ICS 33.050
CCS M30

团　体　标　准

T/CCSA 789 –2026 T/CABEE 126-2026

基于智能家居的居家社区养老总体要求

General technical requirements of smart home based care for elderly with smart property

2026－03－02 发布　　2026－06－01 实施

中国通信标准化协会　中国建筑节能协会　发 布

版权声明

邮箱： IPR@ccsa.org.cn biaoban@cabee.org

电话： 010-62302847 010-57811281

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。

本文件由中国通信标准化协会和中国建筑节能协会提出并归口。

本文件起草单位：深圳市招商观颐养老服务有限公司、泰康保险集团股份有限公司、中国信息通信研究院、山东省建筑设计研究院有限公司、维沃移动通信有限公司、浙江大学华南工业技术研究院、中移（杭州）信息技术有限公司、中国电信集团有限公司、中国移动通信集团有限公司、中兴通讯股份有限公司、威凯（深圳）检测技术有限公司、华为终端有限公司、北京小米移动软件有限公司、高通无线通信技术（中国）有限公司、北京三星通信技术研究有限公司、OPPO广东移动通信有限公司、飞利浦（中国）投资有限公司、中国联合网络通信集团有限公司、博鼎实华（北京）技术有限公司、广东中创智家科学研究有限公司、郑州信大捷安信息技术股份有限公司、航天正阳健康科技（北京）有限公司、泛海物业管理有限公司、北京百度网讯科技有限公司、招商局积余产业运营服务股份有限公司、上海优必选智慧健康科技发展有限公司、河北泓毅环保科技有限公司、泰康之家经营管理有限公司、北京协力人口与社会发展研究所、中国人民大学社会与人口学院老年学研究所、深圳市金融商会、北京天驰君泰律师事务所、中外建设信息有限责任公司、北京易住行技术有限公司、北京中物智汇信息科技股份公司、长城物业集团股份有限公司、北京首开寸草养老服务有限公司、深圳数智乐居科技有限公司、知真行远数字技术（杭州）有限责任公司。

本文件主要起草人：李玉琳、柴文忠、刘政、马虹、庞帅、文艳红、刘春生、周斌、尚治宇、陈奇、刘思阳、姚兴宇、王亚忠、曹宇琼、贾景润、田更、徐龙杰、赵奕捷、施超、金剑超、丁雪莲、马伟、徐嘉利、叶扬韬、安康、史振宁、沈传军、赵牧、刘洋、吴越、吕小强、张峰昌、温锋、马凡、黄伟彬、刘献伦、贾云竹、张冬梅、李野、于文龙、王安格、王鹏、赵波、吴镝、毕建奎、朱文芳、黄万崇、胡晓晓、焦德明、孔丽丽、李春俐、李志建、刘兵伟、刘力铱、刘鹏、刘善武、马宏波、倪赤丹、仇晨卉、孙福临、王沁、吴可欢、杨熙、周杰、朱涛、廖景明、常城。

基于智能家居的居家社区养老总体要求

1 范围

本文件规定了基于智能家居的居家社区养老总体技术要求，包括居家社区养老系统的应用服务及相应的家庭、社区和城市基础设施要求，以及基于智能家居的居家社区养老服务系统中具备的功能、通用要求和信息安全要求。

本文件适用于智慧康养场景下的智能家居产品研发、平台搭建、项目运营和必要基础设施等。

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 9706.1-2020 医用电气设备 第1部分：基本安全和基本性能的通用要求

GB/T 21741 住宅小区安全防范系统通用技术要求

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 30147 安防监控视频实时智能分析设备技术要求

GB 35114 公共安全视频监控联网信息安全技术要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 38671-2020 信息安全技术 远程人脸识别系统技术要求

GB/T 41772-2022 信息技术 生物特征识别 人脸识别系统技术要求

GB/T 41819-2022 信息安全技术 人脸识别数据安全要求

GB/T 42981-2023 信息技术 生物特征识别 人脸识别系统测试方法

GB/T 44248-2024 信息技术 生物特征识别 人脸识别系统应用要求

GB 50348 安全防范工程技术标准

GA/T 1127 安全防范视频监控摄像机通用技术要求

YY 9706.111-2021 医用电气设备 第1-11部分：基本安全和基本性能的通用要求 并列标准：在家庭护理环境中使用的医用电气设备和医用电气系统的要求

YY 9706.102-2021 医用电气设备 第 1-2 部分：基本安全和基本性能的通用要求 并列标准：电磁兼容 要求和试验

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能家居系统 smart home system

利用家庭网络技术将家庭中各种通信设备、家用电器、家庭安保等装置连接到家庭智能化系统上进行集中的通信、监视、控制和家庭事务管理，以给智能家居用户提供便利舒适、安全、高效、环保的家庭生活的设备、网络、平台、应用的总称。

[来源：GB/T 39579-2020,3.1]

3.2

智慧社区 Smart community

运用信息通信技术，有效整合各类社区管理系统，推动社区管理和服务精细化，提升社区管理和服务水平，实现可持续发展的一种新型社区。

[来源: GB/T 42455.1-2023,3.1]

3.3

居家社区养老服务 home and community-based elderly care services

以家庭为基础、城乡社区为依托、社会保障制度为支撑，由政府提供基本公共服务，企业、社会组织提供专业化服务，村民委员会、居民委员会和志愿者提供公益互助服务组成的社会化养老活动。

3.4

智能家居云服务平台 smart home application cloud

通过网络统一组织和灵活调用各种智能家居信息资源，实现智能家居信息大规模计算的处理方式。其利用分布式计算和虚拟资源管理等技术，通过网络将分散的ICT资源（包括计算与存储、应用运行平台、软件等）集中形成共享的智能家居资源池，并以动态按需和可度量的方式向用户提供服务。

注：在本文件中，智能家居云服务平台简称为“云平台”。

[来源：YD/T 4657-2024，3.3]

4 缩略语

下列缩略语适用于本文件。

ABAC：基于属性的访问控制 （Attribute Based Access Control）

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

BLE：低功耗蓝牙 （Bluetooth Low Energy）

CoAP：受限应用协议 （Constrained Application Protocol）

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

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

NB-IoT：窄带物联网 （Narrow Band Internet of Things）

PLC：电力线通信 (Power Line Communication)

RBAC：基于角色的访问控制 （Role-Based Access Control）

USB：通用串行总线 （Universal Serial Bus）

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

5 系统架构

基于智能家居的居家社区养老系统总体架构包括设施与设备层、系统与平台层、应用与场景层三部分，如图1所示。

设施与设备层包括但不限于健康体检设备、睡眠监测设备、呼叫终端设备、视频监控设备、人脸识别设备等智慧养老设备，以及智慧监控系统、远程医疗网络、应急响应中心等智慧养老设施。设施和设备装配、部署于家庭内部或社区养老服务中心。

系统与平台层是基于智能家居的居家社区养老系统总体架构的核心层，以及通信网络等，负责设备接入、设备管理、数据上报，实现居家养老信息的感知与控制执行，以及对传输到系统与平台的数据进行存储分类和处理分析，提取出有价值的信息，并对这些信息进行管理和控制，支撑居家养老应用服务。其中各基础设施和平台为跨家庭和社区的总体性提供支撑能力，为各社区养老服务提供共性数据服务。

应用与场景层主要负责将处理后的数据应用到各个场景与服务中，实现系统管理、健康管理、健康监测、智能报警、信息发布等应用场景下的智能化管理和控制，各社区依据本社区需求选定必要场景进行建设，以满足不同居家养老业务服务的需求。

附录A中提供了一种典型的基于智能家居的居家社区养老服务模式的介绍。

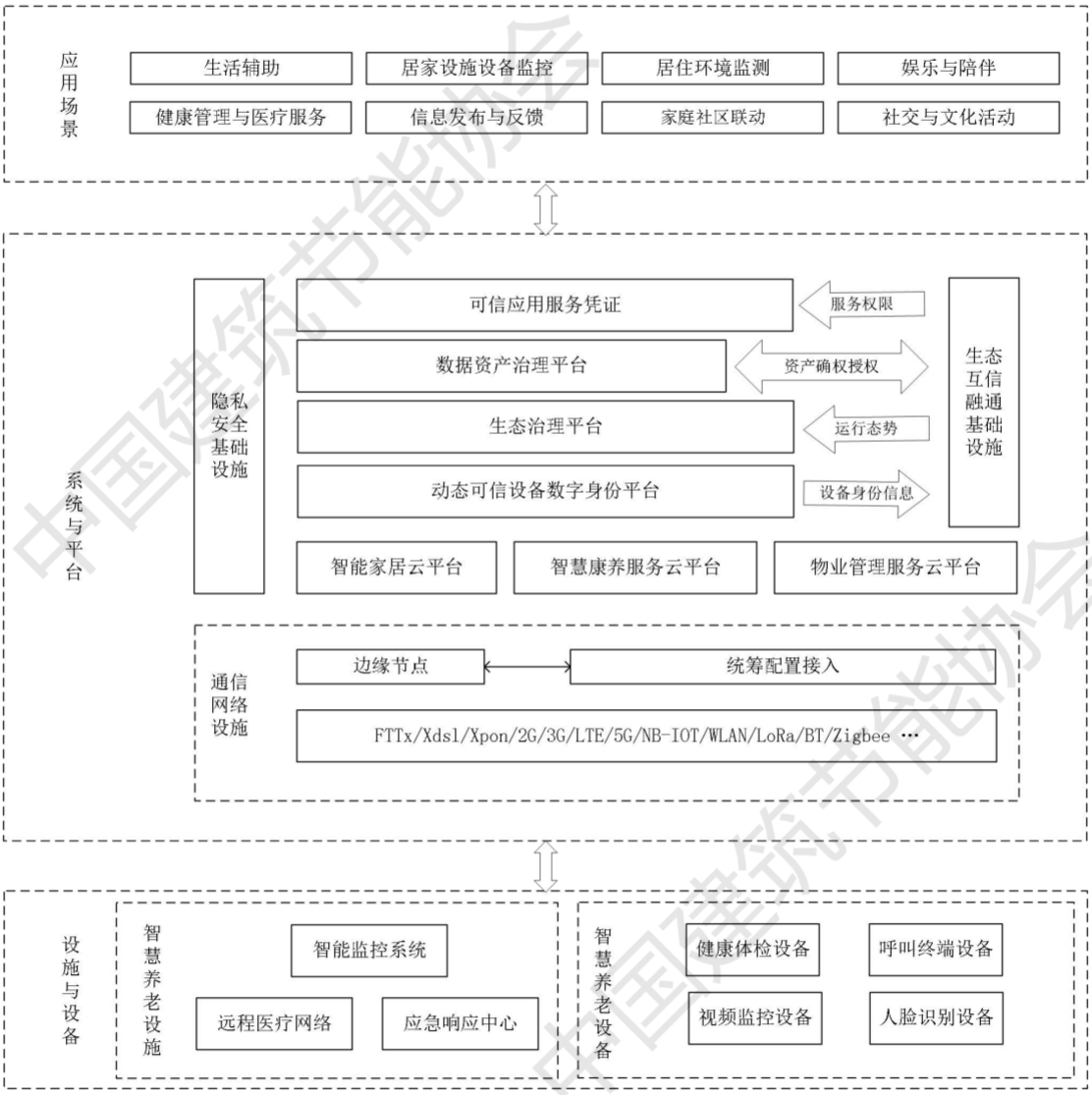

图 1　基于智能家居的居家社区养老系统总体架构

6　应用服务

6.1　健康管理与医疗服务

利用智能家居设备实现老年人健康状况的实时监测和医疗服务的便捷接入。设备通过蓝牙或WLAN将数据传输至终端设备，实现远程监控及报警。智能家居系统可与医疗服务提供商

的健康系统相连接，实现医疗信息的对接和交互。在紧急情况下，智能家居系统能自动触发报警并呼叫救援服务。

6.2 生活辅助服务

智能家居设备可相互连接和协同工作，形成高度集成的智能家居生态系统。老年人可通过语音指令或智能终端发出控制命令。

6.3 居住环境监测

通过各种传感器实时监控家庭环境的安全和舒适性。传感器可检测室内的温度、湿度、空气质量、噪声等参数。检测到异常情况，智能家居系统会报警并自动调节相应家电设备的运行，以维持室内环境的舒适度。

6.4 居家设施设备监控

允许用户远程监控家中的各种电器设备，通常包括安全摄像头、门窗传感器、水浸传感器、烟雾和一氧化碳探测器、智能白电设备等。用户可通过智能终端实时查看家中设备运行及能耗情况，接收安全警报和故障警报，并在需要时进行远程操作。

6.5 社交与文化活动

依托平台促进老年人之间的交流互动，帮助老人参与更多的社会活动。用户在平台上分享生活经验、提供互助信息、报名线下文化活动，或直接参与各种线上文化活动。

6.6 信息发布与反馈

主要涉及智能家居系统中的信息通知功能，以及老年人与服务提供者之间的互动。智能家居系统可通过智能音箱、手机应用等形式向老年人及其亲属或者物业服务企业发布安全警报、健康提醒、社区活动通知等各种信息；老年人也可通过智能家居系统反馈自己的需求和问题。

6.7 家庭社区联动

社区网格员可与安装智能家居设备的家庭实现家庭社区联动处置，流程包括初步评估、现场处置、信息上报、后续跟进、记录与总结等。智能家居设备检测到紧急情况时能将告警消息实时发送给社区网格员或相关机构，启动联动处置流程为老人提供服务，并可为家庭成员、社区网格员提供相关培训服务。

6.8 娱乐与陪伴

通过智能技术为老年人提供丰富多彩的娱乐活动和情感陪伴。老年人可通过语音指令或简单的触控操作访问各种娱乐内容；利用大数据和人工智能技术，相关系统可根据老年人的访问历史、娱乐偏好等，提供个性化的娱乐内容推荐；智能陪伴机器人可与老年人进行日常对话等陪伴服务。

7 设备要求

7.1 概述

用于养老的智能化基础设施，指集成物联网、大数据等技术的社区或居家养老基础设施，包括智能监控系统、远程医疗网络及应急响应中心等。用于养老的智能化基础设备，主要指

服务于老年人的智能化终端产品和物联网感知设备，包括但不限于健康监测手环、跌倒报警器、语音交互设备、智能家居控制器、康复机器人及门禁、监控等相关设备。智慧养老设施设备需满足下列条件：

a) 设备须通过国家强制性认证，严格遵守《中华人民共和国无线电管理条例》，按照《中华人民共和国无线电频率划分规定》和《微功率短距离无线电发射设备目录和技术要求》使用规定频段；

b) 设备应支持 WLAN、BLE、PLC、NB-IoT 等一种或多种通信方式，并确保数据传输过程符合本文件 9．5 节中的数据安全要求；

c) 设备应具备优异的监测能力和准确率，具备区域动态监测、跌倒监测、卫生间滞留超时监测、坠床监测等告警功能；

d) 睡眠监测设备能对老年人在睡眠状态下的呼吸频率、心率变异和翻身次数等状态进行监测，并基于相关监测数据实现睡眠状态评估功能。设备应提供精细化的睡眠监测，包括生成检测报告、离床过久和卧床过久监测告警功能，所有监测功能的识别准确率均应高于 95%，并支持相关阈值配置；

e) 设备应具备自检功能，能监测自身故障并告警，当发生故障且无法自愈时，应及时上报故障信息，以防止漏检情况的发生；

f) 所有监测和告警功能应支持电话、短信、微信等多种通知方式，确保紧急联系人能及时接收到告警信息并采取相应应急措施。

7.2 健康体检设备

健康体检设备是对老年人的生理医学指标进行检测的设备，能实现对老年人血氧、血压、心率等生理指标的测试，实现对老年人身体健康状态的持续监测。健康体检设备需满足以下要求：

a) 设备应符合 GB 9706.1-2020、YY 9706.111-2021 关于医用电气设备基本安全、基本性能以及在家庭护理环境中使用的相关强制性安全标准要求；

b) 设备应符合 YY 9706.102-2021、YY 9706.111-2021 关于电磁兼容性相关标准要求，确保在预期使用环境中的正常工作；

c) 设备的测量数据（如血压、血氧饱和度、心率等关键生理参数）应准确可靠，满足临床健康监测的基本精度要求；

d) 设备与人体直接接触的部分，其材料应安全无害，符合医疗器械生物学评价标准；

e) 设备应具备必要的稳定性和重复性，确保测量结果可信；

f) 预期用于医疗用途，设备应取得医疗器械注册证。

7.3 呼叫终端

呼叫终端指具备紧急呼叫功能的终端设备，老年人在紧急情况下能通过按键、语音等方式利用该终端设备向相关人员或机构发出求救或报警信号。

对于基于运营商网络通信的居家养老主设备，应按照相关的通信行业标准支持紧急呼叫功能，并符合以下要求：

a) 电源方式：设备可支持 USB 长供电或电池供电方式，且需配备应急电源，当发生停电等异常情况时，确保设备可用；

b) 通信方式：设备应具备 4G/5G、NB-IoT、WLAN 等之一方式进行传输，确保信号稳定及设备稳定性；

c) 交互方式：求救信号发出后，需要通过语音、灯光、蜂鸣等方式，明确告知用户当前的求救信号发送及处理状态。

对于非通信运营商签约类的设备，比如基于家庭WLAN网络和居家养老服务商签约的设备，应具备紧急呼叫实体按键，在此基础之上可通过语音或屏幕点击按键的方式，进行音频或视频紧急呼叫。同时，服务商应确保紧急呼叫的接听和转接，避免无人接听或者无法转接的情况。

7.4 视频监控设备

视频监控设备通过摄像头对居家养老相关环境进行视频记录，可拓展本机存储及报警等功能，实现对居家养老环境的视频监测与记录、危险信息提示。视频监控系统符合下列要求：

a) 监控范围应覆盖建筑周界及各出入口、停车库（场）出入口、主干道、消防通道、重点公共区域等关键位置；
b) 视频监控终端应符合 GA/T 1127 的规定，视频监控系统与其他平台对接、多级联网，信息传输、交换、控制协议应符合 GB/T 28181 的规定；
c) 宜具备可疑人员越界告警、可疑人员滞留监控、特殊用房入侵告警、周界盲点与死角监视、遮挡报警等功能；
d) 其他功能应符合 GB 50348、GB 35114、GB/T 21741、GB/T 30147 的规定。

7.5 人脸识别设备

通过人脸识别功能，实现居家养老环境下对服务人员的身份确认，从而达到人员行动登记以及安全管理的目标。人脸识别设备符合下列要求：

a) 设备应支持用户注册人脸识别系统，允许兼容不同图像源，包括实时视频、录像视频和相片，应能显示已注册用户和人脸图像的数量，以及最大容量；
b) 设备在接收到待识别人脸图像时，应能快速给出识别结果，实时显示状态信息，并提供对已注册用户和人脸图像的查询、删除等管理功能；
c) 设备应具备稳定的数据存储能力，即使在电源断电或更换电池的情况下，也能确保已保存的人脸信息和识别记录不丢失；
d) 设备需同时满足GB/T 41819-2022关于数据安全和GB/T 41772-2022关于技术性能的双重标准，并通过 GB/T 42981-2023 的第三方测试；
e) 其他功能应符合 GB/T 38671-2020、GB/T 44248-2024 和《人脸识别技术应用安全管理办法》的规定。

8 平台要求

8.1 智能家居云平台

智能家居云平台以统一业务功能平台的方式，维护和管理智能家居系统内的各类网关、传感器和终端设备等，主要包括终端管理、数据管理、状态管理、事件管理、业务控制、应用服务提供等功能单元，并以统一的开放接口方式采集传感器和终端设备的状态数据、管理网关和终端设备、提供智能家居综合业务服务，以方便与智慧居家养老等场景相结合。智能家居云平台应具备以下功能：

a) 规范接入设备的模型，使用标准的文件格式；
b) 支持设备配网身份验证，设备配网身份验证流程应采用设备许可码的方式，由设备的云平台生成，并在出厂时在应用终端侧进行预置；
c) 支持智能家居场景的基础数据模型，以及云平台之间智能家居场景的互联互通；

d) 能接入各种不同类型的设备：传感器、监控摄像头、智能手表等。同时应考虑设备的兼容性，以确保各种设备可顺利地接入和使用。医疗设备须具备对应医疗认证资质；

e) 确保设备接入的稳定性，在网络环境差或断网的环境也要能工作，数据在网络恢复正常后，能做自动补偿；

f) 支持设备管理功能，包括查看设备列表中设备的信息，设备的添加、绑定、解绑、删除、修改、场景联动、报警通知、设备生命周期管理以及设备数据的分析和上传展示分析；

g) 支持不同人员登录使用，使整个系统中使用人员的账号统一存储并用于系统登录；并支持账号在不同平台使用，使用户能在网页端和应用程序端中账号互通；

h) 支持多种数据的管理，通过数据管理对数据进行分析，给予用户个性化服务；

i) 支持开放接口 API 及 MQTT、CoAP、HTTP 等通用协议，保障与其他平台及设备之间的互通性。

8.2 智慧康养服务云平台

智慧康养服务云平台运用物联网、云计算、大数据、人工智能等现代信息技术和智能设备，通过对涉老数据信息的采集、汇总、分析研判，实现养老服务的信息化、智能化运作和管理，提供实时、快捷、高效的养老服务。智慧康养服务云平台应具备以下功能：

a) 设备管理：支持多类型智能设备接入，实现设备注册、绑定、状态监控及远程控制，具备设备固件升级、故障诊断与报修闭环管理功能；

b) 数据管理：能多维度采集涉老数据，建立标准化数据字典，支持分布式存储与容灾备份，满足海量数据存储需求，具备数据权限分级管理与隐私保护机制；

c) 数据处理：通过清洗、脱敏等技术提升数据质量，剔除异常值与重复数据；运用机器学习算法构建健康风险模型、行为模式画像，挖掘老人活动规律，实现异常数据实时预警，支持多级预警联动；

d) 应用模块：包含人员信息管理、健康管理、照护管理、生活服务、社交文娱、紧急呼救、运营管理等功能模块，可按需扩展适老化增值服务；

e) 应用呈现：采用适老化界面设计，支持多终端适配；提供语音交互、远程协助等辅助功能，操作步骤控制在 3 步以内；数据呈现便于老人及照护者快速理解。

8.3 物业管理服务云平台

物业管理服务云平台是一种基于云计算技术的物业管理服务系统，具备多种功能包括但不限于物业资源管理、设施设备管理、安全管理、环境管理以及客户服务管理等，通过整合资源、优化流程、提高效率等方式为“物业+居家养老”模式提供多种场景的养老服务。物业管理服务云平台应具备以下功能：

a) 设备管理：对社区基础设施进行权限管理、身份认证、参数配置、数据采集、告警及故障管理、升级管理、日志管理、安全审计等功能；

b) 数据管理：对社区相关的权限数据、人口信息、人体生物特征数据、健康数据、车辆信息、地理信息、房屋信息等数据进行统一管理；

c) 数据处理：对社区相关数据进行数据汇聚、数据存储、数据整理、数据建模、数据挖掘、 数据分析和数据可视化处理；

d) 应用模块：实现人员出入管控、车辆出入管控、防攀爬管理、三维巡更管理、电梯应急呼救、电动车进入电梯管理、高空抛物管理、视频监控、消防栓监测、垃圾分

类监测、水电气管理、停车场监测、智慧灯杆管理、环境监测、运营管理等业务部署；

e) 应用呈现：通过一体化大屏应用、电脑端应用和智能终端应用等方式实现业务可视化和人机交互。

8.4 生态互信融通基础设施

生态互信融通基础设施即数据枢纽体系，是实现基于智能家居的“物业+居家养老”模式的新型数字化基础设施，起联通设施设备、对接应用服务的作用，实现多类型数据对接融通，并且在数据融通过程中对双方身份、传输时间、传输内容摘要进行识别、认定和存证，确保传输过程真实可追溯。生态互信融通基础设施应具备以下功能：

a) 部署于家庭、社区和城市，能面向各类主体提供跨层级和区域的去中心化的数据共享交换，尊重数据生态各方业务关系模式，数据传输不经第三方存储再转发；

b) 支持复杂环境下数据对接融通，支持复杂网络架构下的数据安全路由，支持基于用户和服务身份的端到端数据传输，支持多种数据格式和来源；

c) 能提供基于区块链的交换过程可信保障，通过存证实现数据确权，支持数据授权、发送、接收、计量等交换环节的全过程追溯；

d) 采用数字身份、数据加密、隐私计算等技术手段，保障数据在处理和传输过程中的安全；

e) 具备高效的数据处理能力，可调用云计算、边缘计算、分布式计算、大数据处理、AI 分析等技术；

f) 设置有广泛分布于家庭和社区层级的数据枢纽网关用于支持多重耦合度的边缘节点、设备、系统数据打通对接和身份注册认证；

g) 支持动态线上更新的数据融通业务规范，用以支持对家居设备、物业服务、专业服务商、监管部门不同类别应用场景下的规范化对接；

h) 能提供主体和主体关联系统的身份注册与关联，基于安全身份标识以用于数据融通过程的身份认证；

i) 在系统安全、密码安全、资源互联互通等核心领域，关键技术应自主创新并实现国产化。

j) 支持对家庭、服务方和运营主体的身份认证，基于认证身份实施安全加密。

8.5 可信应用服务凭证

可信应用服务凭证可用于证明身份、权属、合约、交易等各类物业与养老业务场景，凭证可在线和离线验证真实性。可信应用服务凭证平台应具备以下能力：

a) 基于国密算法，具备数字签名，凭证接收方可验证凭证的真实性和完整性；

b) 凭证应由合法持有者持有，保护用户隐私不受侵犯；平台提供隐私安全的凭证保全机制，防止用户凭证丢失造成损失；

c) 确保凭证持有者的身份真实可信，通过数字签名、证书和密钥对等技术验证服务请求方的身份，实现严格的访问控制；

d) 凭证应包含足够的元数据信息，说明其所关联的服务、权限范围、有效期限等，便于自动处理和理解；

e) 凭证应包含时间戳信息，证明凭证的生成时间，并设置合理的有效期，以防止过期或重复使用的问题；同时有明确的有效期，过期后应自动失效，减少凭证被盗用的风险；

f) 有完整的凭证使用日志记录，以便于事后审计和监控。通过数字签名等机制，确保凭证的发送方不能否认其发出的请求或操作，增强责任追溯功能；
g) 遵循最小权限原则，仅授予应用服务完成其功能所需的最小权限，以减少潜在的安全风险；
h) 支持强大且灵活的身份验证和授权机制，确保只有合法的应用或服务能使用凭证；
i) 支持跨平台和跨系统的互操作性，以便于在不同的应用服务中使用；
j) 支持凭证状态的动态管理，如根据安全策略或风险情况即时调整权限，必要时能立即撤销凭证有效性。

8.6 数据资产治理平台

数据资产治理平台对服务产生的数据资产进行产权确权，明确数据资产的所有、使用权益关系，形成各主体数据资产权责清单。提供数据资产产权授权交易功能，在确权授权基础上形成数据融通关系，以此支持养老、物业和设备服务间的协同。数据资产治理平台应具备以下功能：

a) 具备数据确权机制，明确数据产权确权流程和规范，具备区块链存证确权功能；
b) 具备授权机制，明确数据授权流程和规范，通过区块链存证确权，明确数据所有者授予特定主体对数据的访问和使用权限；
c) 具备利益分配机制，明确数据资产所有者、授权运营者和数据使用者之间的权益关系；
d) 具备纠纷处置机制，响应处理数据授权和使用过程中可能出现的争议；
e) 对数据资产进行详细登记，包括数据的来源、类型、格式、敏感性等；
f) 明确数据从创建、存储、使用到归档或删除信息，具备数据资产全生命周期管理功能；
g) 具备对数据资产清洗、验证和标准化功能，确保数据资产的准确性和一致性；
h) 根据数据确权过程，建立数据目录，使用户能发现和理解数据资产的属性和可用性；
i) 能提供数据授权、定价和交付，对于授权交付过程应实现可追溯，包括对数据来源、授权记录和使用历史等信息的追溯；
j) 建立数据产品和服务的评估与监管机制，确保数据产品和服务的质量和合规性。
k) 支持家庭级的本地化数据资产认证和权益保障，可关联家庭身份实现数据资产产权认证。
l) 可根据养老服务提供数据授权功能，支持家庭和社区层级的服务必要数据资产授权。

8.7 生态治理平台

生态治理平台面向参与数字化生态治理工作主体，支持开展多方对等协商交流、分析评估生态态势发展态势、订立发布标准规范引导意见等生态层级治理工作。生态治理平台应具备以下功能：

a) 能对物业、智能家居、养老三领域的生态发展进行监测，支持对主体多样性、服务协同性、人才培养情况等态势的感知和分析；
b) 支持对协同合作商议、标准规范更新和大型活动组织等涉及生态发展调控业务的实施；
c) 能组建生态治理主体，为多主体共同组成专职生态治理业务的主体联盟提供协商平台；
d) 能提供跨主体业务协同协商，支持主体间的交流和协议订立；

e） 能提供信息归集和发布，支持对生态发展相关的重要信息汇总梳理、发布告知的功能，为生态发展提供必要信息源；

f） 能协商生态互信融通基础设施建设，明确基础设施的建设范围、建设内容和实施平台。

8.8 隐私安全基础设施

隐私安全基础设施构建可信运行环境，为主体提供获知、控制自身隐私数据的能力，为数据产权权属方维护自身利益提供工具，调和数据安全与数据应用之间的矛盾。隐私安全基础设施应具备以下功能：

a） 具备先进的加密算法和匿名化技术，对敏感数据进行加密处理；

b） 遵循数据最小化原则，仅收集和处理符合合法目的的必要数据，确保数据安全存储和传输，避免数据泄露和滥用；

c） 引入安全计算技术，在不暴露用户敏感数据的情况下进行计算和分析，用户的隐私得到充分保护；

d） 部署有效的防火墙和入侵检测系统，以监控、检测和阻止网络攻击，记录所有网络活动和事件；

e） 实施严格的身份验证和授权机制，限制数据的访问权限，仅经过授权的用户能获取敏感数据；

f） 建立用户的授权和许可机制，包括但不限于访问、更正、删除和投诉的权利，确保用户可有效控制其个人数据的使用和披露；

g） 应具备安全审计功能，记录和分析安全事件，确保对安全问题的追踪和响应；

h） 应建立应急响应机制，一旦发生数据泄露或其他安全事件，能迅速采取措施进行应对；

i） 应具备在发生故障或攻击时能快速恢复数据和服务；

j） 遵循相关法律法规和隐私保护标准，并提供数据审计和合规性检查功能，确保合规性；

k） 实时监控隐私安全基础设施的运行状态和安全性，及时发现潜在威胁和风险。定期进行安全审计和风险评估，识别和解决潜在的安全漏洞和隐患，根据安全需求变更持续评估和改进；

l） 采取有效的数据保护措施，包括但不限于技术、组织和人员方面的措施。定期进行数据隐私保护的自查和评估。

8.9 动态可信设备数字身份平台

动态可信设备数字身份平台为每个设备提供唯一身份的注册和验证功能，为与其关联设备或服务提供存证追溯。动态可信设备数字身份平台应具备以下功能：

a） 能高效进行身份认证与授权，确保身份认证过程的安全性和可靠性，并提供灵活的授权机制，支持在线和离线认证，支持基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC），实现精准授权；

b） 采用隐私计算、数据加密等技术手段，确保基于身份的数据在存储、传输和使用过程中的安全性和隐私性，同时具备数据脱敏和匿名化处理功能，以保障数据隐私的同时实现数据的合规流通；

c） 能动态更新与管理，支持线上实时更新身份数据和认证信息，确保系统的灵活性和适应性，同时支持对接智能家居设备、物业服务、市场服务商、监管部门等多种主体的身份认证需求，提供统一的身份管理规范；

d) 能实现跨平台身份认证与互操作，支持多种操作系统和设备的互操作，确保不同平台和设备间的身份数据互通互认，并提供标准化的接口，支持与第三方应用服务系统的数据对接和身份认证集成，保障系统的开放性和兼容性；

e) 能对身份数据进行追溯与审计，提供详细的身份操作记录和日志，支持审计和追溯查询，保障身份数据使用的透明度和合规性，并支持身份认证和授权过程的监控和记录，提供异常检测和告警功能，确保系统的安全运行。

9 数据要求

9.1 元数据要求

元数据是数据模型的定义，包含数据的类型、关系、字段、约束等。元数据规定了多方业务协同中，对所交换的数据内容的语义和约束性要求。应支持基于元数据的业务标准化，形成行业共识，提高数据融通交换中的互操作性。元数据体系应满足下列条件：

a) 支持标准演进，元数据应当有版本标识，并描述向上兼容和向下兼容的范围；

b) 提供元数据的表决和行业共同治理机制；

c) 支持对业务类型和业务流程中的共性活动环节进行定义；

d) 对共性业务活动进行定义，应规定参与方主体的身份与角色范围；

e) 定义共性业务活动时，应明确必要数据项、建议数据项和可选数据项，应明确数据格式，应明确数据取值范围与约束关系。

9.2 数据交换

数据交换应满足下列条件：

a) 包含业务类型标识，业务线标识、业务活动标识，三者唯一确定一项特定的业务活动；

b) 包含业务活动执行者，信息系统或设备的标识；

c) 包含业务活动时间戳，业务活动操作类型，业务活动状态类型；

d) 包含业务内容，一项业务活动的所有需交换的数字信息；

e) 业务内容格式支持结构化、半结构化和非结构化数据；

f) 支持一个业务活动多方接收；

g) 支持数据一致性检查，包含业务内容摘要、附件摘要；摘要算法应采用国密标准的摘要算法；

h) 具备防抵赖机制，存证交换活动和参与方签名；

i) 支持数据交换记录可追溯、审计和监管；

j) 数据交换核验信息支持区块链存证和查验。

9.3 凭证

凭证可用于证明身份、权属、合约、交易等。凭证应满足下列条件：

a) 含凭证的颁发者、持有者和其他第三方会签者的身份和数字签名；

b) 可验证凭证的出示人和出示用途，确保凭证出示合法；

c) 支持只向接收方提供必要的信息字段，并且接收方可验证所收到的信息的真实性；

d) 根据需要可更新凭证状态，如实现凭证吊销、禁用等功能，并可做状态回溯；

e) 对特定类型的凭证，可规定凭证的有效颁发单位身份列表、必需字段、可选字段等。

9.4 数据资产

数据资产满足下列条件：

a） 具备包含资产权属关系、更新时间、数据类型、关联业务等描述信息；

b） 数据资产信息应根据服务业务频度同步更新，并明确数据资产的更新信息；

c） 数据资产应明确其数据资源持有权、数据加工使用权等权属关系，并形成同主体高度关联的权属关系；

d） 数据资产交易过程中，应明确数据的提供和获取形式、更新频度、应用范围和供需双方身份；

e） 数据资产交易内容和过程应形成双方认可的协议并经客观可信的过程存证，该协议应具备可追溯性；

f） 数据资产应依照其产生、流通和应用场景与相关主体进行资产分类，明确各分类产生环节、流通关系、应用场景和涉及主体；

g） 应根据数据资产分类，明确各分类的资产产权设立、变更、转让和消灭的特性。

10 信息安全要求

10.1 硬件安全

10.1.1 环境安全

环境安全要求如下：

a） 应具备防盗窃、防破坏、防水、防尘、防高温等防护措施；

b） 应保证设备供电稳定可靠，同时提供技术和管理手段监测设备的供电情况，并能在电力不足时及时报警；

c） 应在信号防干扰、防屏蔽、防阻挡等方面满足环境部署的要求。

10.1.2 接口安全

接口安全要求如下：

a） 调试接口应遵循最小化原则，禁用无用的调试接口、去除电路板上调试接口丝印；

b） 若存在调试接口，应支持身份鉴别机制且不存在弱口令；

c） 应禁止外部接口引导系统启动。

10.1.3 身份标识

身份识别要求如下：

a） 应具有明确的身份标识，型号名称应通过设备上的标签或通过物理接口进行清晰识别；

b） 设备身份应支持防篡改的唯一识别码的能力。

10.1.4 芯片安全

设备主要芯片（包括安全芯片、通信模组和主处理器件等）应支持防侧信道攻击的能力。

10.2 固件安全

10.2.1 固件保护

固件保护要求如下：

a） 若存在物理接口，应确保固件不能通过物理接口被提取出来，如串口读取等；

b） 固件应具备自身防护的能力，关键代码及重要数据具有防逆向、防调试和防篡改的功能。

10.2.2 升级安全

升级安全要求如下：

a） 当进行安全升级时，制造商应以明显的方式通知用户（含相关升级风险的信息）；
b） 应具备固件自动或手动升级机制，且升级前应向用户进行确认；
c） 应对固件升级文件的来源进行校验，保证固件的真实性和完整性；
d） 应确保固件下载传输通道可信，防止中间人劫持或者嗅探；
e） 应确保固件升级失败后设备能稳定运行。

10.3 应用安全

10.3.1 身份鉴别

身份鉴别要求如下：

a） 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
b） 用户身份标识应具备不易被冒用的特点，口令做身份鉴别时的密码复杂度要求只适用于使用口令做身份鉴别的场景；
c） 应禁止存在默认口令，若存在默认口令，则需要在第一次使用时强制修改；
d） 不应限制应用用户账号的多重并发会话。

10.3.2 访问控制

访问控制要求如下：

a） 应对用户进行访问控制管理，管理不同用户所能访问的数据、访问权限和访问时效性；
b） 访问控制的粒度应达到主体为用户级，客体为文件级。

10.3.3 应用防护

应用保护要求如下：

a） 应具备自身防护机制，具备防篡改、防攻击、防编译等能力；
b） 在运行过程中出现功能失效等类似现象时，应具备稳定运行及修复能力；
c） 应确保不使用包含 CNVD、CNNVD 已公布 90 天以上的高危等级未处置漏洞（含第三方库和开源组件），并应具备根据新曝光漏洞自动或手动安装升级补丁的功能；
d） 应用服务应遵循最小化原则，仅安装需要的组件。

10.3.4 日志审计

日志审计要求如下：

a） 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c） 应对审计记录进行保护、定期备份，避免受到未预期的删除、修改或覆盖等。

10.4 网络安全

10.4.1 网络接入认证

网络接入认证要求如下：

a) 应在接入网络中具有唯一网络身份标识；
b) 应能向接入网络证明其网络身份，应支持基于密码机制的鉴别；
c) 应支持与接入网络间双向认证的能力；
d) 应保证密钥存储和交换安全。

10.4.2 传输完整性

传输完整性要求如下：

a) 应具备通信完整性校验机制，实现数据传输的完整性保护；
b) 应具有通信延时和中断的处理机制。

10.5 数据安全

10.5.1 通用数据安全要求

基于智能家居的居家社区养老业务应该保证数据生命周期内数据的机密性、完整性，包括采集、传输、存储、处理、交换、销毁等环节。采集应在用户同意的前提下进行，并且数据采集行为的实施与采集的范围应符合隐私协议的描述。

10.5.2 存储安全

对居家养老数据的存储安全要求包括：

a) 存储期限应为实现业务的目的所必需的最短时间；
b) 存储期限应告知用户并征得用户的同意；
c) 超出上述存储期限后，应对其中的个人信息进行删除或匿名化处理；
d) 原则上不应存储原始个人生物识别信息（如样本、图像等）；
e) 存储个人敏感信息时，应采用数据加密、存储在加密数据库或加密存储区等安全措施。

10.5.3 传输安全

对居家养老数据的传输要求包括：

a) 传输居家养老数据时，应采用安全通道；
b) 传输个人敏感信息时，应采用数据加密等安全措施。

10.5.4 个人敏感信息保护

对居家养老数据中个人敏感信息保护应符合GB/T 35273-2020。

10.6 个人信息保护

10.6.1 个人信息保护政策模板

参考GB/T 35273—2020 附录D 个人信息保护政策模板，个人信息保护政策内容应满足个人信息保护政策模板要求。

a) 检查个人信息保护政策披露的个人信息控制者的基本情况，包括主体身份、联系方式，通过工商信息查询、拨打联系电话、向联系邮箱发送邮件等方式验证，上述信息应真实、准确、完整；

b) 检查、测试业务功能及其收集个人信息的行为，验证业务功能以及各业务功能分别收集的个人信息类型，应与个人信息保护政策告知的信息相符；
c) 检查、技术检测个人信息收集方式，验证个人信息收集方式，应与个人信息保护政策披露的个人信息收集方式相符；
d) 检查个人信息保护政策披露的个人信息主体的权利和实现机制，如查询方法、更正方法、删除方法、注销账户的方法、撤回授权同意的方法、获取个人信息副本的方法等，通过操作相应功能、拨打联系电话、向联系邮箱发送邮件等方式验证，上述信息应真实、准确、完整；
e) 查看个人信息保护政策披露的处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式，通过操作相应功能、拨打联系电话、向联系邮箱发送邮件等方式验证，上述信息应真实、准确、完整；
f) 通过人员访谈和服务端核查验证个人信息保护政策对个人信息存储期限的告知，上述信息应真实、准确、完整；
g) 通过人员访谈和服务端核查验证个人信息保护政策对个人信息的共享、转让、公开披露行为的告知，上述信息应真实、准确、完整；
h) 通过人员访谈和服务端核查验证个人信息保护政策对个人信息安全防护措施的告知应真实、准确、完整；
i) 检查个人信息保护政策，应提供简体中文版；字体大小、颜色、排版应易于阅读；个人信息保护政策语言应通顺且易于理解，不存在概念混淆、逻辑混乱、冗长繁琐等；不存在错别字；
j) 检查管理控制应用，首次运行时应通过弹出窗口等明显方式提示用户阅读隐私政策等收集使用规则；
k) 检查管理控制应用注册及登录页面（若有注册、登录功能），应具有个人信息保护政策或个人信息保护政策有效链接；
l) 检查管理控制应用主界面，应通过 4 次及以下点击等操作能访问到个人信息保护政策；
m) 检查管理控制应用，应包含个人信息保护政策；
n) 若在管理控制应用中未找到个人信息保护政策，应存在逐一送达个人信息保护政策时成本过高或有显著困难的情况，例如当应用程序不存在用户交互界面时，此种情况下，应用程序提供者应在其官方网站公开发布个人信息保护政策；
o) 检查个人信息保护政策，应标注更新日期；
p) 检查个人信息保护政策更新行为，存在个人信息保护政策所载事项发生变化时，应及时通知更新个人信息保护政策的情况；
q) 检查个人信息保护政策更新行为，若个人信息保护政策更新过，应向用户明示更新后的个人信息保护政策并告知个人信息保护政策的更新情况；
r) 检查个人信息保护政策更新行为，在个人信息保护政策更新后，应重新告知用户。

10.6.2 征得授权同意的例外

征得授权同意的例外情况如下：
a) 检查个人信息保护政策，应告知“征得授权同意的例外”；
b) 检查“征得授权同意的例外”，不应包含不合理的例外情形。

10.7 系统安全

10.7.1 日志管理

系统宜支持日志记录功能，支持审计日志查阅和访问控制能力，宜具有6个月记录期限。

10.7.2 安全策略

系统应支持以下安全策略要求：

a) 系统应具备身份鉴别和接入认证能力，支持安全协议和传输加密，完整性保护，避免非法设备接入而导致的敏感数据泄露、功能异常或失效；

b) 系统应具备识别应用软件签名能力，在应用软件安装时能识别应用软件的签名状态，并能根据签名状态给用户相应的提示。不得安装国家禁止和国家相关部门明令通报存在窃取用户个人敏感信息行为的应用软件；

c) 系统内置的防火墙功能应该具有抗逃逸能力，能抵抗常见的攻击手段，避免过滤规则被绕过。

10.7.3 风险评估

当系统新引入感知设备、传输设备、平台设备以及第三方组件时，应对其进行信息安全风险评估。

11 运行维护要求

11.1 人员配备

人员配备要求如下。

a) 技术支持人员：物业服务企业或设备供应方应配备专业的技术支持团队或人员，负责智能家居系统的日常维护、故障排除和技术支持。

b) 应急响应人员：确保在老人遇到紧急情况时，能及时响应和处理，包括救援、维修等紧急服务人员。

11.2 运行管理

建立系统运行监控机制，定期对智能家居系统的运行状态进行监测和评估，生成运行报告并分析系统的稳定性和性能。

11.3 设施管理

设施设备管理应符合下列要求：

a) 设备采购与选型：在采购智能家居设备时，应考虑设备的质量、性能、维护便利性等因素，确保选择符合标准要求的产品；

b) 设备维护与保养：确保智能家居和智慧养老设备的正常运行，包括定期检查、维护和保养，保证设备的长期稳定性和可靠性；

c) 设备更新与升级：定期对智能家居和智慧养老设备进行软硬件更新和升级，保持系统功能的先进性和兼容性；

d) 设备退役与替换：制定设备退役和替换计划，根据设备的使用寿命和技术更新，及时替换老化或不再适用的设备。

11.4 优先级

在紧急事件发生时，应支持物业人员拥有首要的响应与处理权限，其优先级高于其他相关方。

附 录 A
（资料性）
基于智能家居的居家社区养老服务模式

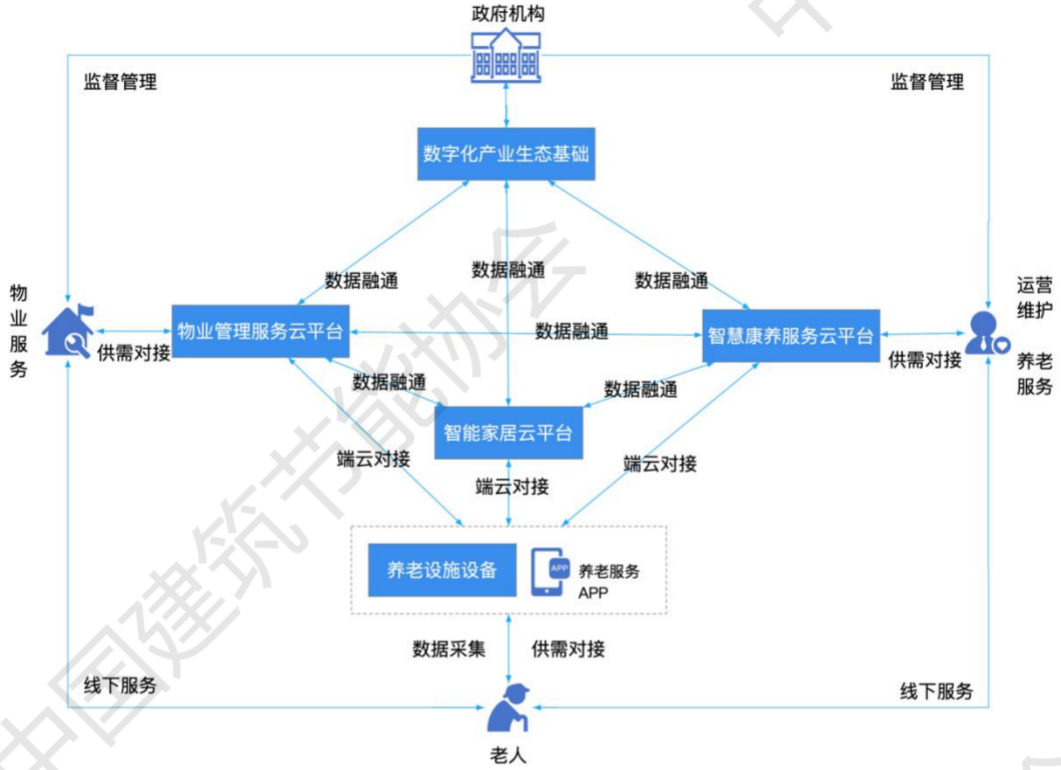

图 A.1 基于智能家居的居家社区养老服务模式

在智能家居背景下的居家社区养老服务模式（见图A.1）中，各个参与方的角色和职责如下：

a) 政府机构：负责监督管理整个数字化养老服务系统，与数字化产业生态基础进行数据融通，以获取必要的信息和数据，进而制定政策和实施监管。

b) 数字化产业生态基础：作为系统的核心，连接各个服务平台，实现数据和服务的联动，为物业管理服务云平台、智能家居云平台和智慧康养服务云平台提供基础服务和数据支持。

c) 物业服务：负责建立客户信任关系、设备安装与维护、最后 100 米的应急响应服务等。通过物业管理服务云平台与数字化产业生态基础进行数据融通和供需对接，提供线下服务，满足老人在居住环境中的需求。

d) 智慧康养服务云平台：负责对涉老数据信息进行采集、汇总、分析研判，实现养老服务的信息化、智能化运作和管理，提供实时、快捷、高效的养老服务。与养老设施设备端云对接、与数字化产业生态基础、物业管理服务云平台和智能家居云平台进行数据融通获取数据。

e) 运营维护与养老服务：负责整个系统的运营和维护工作，确保系统的稳定运行，与数字化产业生态基础进行数据融通，获取必要的信息和数据，进行系统的优化和升级。同时，通过智慧康养服务平台与数字化产业生态基础进行数据融通和供需对接，直接提供为老服务政策指导和社会工作支持，如医疗指导、健康宣教和健康管理服务，专业的居家上门照护和康复服务，以及日常生活服务等。

f） 智能家居云平台：与数字化产业生态基础进行数据融通，实现智能家居设备的远程控制和监控，通过端云对接与养老设施设备相连，收集和分析老人的生活数据。

g） 物业管理服务云平台：作为物业管理服务的数字化接口，与数字化产业生态基础进行数据融通，实现供需对接。通过端云对接与养老设施设备相连，收集和分析老人的生活数据，提供更精准的物业管理服务。

h） 养老设施设备：直接服务于老人，收集老人的生活和健康数据，通过端云对接与智能家居云平台相连，实现数据的上传和设备的远程控制。

i） 老人：作为服务的最终受益者，享受物业管理服务和养老服务提供的线下服务，同时通过养老设施设备，老人的生活和健康数据被收集，以便于提供更个性化的服务。

参 考 文 献

[1] GB/T 39579-2020 公众电信网 智能家居应用技术要求

[2] GB/T 42455.1-2023 智慧城市 建筑及居住区 第1部分：智慧社区信息系统技术要求

[3] YD/T 4657-2024 移动互联网+智能家居系统 跨平台接入认证技术要求

[4] 中华人民共和国无线电管理条例（中华人民共和国国务院、中华人民共和国中央军事委员会令第672号）

[5] 中华人民共和国无线电频率划分规定（工业和信息化部令第62号）

[6] 人脸识别技术应用安全管理办法（国家互联网信息办公室 中华人民共和国公安部令第19号）

[7] 微功率短距离无线电发射设备目录和技术要求（中华人民共和国工业和信息化部公告 2019年第52号）