ICS：35.040

CCS：L80

DBXX

湖　北　省　地　方　标　准

DBXX/T XXXX—XXXX

湖北省养老电子设备数据安全管理规范

Hubei Province Data security management specification for elderly Internet of Things devices

（征求意见稿）

202X-XX-XX 发布　　202X-XX-XX 实施

湖北省市场监督管理局　发 布

目　次

前　言

本标准按照 GB/T　1.1-2020 给出的规则起草。

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这些专利的责任。

本标准由中南财经政法大学国家智能社会治理实验基地（养老）提出。

本标准由湖北省民政服务标准化技术委员会养老服务标准化工作组归口。

本标准主要起草单位：中南财经政法大学、湖北省养老机构协会、武汉光谷信息技术股份有限公司武汉云视科技技术有限公司。

本标准主要起草人：

本标准首次发布。

本文件实施应用中的疑问，可咨询中南财经政法大学国家智能社会治理实验基地（养老），联系电话：13296680625，邮箱：1667014835@qq.com。在执行过程中如有意见和建议请邮寄中南财经政法大学智慧养老研究院。

引　言

近年来，随着我国人口老龄化进程的不断加速，养老服务需求不断增长。为了满足老年人的养老需求，电子设备在养老领域的应用越来越普遍。这些设备包括但不限于计算机、服务器、网络设备、智能硬件、移动设备等，为养老机构的信息化建设提供了便利，也带来了数据安全管理的挑战。

数据安全是信息化建设的核心问题之一，特别是在养老领域，涉及到老年人的个人信息、健康状况等敏感信息，必须保证数据的安全性和保密性。为此，本规范制定了养老电子设备数据安全管理规范，旨在规范养老机构电子设备数据的管理和保护，确保老年人的个人隐私得到充分保障，同时维护养老机构的正常运营和发展。

本规范适用于所有从事养老服务的机构和个人，旨在为其提供一个全面、系统的管理规范，以确保养老机构的数据安全得到充分保障。同时，本规范也为相关监管部门提供了一个参考标准，以促进养老服务行业的规范发展。值得注意的是，该规范主要服务于养老服务的机构和个人以及享受服务的老年人，而养老电子设备的生产厂家并不直接涉及到该规范，只需遵守相关的技术标准和规范，保证其生产的设备符合国家标准并具有一定的安全性能即可。

湖北省养老电子设备数据安全管理规范

1 范围

本文件规定了养老电子设备分类，养老电子设备数据安全的基本要求，养老电子设备数据分类及数据保护措施，养老电子设备数据安全采集、传输、存储、应用技术要求，数据共享和公开的安全要求，养老电子设备数据安全管理的应急预案和人员培训、监督检查和处罚等内容。也为相关的民政、网络安全政府监管部门提供了一个参考标准建议，以便于对养老服务行业的监督和管理。

本文件适用于湖北省内从事养老服务的机构和个人，包括但不限于养老院、社区养老服务中心、家庭养老服务机构等，以及这些机构和个人所使用的所有电子设备和数据，如计算机、服务器、网络设备、智能硬件、移动设备等。旨在规范和保护养老机构电子设备数据安全的管理，确保老年人的个人隐私得到充分保障，同时维护养老机构的正常运营和发展。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 7027-2002 信息分类和编码的基本原则与方法

GB/T 37973-2019 信息安全技术 大数据安全管理指南

GB/T 38624.1-2020 物联网 网关 第1部分：面向感知设备接入的网关技术要求

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 37721-2019 信息技术 大数据分析系统功能要求

GB/T 29765-2021 信息安全技术 数据备份与恢复产品技术要求与测试评价方法

GB/T 36478.4-2019 物联网 信息交换与共享 第四部分：数据接口

GB/T 41479-2022 信息技术安全 网络数据处理安全要求

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

DB3302/T 1126-2021 公共数据管理 数据共享规范

3 术语与定义

下列术语和定义适用于本标准。

3.1

养老物联网 Internet of Things for the elderly

通过信息传感设备，按照约定的协议，把养老行业相关设备与互联网连接起来，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络，实现了老人与设备，老人行为与设备的信息交换和通信。

3.2

脏数据 Dirty Read

指养老电子设备产生的数据不在给定的范围内或对于实际老人服务中毫无意义，或是数据格式非法，以及在相应平台中存在不规范的编码和含糊的业务逻辑。

3.3

养老物联网管理平台 Elderly care IoT management platform

对于智慧养老行业中开发的专门针对接入安全、健康等多种养老电子设备、深度结合老年人服务特点进行场景化设计，满足老年人安全、健康、舒适生活需求的系统。

3.4

养老数据库 Pension database

对智慧养老中养老电子设备数据、养老服务数据、养老系统等数据的集合组织、存储和管理的数据仓库。

3.5

养老智能网关 Smart gateway for the elderly

针对智慧养老行业的特殊性而使用的智能网关，又为网间连接器、协议转换器。

4 缩略语

下列缩略语适用于本文件。

TCP/IP：传输控制协议/网际协议（Transmission Control Protocol/Internet Protocol）

UDP：用户数据报协议（User Datagram Protocol）

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

HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol over Secure Socket Layer）

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

API：应用程序接口（Application Program Interface）

URL：统一资源定位符（Uniform Resource Locator）
SSL：安全套接层协议（Secure Socket Layer）

5 养老电子设备分类

为了规范和保护湖北省养老机构电子设备数据安全的管理，确保老年人的个人隐私得到充分保障，同时维护养老机构的正常运营和发展，按照《信息安全技术个人信息安全规范》（GB/T 35273-2020）和《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）等相关标准制定，将养老电子设备定义为养老机构、社区或居家养老过程中进行识别、采集、监测、控制、交互、反馈等一系列为老人带来便利或信息化建设所需的网络设备，具体分类包含但不限于：

a) 智能硬件养老电子设备为核心数据收集设备，主要分为感知控制设备、健康采集设备、智能交互设备：

——感知控制设备包括但不仅限于：身份感知设备、门磁感知设备、图像感知设备、安全监控设备、控制设备和其他感知设备，主要是通过传感技术以"无感知"的方式进行老人监测和数据收集的；

——健康采集设备包括电子血压计，电子血氧仪，电子血糖仪，体脂秤，多功能随访仪等便携式健康监测设备，主要是通过不同便携式医疗级别器械对于老人的健康状况进行有人工辅助的检测和记录的。

——智能交互设备包括但不限于语音或视频通话设备，可以进行交互反馈的设备。

b) 普通养老电子设备包括但不仅限于辅助行走机器人，电动护理床，健康一体机等，指没有或者不需要接通相应养老物联网管理平台但是仍然可收取老人信息的设备，。

c) 移动养老电子设备包括但不限于智能移动手环，RFID 佩戴标签，移动智能终端等可佩戴老人身体的设备。

d) 网络电子设备包括但不限于计算机，服务器，交换机等网络通讯设备，用于养老机构的养老信息化建设或设备技术方的数据处理。

6 养老电子设备数据安全的基本要求

a) 养老机构应当建立健全数据安全管理制度，明确数据管理职责和权限，制定相应的数据安全管理制度和流程，并将其纳入养老机构的管理体系。

b) 养老机构应当对电子设备进行安全加固，对重要设备和数据进行安全防护，加强对设备和数据的监控和审计，及时发现和处理安全漏洞和事件。

c) 养老机构应当建立安全审计和监测机制，对设备和数据进行定期审计和监测，及时发现和处理安全事件和威胁。

d) 设备安全：养老电子设备必须符合国家相关安全标准和要求，且需要定期维护保养，及时修复漏洞和缺陷，确保设备本身的安全性。

e) 数据采集安全：在数据采集过程中，需要采用合法合规的方式，确保采集到的数据真实、完整、准确，并对敏感数据进行加密保护。

f) 数据传输安全：在数据传输过程中，需要采用安全可靠的传输方式，如加密传输、VPN 等，防止数据被窃取、篡改或泄露。

g) 数据存储安全：对采集到的数据需要进行分类存储和分级保护，建立完整的数据备份和恢复机制，确保数据安全可靠。

h) 数据访问权限控制：对不同角色的用户进行权限控制，确保用户只能访问其需要的数据，防止数据泄露和滥用。

7 养老电子设备数据分类及数据保护措施

养老机构应当根据数据的重要性和敏感程度，将其分为不同的分类，并采取相应的保护措施。养老机构应当明确数据的保密级别，并采取相应的安全措施，对于保密级别高的数据，应当采取更加严格的保护措施，确保其安全可靠。养老机构应当采取多层次的数据保护措施，包括但不限于访问控制、数据加密、数据备份和恢复等，确保数据的机密性、完整性和可用性。

7.1 数据分类标准

a) 根据养老电子设备产生的数据类型和数据的重要性，参照 GB/T 7027-2002 分类方法，可以将数据分为以下几类：个人基本信息：包括老年人的姓名、性别、出生日期、身份证号码等基本信息；

b) 健康信息：包括老年人的健康状况、疾病史、用药情况等健康信息；

c) 行为轨迹信息：包括老年人的生活行为、社交活动、日常习惯等行为轨迹信息；

d) 安全监控信息：包括老年人的家庭安全监控、紧急呼叫、报警等安全信息。

e) 设备信息：从养老应用与管理维度来分析还可分为以下四种：

——状态数据：即为养老电子设备对老人采集的实时动态原始数据。

——可供行为参考数据：有对老人的后续服务有使用计划的数据。

——反馈交互数据：老人与养老电子设备产生的反馈交互数据。

——个性化数据：养老电子设备采集的个性化特殊数据，后续可定位脏数据或者特殊数据。

7.2 数据保护措施

7.2.1 数据使用及保护符合相关法律要求

a) 养老电子设备数据安全的相关使用与保护义务应遵循《中华人民共和国数据安全法》相关条例。

b) 老人用户信息安全管理首先应遵循 GB/T 35273-2020 的要求。然后对于侵犯用户/老人隐私的属于侵权行为，此行为于我国现行法律中《侵权责任法》第二条讲民事权益范围中也包括了隐私权。根据我国现行立法及有关司法解释，隐私利益是受法律明确保护的一项人格利益，因此构成侵害隐私利益的，行为人就应承担侵权民事责任。

7.2.2 为了确保养老电子设备数据的安全性和可靠性，应采取以下数据保护措施：

a) 敏感数据加密保护：对于个人基本信息、健康信息等敏感数据，需要采用加密算法进行保护，确保数据在传输和存储过程中不被窃取、篡改或泄露。

b) 数据访问权限控制：对于不同角色的用户，需要设置不同的访问权限，确保用户只能访问其需要的数据，防止数据泄露和滥用。

c) 数据备份和恢复机制：建立完整的数据备份和恢复机制，定期进行数据备份，并进行演练，确保数据在灾难或数据损坏等情况下能够及时恢复。

d) 数据销毁机制：对于已经不需要保留的数据，需要采用安全可靠的数据销毁方式进行销毁，确保数据不会被恢复和利用。

e) 数据安全审计：对于数据访问和使用情况进行监控和审计，发现问题及时处理，确保数据的安全性和可靠性。

7.2.3 安全评估要求

a) 数据分类评估：需要通过对设备数据处理活动要素进行识别分类，并且评估数据价值；
b) 威胁识别评估：养老电子设备数据在数据处理活动中，可能发生的对保密性、完整性、可用性造成的危害进行识别评估，判断可能发生的安全问题造成的数据安全风险大小；
c) 数据安全评估系统：在对设备数据的传输、存储、处理、使用等过程中的脆弱性问题及威胁，需要有提前的安全措施，有相对于的安全风险评估体系或系统。

7.3 数据安全保护基本原则

7.3.1 保密性

养老电子设备数据环境下的保密性至少需考虑以下方面：

a) 数据采集与传输的保密性：对于目前不同传输协议类型如 TCP/IP、UDP、HTTP、MQTT 等多种主流协议与连接方式传输的养老电子设备，应当采用相应的安全协议保障数据的采集与分发等操作的传输保密要求，如数据摘要、签名、鉴别等密码算法应采用国家规定或国家强制标准要求的摘要、签名、鉴别等密码算法及其组合[1]。
b) 数据存储的保密性：将多种类型的养老电子设备数据收集，应当设置访问控制与加密机制等；应支持存储分级策略，尤其是支持单机级、跨平台级等级分类的划分；支持数据隔离机制存储与备份，使不同数据使用方的数据相互独立不可见。
c) 敏感信息的加密保护：对于养老物联网采集到的老人隐私数据及个人数据采取加密算法或通过数据隔离机制确保数据不暴露老人敏感数据，或通过数据匿名化使得老人的个人信息主体无法被识别。

7.3.2 完整性

养老电子设备数据环境下的完整性至少需考虑以下方面：

a) 数据来源验证：应确保数据来自己方对接与认证在相应养老物联网管理平台的数据源。
b) 数据传输完整性：传输时支持信息完整性校验机制，实现管理数据、鉴别信息、敏感信息、重要养老数据等数据的传输完整性保护，如：校验码、消息摘要、数字签名等；具有通信延时和中断处理功能，配合终端进行完整性保证。
c) 数据存储完整性：应确保分布式存储设备数据，支持对关键数据如可供行为参考数据及有价值的反馈交互数据存储备份，保障其备份数据可靠性。

7.3.3 可用性

养老电子设备数据环境下的可用性至少需考虑以下方面：

a) 养老物联网管理平台的安全可靠：具备一定的容灾能力。
b) 养老数据库具备安全分析能力：当养老电子设备数据存在可接受的误差时，有自我分析容错机制保障系统正常运行及数据正确使用。
c) 设备数据具备时效可用：都应根据对于不同老人的不同情况，保持与时俱进，确保数据的使用先进性。

7.3.4 其他需求

其他相关安全需求应遵循 GB/T 37973-2019 中第六章要求。

8 养老电子设备数据安全采集、传输、存储、应用技术要求

8.1 数据安全采集、传输技术要求

8.1.1 数据源选择：

a) 根据需要采集的养老电子设备数据的数据源类型（如：文件、数据库、传感器等），确定数据源连接通讯的方式，明确采集标准范围及属性；
b) 可支持结构化数据和非结构化数据类型；
c) 可支持 MQTT、蓝牙等多种连接方式；
d) 可支持 TCP、UDP、FTP、HTTP 等通讯协议。

8.1.2 数据汇聚采集：

a) 设备数据的收集应满足数据收集相关的合法性要求，满足数据收集的必要性原则和最小化原则，对于恶意采集养老过程中不相关数据的电子设备应当禁止使用；
b) 对于养老中 4G/5G 通讯方式的设备，确保对采集的原始数据进行清洗、转换、分析等处理，确保数据的完整性、准确性和时效性；
c) 对于其他需要养老智能网关收取汇聚数据的养老电子设备，使用的养老智能网关需遵循 GB/T 38624.1-2020 中 5.7 相关要求的同时，也要确保对应网关功能符合养老实际应用，尽量避免功能带来的冗余性，并对网关要做出相关用户鉴别、加密传输机制、攻击保护等安全策略，避免数据泄露与丢失。

8.1.3 数据传输：

a) 不同类型的养老设备的数据在传输养老数据库过程中，需要对数据尤其是敏感数据（老人活动隐私数据、个人信息等）进行加密，对认证和票据相关设备数据使用数字签名等操作。
b) 若对多种类型的养老电子设备数据收集，应支持时序型数据库存储实时性数据，可用于监测、检查设备所采集的状态数据等；支持关系型数据库存储可供行为参考数据，可用于分析及优化后续养老服务。

8.2 数据安全存储技术要求

8.2.1 数据库加密：

养老物联网的数据在保证准确性的同时必须保证其数据的安全性，除了设备数据需经过加密密钥或加密函数转换外，系统服务器必须配备防火墙、入侵检测等安全设备，对数据库访问用户按不同权限访问数据库，全方面防止外部入侵，保证信息平台和数据安全。

8.2.2 **数据库存储策略：**

应建立数据存储、传输、交互的安全策略，保障数据可稳定存储和传输。养老物联网系统计算基础设施相关服务器、网络和安全存储设备的安全，应遵循 GB/T 20271-2006 中第 4 章的要求。

8.2.3 **备份保护：**

对于涉及国家安全、社会公共秩序、公民个人隐私的重要数据进行异地备份，以确保其安全。

8.3 数据安全加工测试与使用技术要求

8.3.1 **数据脱敏：**

根据公共数据相关法律法规、标准的要求以及养老业务需求，对养老电子设备数据进行脱敏处理，保证数据的可用性与安全性的平衡，确保对数据脱敏处理过程后保留状态数据格式和特定属性，满足后续养老服务需求，确保负责该项工作人员具备对数据脱敏的技术方案定制化能力，并能分析脱敏过程中的安全风险，具备处理安全风险能力。

8.3.2 **数据分析安全：**

通过对养老电子设备状态数据的收集，整合分析利用过程中采取适当措施，防止可供行为参考数据中的有价值信息和个人隐私泄露的安全风险，相关技术人员在对其分析过程的统计分析与分析模型要求遵循 GB/T 37721-2019 中第七章与第八章相关要求，并且对数据安全分析中所可能引发的数据聚合的安全风险进行有效评估，并针对分析该养老场景的特殊性具备提出有效的解决方案能力。

8.3.3 **数据备份与恢复安全：**

针对养老行业的特殊性，对养老服务过程中可供行为参考数据的设备分析预警数据采取实时备份和恢复；对其他状态数据采取定期压缩备份与恢复，实现对存储数据的冗余管理，保护数据的可用性；支持镜像备份、冗余备份等方式提高数据存储的可靠性。

在数据备份过程中相关养老机构组织及技术人员需明确定义数据备份和恢复范围、频率、日志记录、数据保存时长等，明确对数据的压缩和加密要求；应支持备份进程并行的容错机制。其他相关备份技术要求应遵循 GB/T 29765-2021 第六章相关要求。

8.3.4 **数据库安全运维：**

养老电子设备的数据如果是通过相应养老物联网管理平台进行访问数据与管理运维：

a) 相应养老物联网管理平台的安全等级保护要求应遵循 GB/T 22239-2019 的安全等级保护基本要求符合等级保护第二级的防护要求，并通过相应测评给出评测证书。
b) 对运维用户的身份、权限和访问控制策略具备配置管理功能；

养老电子设备的数据如果是通过运维客户端访问数据存储系统：

a) 对非法访问请求可以进行拦截和解析，可认证发起请求的用户身份；
b) 可以按照访问控制策略进行非法阻断和告警。

9 养老电子设备数据共享[2]和公开的安全要求

为保障老年人的合法权益，规范养老电子设备数据的共享和公开行为，养老服务机构、设备生产商、设备运维商、系统开发商、系统运营商、老年人、老年人家属、政府管理部门等各方应当遵守以下要求：

9.1 数据共享的基本要求

a) 数据共享应当遵循合法、正当、必要、充分、明确的原则，以保护老年人的个人信息和隐私为前提。

b) 数据共享应当符合法律、法规、行业标准等相关规定，不得违反国家法律法规和养老服务机构的内部规定。

c) 养老服务机构应当在取得老年人同意的情况下，向设备生产商、设备运维商、系统开发商、系统运营商等提供符合安全要求的数据。

d) 设备生产商、设备运维商、系统开发商、系统运营商等应当对接收到的数据进行认真审查，确保数据的安全性和保密性。

e) 在数据共享过程中，各方应当确保数据的真实性和完整性，防止数据被篡改和泄露。

9.2 数据公开[3]的基本要求

a) 数据公开应当遵循合法、正当、必要、充分、明确的原则，以促进养老服务的公开透明为目标。

b) 数据公开应当符合法律、法规、行业标准等相关规定，不得违反国家法律法规和养老服务机构的内部规定。

c) 养老服务机构应当对公开的数据进行审查，确保数据的安全性和保密性，并避免对老年人个人信息和隐私的泄露。

d) 设备生产商、设备运维商、系统开发商、系统运营商等应当根据养老服务机构的要求，对公开的数据进行审查和过滤。

e) 公开的数据应当进行分类，对不同的数据进行不同的保护措施，确保数据的安全性和合理性。

f) 公开的数据应当在充分保护老年人个人信息和隐私的前提下，尽可能满足老年人、老年人家属和社会公众的需求。

9.3 数据共享和公开的技术要求

在养老电子设备数据共享和公开方面，需要考虑以下技术要求：

（1） 数据传输安全：对于数据共享和公开涉及的数据传输，需要采用加密协议和安全通信管道等技术手段，确保数据传输的安全性。

（2） 数据存储安全：对于数据共享和公开涉及的数据存储，需要采用数据分类和分级存储、备份和恢复等技术手段，保证数据的完整性、可靠性和安全性。

（3） 访问控制：对于共享和公开的数据，需要采用合理的权限控制措施，确保只有合法的用户才能访问和使用数据。

（4） 数据匿名化：对于共享和公开的数据，需要采用数据匿名化等技术手段，保护个人隐私和敏感信息的安全。

（5） 安全审计[4]：对于共享和公开的数据，需要采用安全审计技术手段，记录数据的访问和使用情况，以便及时发现和解决安全问题。

（6） 法律合规性：对于共享和公开的数据，需要遵守相关法律法规和政策规定，保证数据使用的合法性和合规性。

10 养老电子设备数据安全管理的应急预案和人员培训

10.1应急预案编制

（1）养老服务机构应根据实际情况制定相应的数据安全应急预案，明确各级应急响应的程序和职责，规定紧急事件的通报、处理、跟踪、评估、反馈等流程。

（2）应急预案应当包括以下内容：应急响应组织机构及其职责、信息通报渠道和流程、应急响应程序、应急响应流程图、应急保障措施、应急处理措施、事故调查及处理、应急演练等。

（3）应急预案应根据实际情况定期演练，演练次数不少于一次/年。演练内容应充分考虑各种紧急情况的可能性和影响，演练结果应记录并及时反馈。

10.2应急演练

（1）应急演练是应急预案的检验和验证，养老服务机构应当按照应急预案的内容进行应急演练。

（2）应急演练应当定期组织，演练周期应根据机构规模、设备数量、数据敏感程度等因素确定。应急演练应当与实际情况相符，应当考虑各种应急情况的可能性和影响，对演练结果进行评估和总结。

（3）应急演练的内容应当包括应急响应、应急保障、应急处理和应急恢复等方面的演练。

10.3人员培训

（1）养老服务机构应当定期对从业人员进行数据安全管理培训，提高其对数据安全的认识和技能水平，增强其数据安全意识和保密意识。

（2）培训内容应当包括但不限于：数据安全意识、数据分类、数据保密级别、数据访问控制、数据备份和恢复、网络安全管理的数据传输部分等方面的知识和技能。

（3）培训方式应当灵活多样，可以采用面对面教学、网络教育等方式进行。养老服务机构应当对从业人员的培训情况进行记录，并对培训效果进行评估。

11 养老电子设备数据安全管理规范的监督检查和处罚

为了确保养老电子设备数据安全管理[5]规范的有效实施，需要建立相应的监督检查和处罚机制。具体措施如下：

a) 监督检查机制：设立专门的监督检查机构，负责定期对养老电子设备数据安全管理情况进行检查，发现问题及时通报，并要求相关单位进行整改[5]。

b) 处罚制度：对于违反养老电子设备数据安全管理规范的单位和个人，将依据有关法律法规和政策规定，给予相应的行政处罚或者其他法律制裁。

c) 奖惩机制：对于积极推进养老电子设备数据安全管理工作，取得显著成效的单位和个人，将给予相应的表彰和奖励，鼓励各方共同参与数据安全管理工作。

d) 网络安全等级保护制度：对于养老电子设备数据安全的网络安全等级保护，应该遵守《中华人民共和国网络安全法》等相关法律法规，按照网络安全等级保护制度的要求，建立相应的安全等级保护体系，实现养老电子设备数据的有效保护。

以上措施可以有效地提高养老电子设备数据安全管理的水平，保护老年人的个人隐私和敏感信息，维护社会安全稳定。

参考文献

[1] GB/T37025—2018，信息安全技术 物联网数据传输安全技术要求[S].
[2] GB/T 24888-2010，地震现场应急指挥数据共享技术要求[S].
[3] DB15/T 1874-2020，公共大数据安全管理指南[S].
[4] DB3311/T 128—2020，智慧养老服务平台建设总体要求[S].
[5] DB15/T 2197—2021，大数据应用 数据安全管理责任指南[S].

中南财经政法大学国家智能社会治理实验基地（养老）