ICS 33.050
CCS M 30

团　体　标　准

T/TAF XXX-XXXX

智能可穿戴设备安全　医疗健康可穿戴设备安全技术要求与测试方法

Security of smart wearable devices—Security technical requirements and testing methods for medical and health wearable devices

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

电信终端产业协会　发布

目　　次

前　言

本文件按照 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、郑州信大捷安信息技术股份有限公司、联想（北京）有限公司、百度在线网络技术（北京）有限公司。

本文件主要起草人：国炜、徐晓娜、宁华、魏凡星、路晔绵、李煜光、杜云、刘为华、刘献伦、李汝鑫、杨磊、吴月升、唐佳伟。

引　　言

随着医疗健康可穿戴设备的应用场景越来越丰富，智能手环/手表、智能眼镜、家用血压计、血糖仪等可联网的医疗健康可穿戴设备已广泛应用于个人和家庭健康监测，如果仅沿用通用的消费电子产品的测试标准和设备，已不能够评价真实的使用环境、使用场景对结果可靠性的影响。同时，可联网医疗健康可穿戴设备的数据和网络安全成为了当前行业最为关注的问题。可联网的医疗健康可穿戴设备当前作为最贴近人体实时监测健康数据的装置，其监测得到的数据大多属于个人信息。然而，近几年中相关行业出现了大量安全漏洞并发生数据泄露事件，可联网的医疗健康可穿戴设备正日益成为数据和网络安全违规的渠道。如果用户数据安全得不到有效保障、设备网络安全威胁得不到有效遏制，这些风险会给设备管理和运营方产生重大影响，同时也对用户的数据安全及切身利益带来极大危害。

本文件从信息通信安全的角度制定可联网的医疗健康可穿戴设备安全技术要求和测试方法，适用于相关产品设备生产厂商、方案商、行业用户及测试实验室等，可为国内该领域产品提供技术参考，为相关产品的评测提供依据。

智能可穿戴设备安全　医疗健康可穿戴设备安全技术要求与测试方法

1　范围

本文件规定了可联网的医疗健康可穿戴设备信息安全技术要求和测试方法。

本文件适用于可联网的医疗健康可穿戴设备。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34978-2017　信息安全技术 移动智能终端个人信息保护技术要求

GB/T 35273　信息安全技术 个人信息安全规范

3　术语和定义

GB/T 25273界定的以及下列术语和定义适用于本文件。

3.1

医疗健康可穿戴设备　medical and health wearable device

通过传感器、无线通信、多媒体等技术，以直接穿戴在身上（如手环、手表、眼镜、服饰等）、表皮植入或搭载在移动通信设备上的应用形式，进行人体各项生理体征数据测量\采集的便携式医疗或健康电子设备。

3.2

用户基本信息　user basic information

通常由用户录入，反映用户个人基本情况的信息，包括个人基本资料、个人身份信息、个人生物识别信息、个人一般健康数据、疾病史等。

注1：个人基本资料包括个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等。

注2：个人身份信息包括身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等。

注3：个人生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。

注4：个人一般健康数据包括身高、体重等。

3.3

监测诊疗数据　monitoring & diagnosis data

设备监测采集的用户生理、生化、体征等数据，包括血压、血糖、心率、血氧饱和度、体温、呼吸、睡眠等。

3.4

行为情绪数据 behavioral & emotional data

设备采集计算的用户行为和情绪相关数据，包括步数、距离、消耗能量、行走轨迹、锻炼时长、情绪变化。

3.5

环境数据 environmental data

设备采集的用户所处环境相关数据，包括温度、湿度、紫外线指数、污染指数、地理位置、噪声等。

3.6

体外数据采集传感器 in vitro data acquisition sensor

主要为MEMS（Micro-Electro-Mechanical System），包括加速度计、磁力计、触控传感器等。

3.7

体征数据传感器 vital sign data sensor

主要为生物传感器，包括血糖传感器、血压传感器、心电传感器、肌电传感器、体温传感器和脑电波传感器等。

4 缩略语

APP：移动通信终端应用程序（Application）

CNNVD：国家信息安全漏洞库（China National Vulnerability Database of Information Security）

CNVD：国家信息安全漏洞共享平台（China National Vulnerability Database）

WLAN：无线局域网（Wireless Local Area Network）

5 医疗健康可穿戴设备概况

5.1 医疗健康可穿戴设备分类及应用场景

医疗健康可穿戴设备主要应用场景包括：辅助诊断、慢性疾病管理、康复护理、健康监测等。

根据应用对象和场景的不同，可分为疾病监测类可穿戴设备和运动健康类可穿戴设备：

——疾病监测类可穿戴设备具有生命体征监测等功能，常用于疾病的辅助诊断、慢病管理和康复护理等；

——运动健康类可穿戴设备具有人体健康态评估等功能，常用于调节人体机能、增进健康。

5.2 整体架构

医疗健康可穿戴设备的整体应用架构图如图1所示，主要包括医疗健康可穿戴设备、管理客户端、云平台。

医疗健康可穿戴设备通过传感器采集用户数据，结合设备自身进行本地存储或实时、定期上传。

管理客户端为用户提供通过云平台对医疗健康可穿戴设备进行远程操作的接口，其应对其临时存储或长久存储的数据进行保护，并配合医疗健康可穿戴设备云平台对数据传输进行保护，同时采用安全机制保障自身安全。

云平台通过网络接入管理客户端和医疗健康可穿戴设备，应保证交互数据的传输安全，同时承担管理客户端对设备端接入、控制、授权等操作的认证功能，以及对所有操作的日志和审计功能。

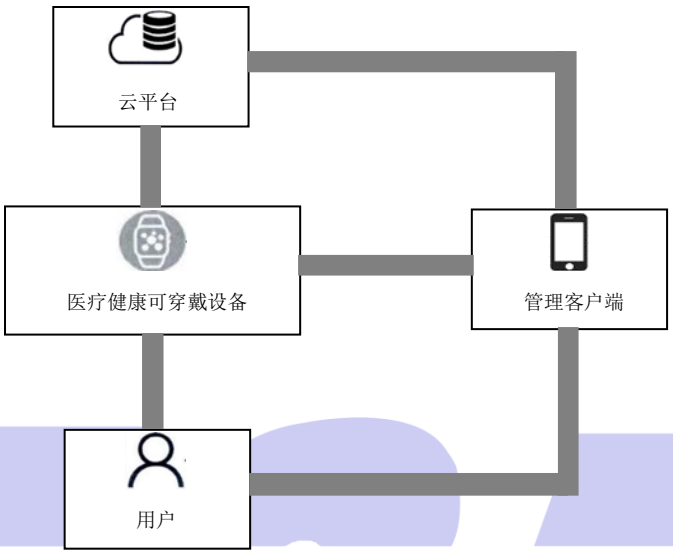

图 1　医疗健康可穿戴设备应用架构

5.3　数据分类及定义

根据内容的不同，医疗健康可穿戴设备的数据分为用户数据和设备数据。

5.3.1　用户数据

用户数据为设备使用用户的个人相关数据，包括用户基本信息、监测诊疗数据、行为情绪数据和环境数据。

5.3.2　设备数据

设备数据为设备运行状况相关的数据，包括用于监视、控制设备运行设备维修方面的数据。

5.4　数据分级

为使医疗健康可穿戴设备对其设备和应用中处理的数据提供完善的安全保护机制，基于泄露对用户隐私造成的影响，将医疗健康可穿戴设备的数据分为2级，分别是敏感级数据、一般级数据，分级具体内容见表1。

表 1　用户数据分级

级别	定义	数据类别举例
敏感级	一旦泄露对用户生命、财产、健康等产生严重影响	个人身份信息、个人生物特征信息、疾病史等

表 1　用户数据分级（续）

级别	定义	数据类别举例
一般级	一旦泄露对用户生命、财产、健康产生较少或可控的影响、或不会产生影响	一般的个人健康数据、监测诊疗数据、行为情绪数据、环境数据、设备数据等

6　总体安全目标

6.1　安全风险

医疗健康可穿戴设备会产生大量与人体健康等密切相关的数据，在为人们提供便捷服务的同时，面临的主要安全风险是数据泄露和被篡改，数据一旦泄露或被篡改，会给设备管理和运营方产生重大影响，同时也对用户的数据安全及切身利益带来极大危害。

医疗健康可穿戴设备面临的安全风险包括本地安全风险和远程安全风险，其中本地安全风险主要有用户数据窃取、固件被非法读取或篡改、本地数据伪造等；远程安全风险主要有远程接入安全、远程非法升级、通信数据泄露、远程指令重放和伪造等。

6.2　安全目标

6.2.1　用户数据安全目标

医疗健康可穿戴设备应具有足够的防护措施，保证用户数据在设备端、云平台和通信过程中的机密性、完整性和防重放保护。

医疗健康可穿戴设备应确保只有合法用户通过设定的方法和权限进行访问、控制，并确保用户数据的安全。

6.2.2　本地安全目标

医疗健康可穿戴设备在固件存储、固件升级等方面应有足够的防护，保证固件安全、固件升级包的完整性和来源可靠性。

医疗健康可穿戴设备应具有足够的安全防护措施，保证设备软硬件安全。

6.2.3　远程安全目标

医疗健康可穿戴设备与云平台、医疗健康可穿戴设备与管理客户端、医疗设备可穿戴设备与网关之间应具有足够的通信加密机制，保证通信数据的机密性、完整性和防重放要求。

医疗健康可穿戴设备与云平台、医疗健康可穿戴设备与管理客户端、医疗设备可穿戴设备与网关之间应具备身份认证和权限控制机制。

7　安全技术要求

7.1　个人信息保护安全要求

个人信息保护安全要求包括但不限于：

a)　医疗健康可穿戴设备对用户数据中用户基本信息的收集通常应在提供相应服务的同时进行。出于业务需要而必须事先收集相关数据，应向用户明示事先收集的目的和范围，并且只有在用户同意的情况下方可继续。医疗健康可穿戴设备应向用户提供关闭数据采集功能；

b) 疾病监测类可穿戴设备在关闭数据采集功能前，应对用户身份进行认证；
c) 医疗健康可穿戴设备在将用户数据存储在终端内部时，敏感级信息应与监测诊疗数据分开存储。存储敏感级数据时，应采用加密形式保存；
d) 医疗健康可穿戴设备若通过网络接口传输用户数据，应对数据进行加密，确保信息在网络传输过程中的安全；
e) 医疗健康可穿戴设备终端不应有未向用户明示且未经用户同意，擅自修改、删除、转移或拷贝用户基本信息的行为。若将用户基本信息存储在终端内部，终端设备应提供相应选项，允许用户修改或彻底物理删除已存储的用户基本信息。

7.2 无线通信安全要求

7.2.1 协议一致性

所采用WLAN、蓝牙、ZigBee等无线通信协议应支持设备授权认证、加密传输等安全扩展功能。

7.2.2 协议健壮性

应具备非法报文处理能力，当接收到非法报文时应能够正确处理，防止非预期的异常情况发生。

7.3 传输安全要求

7.3.1 传输完整性要求

传输完整性要求包括但不限于：
a) 医疗健康可穿戴设备各个执行主体之间在进行数据传输时，除传输数据主体外，应附加用于对数据进行完整性校验的校验信息；
b) 医疗健康可穿戴设备各个执行主体之间在进行数据传输时，可根据传输不同分类级别的数据采用不同的数据完整性校验方法；
c) 医疗健康可穿戴设备各个执行主体之间在进行数据传输时，应采用密码机制保证数据传输完整性，采用的密码机制应符合有关法律、行政法规和相关国家标准、行业标准要求；
d) 在检测到传输数据的完整性遭到破坏时，应采取措施恢复或重新获取数据。

7.3.2 传输机密性要求

传输机密性要求包括但不限于：
a) 医疗健康可穿戴设备各执行主体之间在进行数据传输时，应采用密码机制对传输数据进行加密；
b) 医疗健康可穿戴设备各执行主体之间对于敏感级数据的传输，应采用有必要安全强度的加密算法对数据进行加密；
c) 医疗健康可穿戴设备各执行主体之间在传输加密数据时，应每次采用不同密钥的加密传输方式；
d) 医疗健康可穿戴设备各执行主体之间传输数据时的加密算法应符合有关法律、行政法规和相关国家标准、行业标准要求；
e) 医疗健康可穿戴设备各执行主体之间在进行数据传输时，若涉及密钥管理，密钥管理策略应能够解决周期密钥更新、密钥撤销和密钥分发等问题。

7.3.3 传输抗重放要求

传输抗重放要求包括但不限于：

a) 医疗健康可穿戴设备各执行主体之间在进行数据传输时，应采用机制防止数据包或报文的重排或重放；
b) 医疗健康可穿戴设备各执行主体之间在进行数据传输时，可使用序列码或时间戳实现抗重放攻击；
c) 医疗健康可穿戴设备各执行主体之间在进行数据传输时，可在数据中加入与当前事件有关的一次性随机数。

7.4 系统安全漏洞修复与更新要求

7.4.1 安全防护要求

系统安全防护能力包括但不限于：
a) 宜支持对病毒、木马的查杀，拦截恶意软件的攻击；
b) 不应存在已知或在CNVD、CNNVD等平台公布6个月以上的高危及以上等级漏洞。

7.4.2 安全更新要求

系统应具备更新机制，更新前应向用户提示更新内容的简要说明，供用户判断和选择。安全更新要求包括但不限于：
a) 系统更新时，应对更新文件的来源和完整性进行校验，并应具有原始数据备份能力，能够进行必要的回滚操作，避免更新失败导致系统失效；
b) 系统更新失败时，应保证系统的可用性并给予用户相应的提示；
c) 系统应具备通过补丁或软件升级的方式消除高危及以上等级安全漏洞的能力。

7.5 接口安全要求

7.5.1 业务接口安全

应具备防止越权攻击能力，避免未经授权的访问。

7.5.2 身份鉴别

身份鉴别要求包括但不限于：
a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
b) 应提供并启用用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；
c) 应提供并启用登录失败处理功能，可采取结束会话、限制非法登录尝试次数等措施；
d) 应支持对异常登录行为的审计功能。

7.5.3 访问控制

访问控制要求包括但不限于：
a) 应实现用户权限最小化管理，使用分权原则，避免发生权限被滥用等情况；
b) 疾病监测类可穿戴设备如具备多种用户角色，应对设备作用用户（被监测者）和设备操作用户（医护人员等）进行角色分离设置，在对角色权限控制的基础上，按照业务流程的需求触发操作授权。

7.5.4 网络端口安全

网络端口安全要求包括但不限于：

a) 不应存在未经声明的外围网络端口。
b) 设备网络端口不应泄露敏感Banner信息，防止攻击者获取后降低攻击难度。

7.6 应用软件安全要求

7.6.1 应用软件签名认证机制

医疗健康可穿戴设备运行的应用软件应采用认证签名机制，未经认证签名的应用软件仅当用户进行确认后才能执行下一步操作。

7.6.2 预置应用软件安全要求

预置应用软件不应存在后门等隐藏接口，不应存在已知或在CNVD、CNNVD等平台公布6个月以上的高危及以上等级漏洞，不应含有非授权收集或泄露用户信息、非法数据外传等恶意行为。

7.7 管理客户端安全

7.7.1 访问控制

客户端APP应能对访问者进行身份验证，只接受通过认证的用户的访问，同时应对敏感级数据进行访问权限控制。

7.7.2 数据安全保护

应加密存储敏感级数据，敏感级数据存储路径应设置严格的访问控制机制，避免数据泄露。用于加密的密钥应采取防护机制进行保存，避免被直接获取。

应禁止日志数据包含与用户数据相关的信息。

7.7.3 反逆向保护

应采取代码混淆、加壳等防护措施，实现客户端APP反编译保护。

7.7.4 反盗版保护

应采取签名机制，防止客户端APP被重打包。

7.7.5 防篡改攻击

应对程序的完整性、参数内容的完整性和有效性进行检查，以防御篡改攻击。

7.8 硬件安全要求

7.8.1 硬件功能安全

硬件功能实现应与提供给用户的说明文档相一致，不应存在未声明或隐藏的功能。例如应关闭隐藏调试功能，防止厂商在未获得用户授权的情况下获得对芯片内部的访问或芯片功能更改的能力。

7.8.2 硬件设计安全

硬件设计安全要求包括但不限于：

a) 硬件内部模块的安全属性和芯片间通信协议等安全实现应符合有关法律、行政法规和相关国家标准、行业标准要求，随机数熵源应达到相关标准要求；

b) 硬件资源支持密码算法的安全性应符合有关法律、行政法规和相关国家标准、行业标准要求，密钥的产生、分发、使用、存储、销毁应有相应安全保障机制；
c) 对于安全等级要求高的疾病监测类可穿戴设备，宜采用符合相关国家标准、行业标准要求的硬件安全模块进行密钥等数据的保护；
d) 应关闭不必要的下载、调试端口。

7.8.3 芯片安全能力

芯片安全能力要求包括但不限于：
a) 应具备容错能力，能够防御由针对芯片的故障注入攻击所导致的功能失效；
b) 对于支持安全模块的芯片，应具备固件芯片的物理写保护的功能，防止固件被篡改；
c) 对于支持安全模块的芯片，宜具备侧信道攻击防护能力；
d) 宜具备安全启动硬件保护能力；
e) 宜具备安全域隔离功能，提供可信执行环境；
f) 芯片宜使用拆卸存迹硬质涂层，防止直接观察、探测芯片内部，并在企图拆卸或移动芯片后留下证据；
g) 应开启芯片的读保护功能，防止固件被读取后进行逆向、篡改。

7.9 能耗保护安全能力

应具备抗能耗攻击能力，避免由于恶意的能耗攻击，导致设备电池电量快速耗尽而功能失效。

7.10 安全分级要求

根据医疗健康可穿戴设备的安全技术要求的强弱，将产品分为基础级和增强级，具体安全技术要求的等级划分如表2所示，其中增强级需同时满足基础级和增强级要求。

表 2 用户数据分级

安全技术要求	基础级	增强级
个人信息保护安全要求	7.1 a)、c)-e)	7.1 b)
无线通信安全要求	7.2	
传输安全要求	7.3.1 a)-c)； 7.3.2 a)、c)-e)； 7.3.3	7.3.1 d)； 7.3.2 b)
系统安全漏洞修复与更新要求	7.4.1 b)-d)； 7.4.2	7.4.1 a)；
接口安全要求	7.5.1-7.5.2； 7.5.3 a)； 7.5.4	7.5.3 b)
应用软件安全要求	7.6	
管理客户端安全	7.7	
硬件安全要求	7.8.1； 7.8.2 a)、b)、d)； 7.8.4 g)	7.8.2 c)； 7.8.3 a)-f)
能耗保护安全能力	7.9	

8 测试方法

8.1 个人信息保护安全测试

测试目的	7.1 个人信息保护安全要求
要求	a) 医疗健康可穿戴设备对用户数据中用户基本信息的收集通常应在提供相应服务的同时进行。出于业务需要而必须事先收集相关数据，应向用户明示事先收集的目的和范围，并且只有在用户同意的情况下方可继续。医疗健康可穿戴设备应向用户提供关闭数据采集功能； b) 疾病监测类可穿戴设备在关闭数据采集功能前，应对用户身份进行认证； c) 医疗健康可穿戴设备在将用户数据存储在终端内部时，敏感级信息应与监测诊疗数据分开存储。存储敏感级信息时，应采用加密形式保存； d) 医疗健康可穿戴设备若通过网络接口传输用户数据，应对数据进行加密，确保信息在网络传输过程中的安全； e) 医疗健康可穿戴设备终端不应有未向用户明示且未经用户同意，擅自修改、删除、转移或拷贝用户基本信息的行为。若将用户基本信息存储在终端内部，终端设备应提供相应选项，允许用户修改或彻底物理删除已存储的用户基本信息。
预置条件	保证设备正常运行；
测试步骤	a) 检查设备及控制端应用是否存在收集用户基本信息的行为，若存在收集用户基本信息的行为，判断其在收集前是否向用户明示收集的目的和范围，且征得了用户同意； b) 检查设备及控制端应用是否具备关闭数据采集功能，针对疾病监测类可穿戴设备，检查是否在关闭数据采集功能操作前对用户身份进行认证； c) 检查存储在终端内部的用户数据，是否将用户基本信息与监测诊疗数据分开存储； d) 读取设备上存储的数据，查看敏感级信息是否是加密存储； e) 抓包查看传输的数据是否进行了加密； f) 检查设备及控制端应用在修改、删除、转移或拷贝用户基本信息之前是否向用户明示且经用户同意； g) 检查设备及控制端应用是否提供修改或删除已存储的用户基本信息的选项。
预期结果	a) 设备及控制端应用不存在收集用户基本信息的行为；若存在收集用户基本信息的行为，则收集前明示用户收集目的和范围，并在收集前经过了用户同意； b) 具备关闭数据采集功能，疾病监测类可穿戴设备在关闭数据采集功能操作前对用户身份进行认证； c) 用户基本信息与监测诊疗数据在终端内部分开存储； d) 敏感级信息加密存储； e) 传输的数据进行了加密； f) 在修改、删除、转移或拷贝用户基本信息之前向用户明示且经用户同

	意； g) 提供修改或删除已存储的用户基本信息的选项。
实测结果	与预期结果一致
备注	无

8.2 无线通信安全测试

8.2.1 协议一致性测试

测试目的	7.2.1 协议一致性
要求	所采用 WLAN、蓝牙、ZigBee 等无线通信协议应支持设备授权认证、加密传输等安全扩展功能。
预置条件	保证设备正常运行；
测试步骤	检查设备所用通信协议配置信息，查看是否支持设备授权认证、加密传输等安全扩展功能。
预期结果	支持设备授权认证、加密传输等安全扩展功能。
实测结果	与预期结果一致
备注	无

8.2.2 协议健壮性测试

测试目的	7.2.2 协议健壮性
要求	应具备非法报文处理能力，当接收到非法报文时应能够正确处理，防止非预期的异常情况发生。
预置条件	保证设备正常运行；
测试步骤	检查设备所用通信协议配置信息，查看是否具备非法报文处理机制。
预期结果	具备非法报文处理机制。
实测结果	与预期结果一致
备注	无

8.3 传输安全测试

8.3.1 传输完整性测试

测试目的	7.3.1 传输完整性要求
要求	a) 医疗健康可穿戴设备各个执行主体之间在进行数据传输时，除传输数据主体外，应附加用于对数据进行完整性校验的校验信息； b) 医疗健康可穿戴设备各个执行主体之间在进行数据传输时，可根据传输不同分类级别的数据采用不同的数据完整性校验方法； c) 医疗健康可穿戴设备各个执行主体之间在进行数据传输时，应采用密码机制保证数据传输完整性，采用的密码机制应符合有关法律、行政法规和相关国家标准、行业标准要求； d) 在检测到传输数据的完整性遭到破坏时，应采取措施恢复或重新获取数据。
预置条件	保证设备正常运行；
测试步骤	a) 检查是否具有传输数据的完整性校验机制； b) 检查不同分类级别的数据是否采用不同的数据校验方法； c) 检查数据传输时是否具有密码机制，抓包查看传输的数据是否进行了

	加密，检查传输数据的加密算法； d) 抓包获取传输的数据，破坏其完整性，并发送完整性被破坏的数据，检查是否采取措施恢复或重新获取数据。
预期结果	a) 具有传输数据的完整性校验机制； b) 不同分类级别的数据采用不同的数据校验方法； c) 数据传输时具有密码机制，传输的数据进行了加密，加密算法符合要求； d) 可以恢复或重新获取数据。
实测结果	与预期结果一致
备注	无

8.3.2 传输机密性测试

测试目的	7.3.2 传输机密性要求
要求	a) 医疗健康可穿戴设备各执行主体之间在进行数据传输时，应采用密码机制对传输数据进行加密； b) 医疗健康可穿戴设备各执行主体之间对于敏感级数据的传输，应采用有必要安全强度的加密算法对数据进行加密； c) 医疗健康可穿戴设备各执行主体之间在传输加密数据时，应采用不同密钥的加密传输方式； d) 医疗健康可穿戴设备各执行主体之间传输数据时的加密算法应符合有关法律、行政法规和相关国家标准、行业标准要求； e) 医疗健康可穿戴设备各执行主体之间在进行数据传输时，若涉及密钥管理，密钥管理策略应能够解决周期密钥更新、密钥撤销和密钥分发等问题。
预置条件	保证设备正常运行；
测试步骤	a) 检查数据传输时是否具有密码机制，抓包查看传输的数据是否进行了加密； b) 检查敏感级数据传输时的加密算法； c) 检查数据传输时否每次采用不同密钥的加密传输方式； d) 检查传输数据的加密算法是否符合要求； e) 检查文档，若涉及密钥管理，查看是否保证密钥更新、密钥撤销和密钥分发等环节的安全性。
预期结果	a) 数据传输时具有密码机制，抓包查看传输的数据进行了加密； b) 敏感级数据传输时的加密算法符合要求； c) 具备每次采用不同密钥的加密传输方式； d) 传输数据的加密算法符合要求； e) 密钥管理方案能保证密钥更新、密钥撤销和密钥分发等环节的安全性。
实测结果	与预期结果一致
备注	无

8.3.3 传输抗重放测试

测试目的	7.3.3 传输抗重放要求
要求	a) 医疗健康可穿戴设备各执行主体之间在进行数据传输时，应采用机制防止数据包或报文的重排或重放；

	b) 医疗健康可穿戴设备各执行主体之间在进行数据传输时，可使用序列码或时间戳实现抗重放攻击； c) 医疗健康可穿戴设备各执行主体之间在进行数据传输时，可在数据中加入与当前事件有关的一次性随机数。
预置条件	保证设备正常运行；
测试步骤	a) 检查数据传输是否具有抗重放保护措施；若有，抓包传输的数据并将之重放，查看数据接收方的处理是否满足抗重放保护要求； b) 检查是否使用序列码或时间戳实现抗重放攻击； c) 检查是否使用随机数。
预期结果	a) 具备抗重放保护机制，数据接收方可识别重放数据并将其丢弃； b) 使用序列码或时间戳实现抗重放攻击； c) 使用随机数。
实测结果	与预期结果一致
备注	无

8.4 系统安全漏洞修复与更新测试

8.4.1 安全防护测试

测试目的	7.4.1 安全防护要求
要求	a) 宜支持对病毒、木马的查杀，拦截恶意软件的攻击； b) 不应存在已知或在 CNVD、CNNVD 等平台公布 6 个月以上的高危及以上等级漏洞。
预置条件	保证设备正常运行；
测试步骤	a) 检查是否支持对病毒、木马的查杀，拦截恶意软件的攻击； b) 使用漏扫工具查看是否存在已知或在 CNVD、CNNVD 等平台公布 6 个月以上的高危及以上等级漏洞。 注：对于 6 个月以上仍未公布漏洞修复方法的情况，可采取一定的补救措施，降低安全风险。
预期结果	a) 支持对病毒、木马的查杀，拦截恶意软件的攻击； b) 不存在已知或在 CNVD、CNNVD 等平台公布 6 个月以上的高危及以上等级漏洞。
实测结果	与预期结果一致
备注	无

8.4.2 安全更新测试

测试目的	7.4.2 安全更新要求
要求	a) 系统更新时，应对更新文件的来源和完整性进行校验，并应具有原始数据备份能力，能够进行必要的回滚操作，避免更新失败导致系统失效； b) 系统更新失败时，应保证系统的可用性并给予用户相应的提示； c) 系统应具备通过补丁或软件升级的方式消除高危及以上等级安全漏洞的能力。
预置条件	保证设备正常运行；
测试步骤	a) 启动系统更新，检查系统更新前是否对系统更新包、更新版本进行完整性校验并验证来源可靠性；

	b) 尝试使系统更新失败，验证设备是否恢复到更新前可用的版本，并给予用户相应提示； c) 检查系统是否具备通过补丁或软件升级的方式消除高危及以上等级安全漏洞的能力。
预期结果	a) 能安全更新系统； b) 统更新失败后，设备保持更新前系统版本，并提示用户； c) 具备通过补丁或软件升级的方式消除高危及以上等级安全漏洞的能力。
实测结果	与预期结果一致
备注	无

8.5 接口安全测试

8.5.1 业务接口安全测试

测试目的	7.5.1 业务接口安全
要求	应具备防止越权攻击能力，避免未经授权的访问。
预置条件	保证设备正常运行；
测试步骤	检查是否具备防止越权攻击能力，尝试进行未授权访问，检查是否能成功访问。
预期结果	具备防止越权攻击能力，未授权访问失败。
实测结果	与预期结果一致
备注	无

8.5.2 身份鉴别测试

测试目的	7.5.2 身份鉴别
要求	a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别； b) 应提供并启用用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用； c) 应提供并启用登录失败处理功能，可采取结束会话、限制非法登录尝试次数等措施； d) 应支持对异常登录行为的审计功能。
预置条件	保证设备正常运行；
测试步骤	a) 检查是否具备专用的登录控制模块对登录用户进行身份标识和鉴别； b) 检查是否具备并启用用户身份标识唯一和鉴别信息复杂度检查； c) 检查是否具备并启用登录失败处理功能； d) 检查是否具备对异常登录行为的审计功能。
预期结果	a) 具备专用的登录控制模块对登录用户进行身份标识和鉴别； b) 具备并启用用户身份标识唯一和鉴别信息复杂度检查措施； c) 登录失败后，能够结束会话、限制非法登录次数等措施； d) 具备对异常登录行为的审计功能。
实测结果	与预期结果一致
备注	无

8.5.3 访问控制测试

测试目的	7.5.3 访问控制

要求	a) 应实现用户权限最小化管理，使用分权原则，避免发生权限被滥用等情况； b) 疾病监测类可穿戴设备如具备多种用户角色，应对设备作用用户（患者）和设备操作用户（医护人员）进行角色分离设置，在对角色权限控制的基础上，按照业务流程的需求触发操作授权。
预置条件	保证设备正常运行；
测试步骤	a) 检查是否实现用户权限最小化管理，使用分权原则； b) 若设备有多种用户角色，检查是否进行了角色分离设置，并具备角色权限控制机制。
预期结果	a) 具备用户权限最小化管理机制，使用分权原则； b) 若设备有多种用户角色，进行了角色分离设置，并具备角色权限控制机制。
实测结果	与预期结果一致
备注	无

8.5.4 网络端口安全测试

测试目的	7.5.4 网络端口安全
要求	a) 不应存在未经声明的外围网络端口； b) 设备网络端口不应泄露敏感 Banner 信息，防止攻击者获取后降低攻击难度。
预置条件	保证设备正常运行；
测试步骤	a) 检查是否存在未经声明的外围网络端口； b) 检查设备网络端口是否泄露敏感 Banner 信息。
预期结果	a) 不存在未经声明的外围网络端口； b) 设备网络端口未泄露敏感 Banner 信息。
实测结果	与预期结果一致
备注	无

8.6 应用软件安全测试

8.6.1 应用软件签名认证机制测试

测试目的	7.6.1 应用软件签名认证机制
要求	医疗健康可穿戴设备运行的应用软件应采用认证签名机制，未经认证签名的应用软件仅当用户进行确认后才能执行下一步操作。
预置条件	保证设备正常运行；
测试步骤	检查应用软件是否采用认证签名机制，安装未经认证签名的应用软件，查看是否需要用户进行确认后才能执行下一步操作。
预期结果	具备认证签名机制，安装未经认证签名的应用软件，需要用户进行确认后才能执行下一步操作。
实测结果	与预期结果一致
备注	无

8.6.2 预置应用软件安全测试

测试目的	7.6.2 预置应用软件安全要求
要求	预置应用软件不应存在后门等隐藏接口，不应存在已知或在 CNVD、CNNVD

	等平台公布 6 个月以上的高危及以上等级漏洞，不应含有非授权收集或泄露用户信息、非法数据外传等恶意行为。
预置条件	保证设备正常运行；
测试步骤	a) 检查预置应用软件是否存在后门等隐藏接口； b) 漏扫查看是否存在已知或在 CNVD、CNNVD 等平台公布 6 个月以上的高危及以上等级漏洞； c) 检查是否含有非授权收集或泄露用户信息、非法数据外传等恶意行为。
预期结果	a) 不存在后门等隐藏接口； b) 不存在高危及以上等级已知或在 CNVD、CNNVD 等平台公布 6 个月以上的漏洞； c) 未含有非授权收集或泄露用户信息、非法数据外传等恶意行为
实测结果	与预期结果一致
备注	无

8.7 管理客户端安全测试

8.7.1 访问控制测试

测试目的	7.7.1 访问控制
要求	客户端 APP 应能对访问者进行身份验证，只接受通过认证的用户的访问，同时应对敏感级数据进行访问权限控制。
预置条件	保证设备正常运行；
测试步骤	a) 检查客户端 APP 是否对访问者进行身份验证，尝试未认证用户访问，检查是否访问成功； b) 检查客户端 APP 是否对敏感级数据进行访问权限控制。
预期结果	a) 客户端 APP 对访问者进行身份验证，未认证用户访问失败； b) 访问敏感级数据有权限控制。
实测结果	与预期结果一致
备注	无

8.7.2 数据安全保护测试

测试目的	7.7.2 数据安全保护
要求	a) 应加密存储敏感级数据，敏感级数据存储路径应设置严格的访问控制机制，避免数据泄露。用于加密的密钥应采取防护机制进行保存，避免被直接获取； b) 应禁止日志数据包含与用户数据相关的信息。
预置条件	保证设备正常运行；
测试步骤	a) 读取客户端 APP 存储的数据，检查敏感级数据是否为加密存储，加密的密钥是否具备防护机制进行保存； b) 检查客户端 APP 是否具备敏感级数据的存储路径的访问控制机制； c) 查看日志数据是否包含与用户数据相关的信息。
预期结果	a) 敏感级数据为加密存储，加密密钥具备防护机制进行保存； b) 具备敏感级数据的存储路径的访问控制机制； c) 日志数据不包含与用户数据相关的信息。
实测结果	与预期结果一致
备注	无

8.7.3 反逆向保护测试

测试目的	7.7.3 反逆向保护
要求	应采取代码混淆、加壳等防护措施，实现客户端 APP 反编译保护。
预置条件	保证设备正常运行；
测试步骤	使用工具查看客户端 APP 代码是否采取代码混淆、加壳等防护措施。
预期结果	采取代码混淆、加壳等防护措施。
实测结果	与预期结果一致
备注	无

8.7.4 反盗版保护测试

测试目的	7.7.4 反盗版保护
要求	应采取签名机制，防止客户端 APP 被重打包。
预置条件	保证设备正常运行；
测试步骤	检查 APP 是否具备签名信息。
预期结果	具备签名信息。
实测结果	与预期结果一致
备注	无

8.7.5 防篡改攻击测试

测试目的	7.7.5 防篡改攻击
要求	应对程序的完整性、参数内容的完整性和有效性进行检查，以防御篡改攻击。
预置条件	保证设备正常运行；
测试步骤	a) 将程序文件进行，破坏原程序文件的完整性，生成完整性被破坏的程序文件； b) 将步骤 1 生成的程序文件拷贝到客户端上，查看 APP 是否能正常安装启动。
预期结果	不能正常安装启动。
实测结果	与预期结果一致
备注	无

8.8 硬件安全测试

8.8.1 硬件功能安全测试

测试目的	7.8.1 硬件功能安全
要求	硬件功能实现应与提供给用户的说明文档相一致，不应存在未声明或隐藏的功能。例如应关闭隐藏调试功能，防止厂商在未获得用户授权的情况下获得对芯片内部的访问或芯片功能更改的能力。
预置条件	保证设备正常运行；
测试步骤	检查是否存在未声明或隐藏的硬件功能。
预期结果	不存在未声明或隐藏的硬件功能。
实测结果	与预期结果一致
备注	无

8.8.2 硬件设计安全测试

测试目的	7.8.2 硬件设计安全
要求	a) 硬件内部模块的安全属性和芯片间通信协议等安全实现应符合有关法律、行政法规和相关国家标准、行业标准要求，随机数熵源应达到相关标准要求； b) 硬件资源支持密码算法的安全性应符合有关法律、行政法规和相关国家标准、行业标准要求，密钥的产生、分发、使用、存储、销毁应有相应安全保障机制； c) 对于安全等级要求高的疾病监测类可穿戴设备，宜采用符合相关国家标准、行业标准要求的硬件安全模块进行密钥等数据的保护； d) 应关闭不必要的下载、调试端口。
预置条件	保证设备正常运行；
测试步骤	a) 检查硬件内部模块的安全属性和芯片间通信协议，查看安全实现是否符合有关法律、行政法规和相关国家标准、行业标准要求，随机数熵源是否达到相关标准要求； b) 检查硬件资源支持密码算法的安全性是否符合有关法律、行政法规和相关国家标准、行业标准要求，密钥的产生、分发、使用、存储、销毁是否有相应安全保障机制； c) 检查安全等级要求高的疾病监测类可穿戴设备是否采用符合相关国家标准、行业标准要求的硬件安全模块进行密钥等数据的保护； d) 检查是否关闭了不必要的下载、调试端口。
预期结果	a) 安全实现符合有关法律、行政法规和相关国家标准、行业标准要求，随机数熵源达到相关标准要求； b) 硬件资源支持密码算法的安全性符合有关法律、行政法规和相关国家标准、行业标准要求，密钥的产生、分发、使用、存储、销毁有相应安全保障机制； c) 安全等级要求高的疾病监测类可穿戴设备采用符合相关国家标准、行业标准要求的硬件安全模块进行密钥等数据的保护； d) 关闭了不必要的下载、调试端口。
实测结果	与预期结果一致
备注	无

8.8.3 芯片安全能力测试

测试目的	7.8.3 芯片安全能力
要求	a) 应具备容错能力，能够防御由针对芯片的故障注入攻击所导致的功能失效； b) 对于支持安全模块的芯片，应具备固件芯片的物理写保护的功能，防止固件被篡改； c) 对于支持安全模块的芯片，宜具备侧信道攻击防护能力； d) 宜具备安全启动硬件保护能力； e) 宜具备安全域隔离功能，提供可信执行环境； f) 芯片宜使用拆卸存迹硬质涂层，防止直接观察、探测芯片内部，并在企图拆卸或移动芯片后留下证据； g) 应开启芯片的读保护功能，防止固件被读取后进行逆向、篡改。
预置条件	保证设备正常运行；
测试步骤	a) 使用测试工具验证产品是否能够防御针对芯片的故障注入攻击；

	b) 检查安全模块的芯片是否具备固件芯片的物理写保护的功能； c) 检查安全模块的芯片是否具备侧信道攻击防护能力； d) 检查是否具备安全启动硬件保护能力； e) 检查是否具备安全域隔离功能； f) 检查芯片是否使用拆卸存迹硬质涂层； g) 检查是否开启芯片的读保护功能。
预期结果	a) 能够防御针对芯片的故障注入攻击； b) 安全模块的芯片具备固件芯片的物理写保护的功能； c) 安全模块的芯片具备侧信道攻击防护能力； d) 具备安全启动硬件保护能力； e) 具备安全域隔离功能； f) 芯片使用了拆卸存迹硬质涂层； g) 开启了芯片的读保护功能。
实测结果	与预期结果一致
备注	无

8.9 能耗保护安全能力测试

测试目的	7.9 能耗保护安全能力
要求	应具备抗能耗攻击能力，避免由于恶意的能耗攻击，导致设备电池电量快速耗尽而功能失效
预置条件	保证设备正常运行；
测试步骤	试试能耗攻击，检查是否具备抗能耗攻击能力。
预期结果	具备抗能耗攻击能力。
实测结果	与预期结果一致
备注	无

电信终端产业协会团体标准

智能可穿戴设备安全 医疗健康可穿戴设备安全技术要求与测试方法

T/TAF XXX—XXXX

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn