通过IT使用公共框架监控谁正在做何种操作，因此不需要审核控制。 |
| 授权（AUTH） | √ | 此条款目的是：遵循数据最小化原则施加控制，只有在执行医疗机构在执行要求的任务时，在符合预期用途的情况下，才能对健康数据和功能进行访问  本产品：软件在用户电脑端会设置授权登录，只有授权了才能访问健康数据和功能。 |
| 安全特性配置（CNFS） | × | 此条款目的是：允许医疗机构来决定，如何利用产品的安全能力来满足他们的政策和/或工作流的需求  本产品：不介入医疗机构的系统，因此不适用。  仅通过BLE对授权测试人员使用验证过的外部设备进行数据通讯，无需本地IT管理员，无此特性。 |
| 网络安全产品升级（CSUP） | √ | 此条款目的：创建统一的方式。由现场服务人员、远程服务人员以及可能获得授权的医疗机构人员安装/升级产品安全补丁（可下载补丁）。  本产品：软件通过现场服务人员升级。 |
| 健康数据身份信息去除（DIDT） | √ | 此条款目的：设备具有能够直接去除可能识别患者的信息的能力（应用软件或其他工具）。在返厂前进行数据清洗；架构上允许远程服务，但不需要访问/暴露患者信息；工厂内隔离；标签和培训。  本产品：本产品不保存用户身份信息，返厂删除设备的全部信息。 |
| 数据备份与灾难恢复（DTBK） | √ | 此条款目的：确保医疗服务的提供者能够在数据、硬件、软件损坏或破坏后继续业务。  本产品：将心电数据从网络上备份到本地，还可以手动在本地二次备份副本，需要时直接替换文件进行恢复。 |
| 紧急访问（EMRG） | √ | 此条款目的：确保在需要立即访问存储的健康数据的紧急情况下能够访问受保护的健康数据。  本产品：可以随时在装有该软件的电脑上，进行账号登录和数据下载。 |
| 健康数据完整性与真实性（IGAU） | √ | 此条款目的：确保健康数据没有以未授权的方式被篡改或销毁，且来自创建者。  本产品：验证软件接收数据的完整性与真实性，保证数据无法以未授权的方式篡改或销毁。 |
| 恶意软件探测与防护（MLDP） | √ | 此条款目的：产品能够支持法规、医疗结构和用户需求，以确保对恶意软件的预防、检测和去除提供有效和统一的支持。（需要对设备的运行进行更新后验证测试，以便继续预期的使用和安全）  本产品： 软件具有禁用网络代理防止抓包，防止恶意软件探测和防护。 |
| 网络节点鉴别（NAUT） | √ | 此条款目的：灵活的身份验证策略，以适应本地策略。必要时，在通信健康数据时使用节点身份验证。  本产品：通过用户名和密码验证的验证策略。 |
| 人员鉴别（PAUT） | √ | 此条款目的：灵活的身份验证策略，以适应本地策略。在提供健康数据访问时，要求人员身份验证。控制对设备、网络资源和健康数据的访问，并生成不可否认的审计跟踪。这个特性应能够明确地确定访问网络、设备或资源的个人。  本产品：通过用户名和密码验证的验证策略。 |
| 物理锁（PLOK） | × | 此条款目的：确保系统或数据保密性、安全性和可得性不受非授权访问的危险。  本产品：为软件，无物理锁。 |
| 第三方组件维护计划（RDMP） | √ | 此条款目的：医疗机构要对医疗设备整个生命周期的安全性有所了解。制造商根据内部质量系统和外部规则计划产品的整个生命周期都是可持续的。  本产品：软件可检测软件的版本信息，根据版本信息判断软件的状态。 |
| 系统与应用软件硬化（SAHD） | √ | 此条款目的：调整医疗设备和/或软件应用程序的安全控制，使安全最大化（“强化”），同时保持预期用途。通过端口关闭，移除服务等方式使得攻击最小化。  本产品：设备已关闭其他端口，仅保留一个自定义的数据传输端口。 |
| 安全指导（SGUD） | √ | 此条款目的：确保操作人员和管理员的安全指导是可得的，操作人员和管理员（包括医疗器械的销售和维护）需要单独的手册，因为仅管理员可知晓完整的管理功能。  本产品：已建立管理人员后台管理功能。 |
| 健康数据存储保密性（STCF） | √ | 此条款目的：制造商建立技术控制，以减少存储在产品或可移动媒体上的健康数据的完整性和保密性受到损害的可能性。如基于风险分析考虑对保存在医疗器械上的健康数据进行加密。  本产品：本产品的健康数据基于自定的数据协议，具有保密性，自带加密功能。 |
| 传输保密性（TXCF） | √ | 此条款目的：保证传输的健康数据的保密性，符合当地的法律法规及标准要求。  本产品：该项验证了数据的健康传输保密性，保证健康数据的安全。 |
| 传输完整性（TXIG） | √ | 此条款目的：保证传输的健康数据的完整性。  本产品：该项验证了数据的健康传输保密性，保证健康数据的安全。 |

* 1. 测试环境和设备
  2. 测试项目、测试代号及测试方法
     1. 授权

测试代号：

接受准则：

测试方法/步骤：

结合软件登录授权功能，对其健康数据和功能访问权限符合性进行验证。

* + 1. 网络安全升级

动态心电分析软件，由规定的人员（现场服务人员、远程服务人员以及可能获得授权的医疗机构人员）通过以下方法验证安装/升级产品安全补丁（可下载补丁）登录授权功能，并对其健康数据和功能访问权限符合性进行验证：

1、在测试电脑上首次安装软件,测试在未登录授权的情况下访问数据情况；

2、在授权登录后，测试软件访问数据情况；

3、在软件升级更新后，在未授权登录，测试软件访问数据情况；

4、在软件升级更新后，在授权登录后，测试软件访问数据情况。

* + 1. 健康数据身份信息去除

动态心电分析软件，通过以下方法验证软件具有能够直接去除可能识别用户的信息的能力：

通过软件进入登录界面，可以选择是否保存密码。患者信息不保存，只在登录后才可以看到，退出后即消失。

* + 1. 健康数据完整性与真实性

动态心电分析软件，通过以下方法验证健康数据没有以未授权的方式被篡改或销毁，且来自创建者；

建立两个测试用户（用户1，用户2），使用“用户1”登录软件，并下载一段数据，软件退出登录“用户1”，使用“用户2”登录，测试“用户2”在数据记录中能否发现用户1数据，并删除用户1数据。

* + 1. 恶意软件探测与防护

APP具有禁用网络代理防止抓包,防止恶意软件探测和防护。

* + 1. 网络节点鉴别

通过用户名和密码验证的验证策略。

软件登陆过程中，使用输入用户名和密码方式登录。

* + 1. 人员鉴别

通过用户名和密码验证的验证策略。

软件登陆过程中，使用输入用户名和密码方式登录。

* + 1. 第三方组件维护计划

软件可查看软件版本，根据软件版本判断软件的状态。

* + 1. 系统与应用软件硬化

设备已关闭其他端口，仅保留一个自定义的数据传输端口。

软件仅用8090端口与服务器端通讯。

* + 1. 健康数据存储保密性

本软件的健康数据基于自定的数据协议，具有保密性，自带加密功能。

* + 1. 传输数据的保密性

通过以下方法针对传输数据的保密性进行确认：

测试是否可以接收心电数据，以及心电数据非明文形式。

* + 1. 传输数据的完整性

连续进行5次下载操作，检查数据是否完整，应无掉包现象，连接过程中无断开现象。

* + 1. 相关数据的可得性

任意5个数据进行下载，检查数据是否完整，应无掉包现象，连接过程中无断开现象。

* + 1. 数据的正确性

选择非患者数据，会弹出非官方数据的提示。可以通过重新下载获取正确数据。

* 1. 产品网络安全维护

由于软件的复杂性，一个看似很小的问题解决可能对全局系统产生重大影响。每当软件修订后，不仅要对此修订进行验证，还要确认此修订对整个软件系统的影响程度，对涉及到该软件修订的进行评审、验证和风险分析，软件修改 前后的差别对比，新软件的版本号，这些都将形成文件记录。

公司制定了7.3-3软件维护过程控制程序、7.3-4软件配置管理过程控制程序和7.3-5软件问题解决过程控制程序，并按照7.1.2 软件风险管理过程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。

软件网络安全更新维护的流程如下：



流程说明：

* + 1. 更新确认

研发部会同品质注册部对每个问题报告进行问题研究并评审，确定网络安全问题的严重程度，以决定其对软件产品的网络安全性有何种影响，是否有必要对软件产品进行更改以解决问题。

如果判定问题与网络安全性无关，指导解决，并确认问题是否关闭，如未解决重新进行问题研究。

如果判定问题与网络安全性有关，研发部会同品质注册部正确识别问题，需要立即解决的问题，研发部制定《软件变更实施计划》；可以以后解决的问题，研发部制定《软件问题解决计划》，通过评审后通知相关方。然后研发部实施软件问题解决流程，进行软件改进，并形成《软件问题修改报告单》。品质注册部对改进进行验证，确认问题是否解决。如未解决重新进行问题研究。

问题解决后，问题报告给予关闭。

* + 1. 用户告知

公司品质注册部在获知《软件变更实施计划》或《软件问题解决计划》后，进行评估是否触发药监主管部门备案或注册许可，如

软件工程师按照《软件变更实施计划》或《软件问题解决计划》进行软件改进操作。完成维护后，如果需要对用户软件进行更新，应通知用户软件进行更新以及维护的主要内容。如软件问题涉及重大安全隐患，应通知监管部门。至少应告知用户和监管部门以下信息：

* 已发行软件产品中的任何问题和不更改继续使用的后果。
* 已发行软件产品的任何可获得的更改的性质，以及如何获得并安装更改内容。

维护申请提出用户对维护结果进行反馈和评价。

* 1. 测试项通过准则

每个测试项必须通过其所有测试用例

所有测试结果按实际填写，并对结果进行确认。

* 1. 异常解决

对于出现的异常现象时，需要及时通知相关开发人员，开发人员根据异常现象确认分析，修改代码并自行调试通过后将新的软件交由测试人员。测试人员重新按照测试方案的中任务全面测试，不能只针对原来异常部分或软件更改部分。新的软件版本号需要升级。若新的软件依然存在异常，则按照前面方法重新再做一遍直到没有异常为止。

1. **网络安全可追溯性分析**

*通过分析《医疗器械网络安全注册技术审查指导原则》及网络安全风险管理，提出了适宜的风险控制措施，确定了网络安全需求；将需求纳入《产品需求规范》，并将网络安全需求在设计规范中体现，对产品进行系统测试和用户测试，确认输出满足了输入的要求，风险控制措施得以实施并有效验证， 具体见《软件及网络安全可追溯性分析报告》*

1. **结论**

依据测试结果进行确定，确定测试结果是否满足要求。

1. **附录**
   1. 关联验证文件信息

动态心电分析软件网络安全测试报告。