家用医疗器械数据采集及应用规范

1 范围

本文件给出了家用医疗器械的数据采集及应用的总体要求、数据参与角色及流通场景、数据采集、数据传输、数据存储、数据应用及数据安全的要求。

本文件适用于家用医疗器械数据的采集、传输、存储、应用。

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 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 38637.2 物联网 感知控制设备接入 第2部分：数据管理要求

GB/T 39725 信息安全技术 健康医疗数据安全指南

GB/T 40028.2 智慧城市 智慧医疗 第2部分：移动健康

DB32/T 4155.1 全民健康信息平台共享数据集规范 第1部分：基本健康档案

3 术语和定义

GB/T 25069及GB/T 39725界定的以及下列术语和定义适用于本文件。

3.1

家用医疗器械 household medical device

操作人员通过自主查阅说明书或咨询医师、产品售后服务人员后，可在家庭护理环境中使用的医疗器械。

3.2

家用医疗器械数据 household medical devices data

通过家用医疗器械及配套软件采集的数据，包括但不限于个人基本信息、生命体征参数、健康管理数据、设备运行数据等。

3.3

生命体征参数 vital sign parameters

用于判定人体生命特征的指征。

3.4

采集端 collection terminal

采集家用医疗器械数据的终端设备，包含硬件设备及应用软件。

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

CoAP：约束应用协议（Constrained Application Protocol）

DES：数据加密标准（Data Encryption Standard）

DDoS：分布式拒绝服务（Distributed Denial of Service）

DoS：拒绝服务（Denial of service）

DTLS：数据包传输层安全性协议(Datagram Transport Layer Security)

ECC：误差校正码（Error Correcting Code）

HTTP：超文本传输协议（Hyper Text Transfer Protocol）

LwM2M：轻量级机器对机器物联网协议（Lightweight Machine to Machine）

MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）

RSA：RSA加密算法（RSA algorithm）

TCP：传输控制协议（Transmission Control Protocol）

TLS：安全传输层协议（Transport Layer Security）

UDP：用户数据报协议（User Datagram Protocol）

URL：统一资源定位符（Universal Resource Locator）

SM1：商密1号算法（SM1 cryptographic algorithm）

SM2：商密2号算法（SM2 cryptographic algorithm）

SM4：商密4号算法（SM4 cryptographic algorithm）

3DES：三重数据加密算法（Triple Data Encryption Standard）

5 总体要求

家用医疗器械应取得国家、省、市药品监督管理局颁发的医疗器械注册证或备案凭证，分类应参考国家药品监督管理总局发布的《医疗器械分类目录》。数据采集、传输、存储、应用过程中应遵循：

a) 真实准确、完整有效，保持全过程一致性；

b) 传输至数据平台的数据应包含可识别数据主体的唯一标识 UNION_ID 或采集端设备的唯一标识 DEVICE_SN 或 APP_ID；

c) 数据平台方应明确数据开放及共享的范围，保护数据主体信息安全；

d) 应按照 GB/T 39725 中 6.2 的要求对采集的数据进行分级，针对不同等级的数据制定不同的安全策略,数据安全管理应满足 GB/T 39725 中第 9 章的要求。

6 数据参与角色及场景

6.1 数据参与角色

数据角色分为以下3类，特定场景下，个体或组织可承担多个角色：

a) 数据主体：家用医疗器械数据所标识的自然人；

b) 数据平台：参与家用医疗器械数据平台或系统研发及运维的相关组织；

c) 数据使用方：使用家用医疗数据的个人或组织，常见的数据使用方有：数据主体、综合医院、卫生院、妇幼保健院、诊所等医疗机构、医疗设备生产企业、及 OTC 药房、养老院、疗养院、护理院、健康管理中心等泛健康相关机构。

6.2 数据流通场景

数据流通场景分为以下4类，如图1所示：

a) 数据主体使用采集端设备，完成对数据主体信息的采集。同时，数据主体可以对相关的数据进行授权及管理；

b） 家用医疗器械将数据传输至数据平台，由数据平台进行存储、安全管理及应用管理；

c） 数据平台方按照第 10 章的要求，将数据授权给数据使用方进行使用；

d） 数据使用方基于授权的数据对数据主体提供产品及服务。

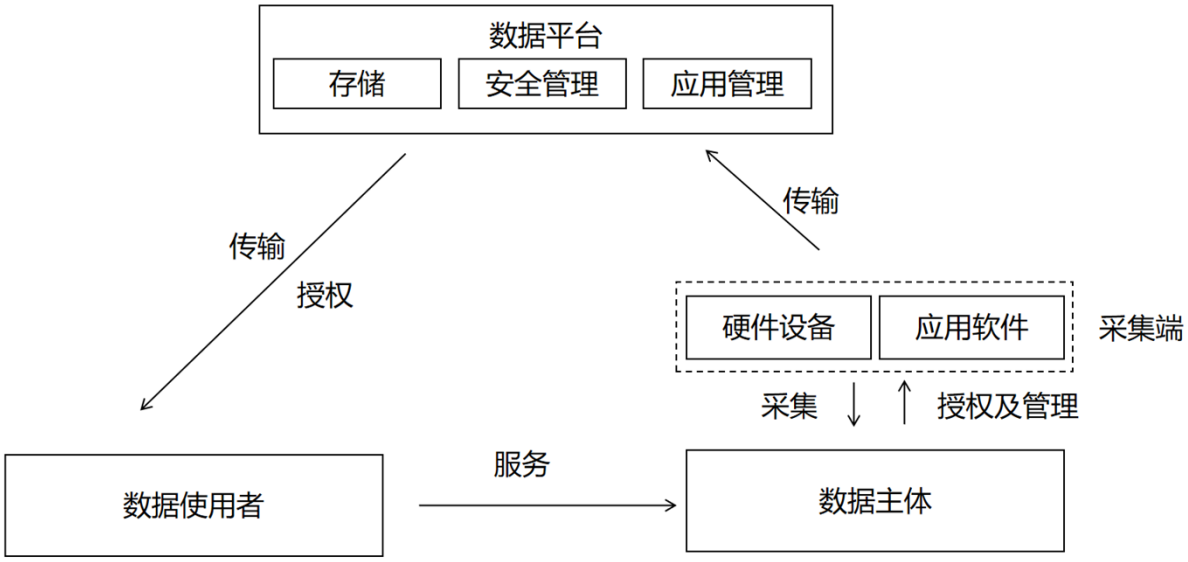

图1 数据流通场景示意图

7 数据采集

7.1 数据分类

家用医疗器械数据包括所有面向家庭的医疗硬件（见附录A）及相关软件通过直接或间接采集得到的数据，也包含对以上方式获取的数据进行二次加工得到的数据。数据形式涵盖：数值信号、编码、文字、图片、语音、视频。家用医疗器械数据分类应符合表1。

表1 家用医疗器械数据分类

数据类别	定义	范围	来源
个人基本信息	可单独或与其他信息结合能够识别特定自然人的数据	包括姓名、年龄、性别、国籍、籍贯、职业、婚姻状态、住址、手机号、身份证等	通过应用软件录入
生命体征参数	用于判定人体生命特征的指征	包括体温、心率、心电图、血糖值、血压值、呼吸、血氧、尿酸、血红蛋白等	由硬件设备收集或软硬件联调采集
健康管理数据	与个人健康、饮食、运动、生活方式、情绪相关的数据	包括饮食食谱、运动时长、睡眠时长、睡眠深度等	通过应用软件录入或软硬件联调采集
设备运行数据	家用医疗器械设备信息及运行状态参数	包括设备类型、设备 ID、运行时长、维修及校准信息、故障代码、故障产生时间、开/关	由硬件设备收集

		机时间等	

7.2 数据内容及格式

7.2.1 个人基本信息

个人基本信息采集应符合附录A.1的要求，应包含UNION_ID（见9.1）。

7.2.2 生命体征参数

生命体征参数的采集方法包括硬件直接采集和软硬件联调采集两种，操作人员应按照产品说明书规范进行操作。不同类型家用医疗器械采集的数据应符合附录A.2的要求。如有其他类型的家用医疗器械数据，采集信息中应包含UNION_ID或DEVICE_SN、使用时间及主要设定参数。其中，具有生命体征参数检测功能的器械应包含测量时间及测量值。

7.2.3 健康管理数据

健康管理数据可通过应用软件录入或软硬件联调采集。不同类型健康管理数据应符合附录A.3的要求。如有其他类型健康管理数据，采集信息应包含UNION_ID及APP_ID。

7.2.4 设备运行数据

设备数据应符合附录A.4的要求，通过硬件设备采集时应包含DEVICE_SN，通过应用软件采集时应包含APP_ID。

7.3 采集授权

采集数据前，应取得数据主体授权，应符合GB/T 35273-2020中第5章的要求。用户协议中应说明数据的使用目的、使用场景及可能产生的后果，应明确数据使用方的类型、身份及数据安全能力。

8 数据传输

8.1 采集端到数据平台

采集端到数据平台之间的数据传输应满足以下要求：

a) 硬件设备采集应使用 MQTT、HTTP、CoAP、LwM2M 等物联网传输协议；

b) 应用软件采集应使用 HTTPS 传输协议；

c) 数据采集内容需要加密传输；

d) 数据平台接收数据时应有数据完整性验证；

e) 数据传输到平台应有重发机制、异常处理机制保证数据传输的稳定。

8.2 数据平台到数据使用方

数据平台到数据使用方之间的数据传输应满足以下要求：

a) 应采用 TLS、DTLS 等加密方式传输；

b) 数据平台的数据推送应有重发、超时、异常处理机制保证数据传输稳定。

8.3 数据接口

8.3.1 硬件数据传输接口

硬件采集的信息包含设备运行的状态和事件，事件一般包含需要被外部感知和处理的通知信息，可包含多个输出参数。硬件可通过topic实现消息的发送和接收，从而实现服务端与设备端的通信。数据应按照9.1定义的tablename进行上传。

a) 状态 topic 应符合以下格式内容要求：

1) 上报设备属性：/{tablename}/{DEVICE_SN}/properties/report；

2) 上报内容：应符合附录表 A.20、表 A.22 的要求；

3) 上报格式：json。

b) 事件 topic 应符合以下格式内容要求：

1) 上报测量事件：/{tablename}/{DEVICE_SN}/event；

2) 上报内容：应符合附录表 A.2～表 A.9 的要求；

3) 上报格式：json。

8.3.2 软件数据传输接口

通过应用软件传输时数据接口应符合以下要求：

a) 软件采集的数据通过服务器之间进行通讯，应采用 HTTPS API 接口模式通讯；

b) 请求方式应采用 POST，数据格式应采用 json；

c) 数据应按照 9.1 定义的 tablename 进行上传；

d) URL 应符合格式：https://域名:端口/api/upload/{tablename}/{APP_ID}；

e) 接口内容应符合附录表 A.2～表 A.19；

f) 响应参数应符合表 2 内容及格式。

表2　软件数据传输响应参数内容及格式

参数名	数据类型	长度	必选/可选	描述	说明或允许值
RESULT	Varchar	10	必选	请求结果	
MESSAGE	Varchar	100	必选	描述	

8.3.3　数据开放接口

数据开放接口规定了数据从数据平台传输至数据使用方的接口规范，应符合以下要求：

a)　开放的数据通过服务器之间进行通讯，应采用 HTTPS API 接口模式通讯；

b)　请求方式应采用 GET，数据格式应采用 json；

c)　URL 应符合格式：https://域名:端口/api/query/data；

d)　返回数据格式应使用 json；

e)　请求参数应符合表 3 内容及格式要求；

f)　响应参数应符合表 4 内容及格式要求。

表3　数据开放请求参数内容及格式

参数名	数据类型	长度	必选/可选	描述	说明或允许值
UNION_ID	Varchar	40	可选	用户唯一标识	如请求参数不包含 DEVICE_SN，则为必选
DEVICE_SN	Varchar	20	可选	设备号	如请求参数不包含 UNION_ID，则为必选
TABLE_NAME	Varchar	20	必选	数据类型	
START_TIME	Datetime	20	必选	开始时间	格式：yyyy-MM-dd HH:mm:ss
END_TIME	Datetime	20	必选	结束时间	格式：yyyy-MM-dd HH:mm:ss
CURRENT_PAGES	Number	5	必选	当前页数	
QUANTITY_PER_PAGES	Number	5	必选	每页数量	

表4　数据开放响应参数内容及格式

参数名	数据类型	长度	必选/可选	描述	说明或允许值
UNION_ID	Varchar	40	可选	用户唯一标识	如请求参数不包含 DEVICE_SN，则为必选

DEVICE_SN	Varchar	20	可选	设备号	如请求参数不包含 UNION_ID，则为必选
TABLE_NAME	Varchar	20	可选	数据类型	
DATA_LIST	List	/	可选	组装的 json 数据	符合采集的数据
CURRENT_PAGES	Number	5	可选	当前页数	
PAGE_COUNT	Number	5	可选	总页数	
RESULT	Number	1	必选	请求结果	0 正常，1 异常
MESSAGE	Varchar	100	必选	描述	

9 数据存储

9.1 数据结构

数据存储结构应符合以下要求：

a) 数据平台应记录每条上报数据的数据状态和数据上传时间，并对每条上传数据建立唯一标识 U_ID，具体内容见表 5。新增数据应与采集端上报的数据合并存储；

表5 存储新增内容及格式

参数名	数据类型	长度	必选/可选	描述	说明或允许值
U_ID	Varchar	40	必选	数据唯一标识	
DATA_FLAG	Number	1	必选	数据状态	0 删除，1 正常
UPLOAD_TIME	Datetime	20	必选	上传时间	格式：yyyy-MM-dd HH:mm:ss

注：个人基本信息汇总表（附录表A.1）无需存储uId。

b) 数据平台应建立统一的用户唯一标识 UNION_ID 的规则,并要求采集端按照规则进行数据上报，常见的 UNION_ID 有：身份证、手机号等。平台应对上传数据中的 UNION_ID 进行验证，若上传的 UNION_ID 在平台数据库中已存在，应将上传数据与已存数据进行关联；

c) 数据平台应定义不同类型数据的表名 tablename，上报至平台的数据应按照定义的 tablename 解析后进行分类存储；

d) 每个数据主体对应在个人基本信息汇总表中仅存储一条数据，个人基本信息表中的每条属性应以最新上传的数据进行存储。

9.2 存储要求

数据存储应符合以下要求：

a) 数据存储的通用要求与数据存储的调度、监控、管理、备份，应符合 GB/T 38637.2 中 6.2 数据存储的要求；

b) 数据平台应有双机备份机制；

c) 数据平台应建立数据异常处理机制，在数据提交异常时，数据平台管理人员应执行回滚后的处理方案；

d) 数据平台应设定数据存储的有效期，应制定数据失效后的销毁机制；

e) 数据平台应存储数据操作的日志记录，包括数据的接收、授权、调用、更改、删除等，能追踪完整的操作轨迹。

10 数据应用

10.1 典型应用场景

10.1.1 数据主体

对数据应用的场景包含但不限于：

a) 监测个人健康状况；

b) 查看历史数据。

10.1.2 医疗器械生产、经营企业

对数据应用的场景包含但不限于：

a) 了解设备运行状况，及时排除设备故障，提升设备维修效率；

b) 分析用户使用习惯和痛点，优化、升级产品；

c) 为用户提供服务，如指导使用器械、售后服务等。

10.1.3 医疗机构

对数据应用的场景包含但不限于：

a) 筛查预防：适用于制定临床筛选标准，依据用户数据构建可疑病例的筛选模型，对符合的可疑病例进行线下核实处置；

b) 疾病诊断：适用于医生在提供诊疗服务过程中调阅用户相应的居家监测数据，并进行医学诊断的场景，包括线上远程医疗、互联网医院在内的线上诊疗服务；

c） 随访监测：适用于居家健康管理监测的场景，用户居家进行自我调节，及早发现问题并进行干预。医生在诊后实时把控患者健康状况，辅助患者复诊或康复治疗；

d） 预后疗效跟踪：适用于跟踪用户接受治疗后的健康状况。

e） 紧急救助：适用于在紧急情况如突发事件、重大疾病下调用数据，辅助医生进行诊断及救助；

f） 医疗资源分配：适用于根据区域内人群的健康数据，统筹再分配医疗资源，包括人员、场地、设备等；

g） 公共卫生政策制定；

h） 不良反应上报及分析。

10.1.4 泛健康相关机构

对数据应用的场景包含但不限于：

a） 通过数据分析，为用户或患者提供服务及产品，如慢病管理服务、会员营销及管理、线上咨询用药等；

b） 通过数据驱动服务模式创新及管理模式创新。

10.1.5 医学科研机构

对数据应用的场景包含但不限于：

a） 疾病大数据分析；

b） 临床诊疗预测；

c） 医疗质量监测评估；

d） 专科疾病干预策略研究；

e） 医疗器械效果评估；

10.2 应用授权

数据应用应包含数据的授权，数据授权应符合以下要求：

a） 数据使用方在获取数据前，应向数据平台发送授权申请。申请应包含使用范围、使用期限、使用目的、使用方式；

b） 数据平台应成立数据管理委员会，对数据使用方的申请进行审批，基于使用人身份、使用场景、及使用目的制定授权策略，明确授权数据的范围、类型及方式；

c) 数据使用方以数据接口或平台开放的入口形式进行数据查询时，需每次进行身份验证。身份验证方式包括账号口令、基于数字证书的身份认证、生物特征识别认证等多因素结合的认证方式；

d) 接入平台的设备应向数据主体提供进入平台的入口。数据主体对与其相关的数据进行操作前，应进行身份验证；

e) 未经授权，数据使用方不得用作授权以外的其他用途或进行二次授权，包括但不限于商业推广、商业活动等；

f) 数据使用者如不必要持有数据授权权限（如数据使用业务被取消），数据平台应收回数据权限；

g) 平台应制定紧急访问策略，在紧急的情况(如抢救、急救)下,临床用户能够在不使用个人身份标识或未经授权的情况下对健康数据进行访问。

11 数据安全

11.1 采集端

应符合以下安全要求：

a) 采集端应采用加密算法对隐私数据和重要业务数据等敏感信息进行加密保护；对称算法应至少支持 SM1、SM4、DES、3DES 中的一种，非对称算法应至少支持 SM2、RSA、ECC 中的一种；

b) 采集端安全加密的等级应至少达到国家密码管理局国密 1 级要求。

11.2 传输

11.2.1 传输完整性

数据传输过程中应具备完整性校验机制，包括但不限于采集端与数据平台的传输，数据平台与数据使用方的传输。完整性校验机制应包含鉴别信息、隐私数据、数字签名和重要业务数据等数据。

11.2.2 传输通道加密

数据在采集端与数据平台、数据平台与数据使用方的传输过程中，应采用TLS或DTLS等加密协议方式传输，并执行证书校验。

11.3 平台

11.3.1 平台接入

数据平台在从采集端接收数据时应制定：