ICS 35.080

CCS L77

DB3411

滁 州 市 地 方 标 准

DB3411/T 0038—2024

智慧养老服务区块链隐私保护规范

Privacy protection specification for smart elderly care service blockchain

2024－03－15 发布　　2024－03－15 实施

滁州市市场监督管理局　　发 布

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。

本文件由滁州市民政局提出并归口。

本文件起草单位：滁州学院、滁州市民政局、滁州市数据资源管理局。

本文件主要起草人：赵生慧、陈桂林、蔡婷婷、王汇彬、刘进军、柏春艳、高结、訾雪梅、钱尼兵、赵玉艳、杨辉。

智慧养老服务区块链隐私保护规范

1 范围

本文件规定了智慧养老服务区块链的隐私保护原则、隐私保护范围、隐私保护方法、及隐私保护监管要求。

本文件适用于智慧养老服务区块链平台建设。

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 35273—2020 信息安全技术 个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

智慧养老服务 smart elderly care services

利用物联网、云计算、大数据和人工智能技术，通过智能产品和信息平台整合居家、社区和机构养老资源，为老年人提供智能化、个性化的养老服务。

3.2

区块链 blockchain

使用密码技术链接将共识确认过的区块按顺序追加形成的分布式账本。

[来源：GB/T 42752-2023，3.12]

3.3

隐私数据 privacy data

特定自然人的身份、健康状况、活动情况等信息，以及养老服务机构等组织实体的财务、视频监控等信息。

3.4

隐私主体 privacy subject

老年人、老年人监护人、养老服务机构等自然人或组织实体。

3.5

隐私控制者 privacy controller

有能力决定养老服务隐私数据处理目的、方式等的组织或个人。

4 隐私保护原则

隐私控制者开展隐私数据处理活动时应遵循合法、正当、必要的原则，具体包括：

a) 权责一致：采取技术和其他必要的措施保障个人信息的安全，对其个人信息处理活动对隐私主体合法权益造成的损害承担责任。
b) 目的明确：收集和处理个人及组织实体的隐私数据时，明确指定数据的收集和处理目的。
c) 明示同意：向隐私主体明示隐私数据处理目的、方式、范围等规则，征求其授权同意。
d) 最小授权：仅在必要时收集和使用隐私主体的隐私数据，并限制其用途。
e) 公开透明：向隐私主体提供清晰明了的隐私通知，解释数据的收集、处理、存储和共享方式，以及隐私主体的权利。
f) 合法公正：按照法律法规处理隐私数据，不进行欺骗性的数据处理行为。
g) 确保安全：保护隐私数据的保密性、完整性、可用性，防止未经授权的访问、泄露或滥用。
h) 主体参与：隐私主体有权访问自己的隐私数据、请求更正错误的数据、删除不再必要的数据、撤回授权同意，以及行使其他适用的隐私主体权利。

5 隐私保护范围

5.1 数据收集

隐私控制者应在遵循隐私保护原则的前提下，采集真实、准确的隐私主体信息，并保证信息采集过程的安全性。

5.2 数据存储

数据存储应符合GB/T 35273－2020中第6.3条要求。隐私控制者应采取技术措施保障隐私数据的安全，包括身份认证、访问控制、数据加密等措施，同时设置数据访问日志等功能进行监测。

5.3 数据应用

数据存储应符合GB/T 35273－2020中第7章要求。隐私控制者应确保隐私数据的应用合理、必要，不得违反法律法规和行业规范，并对数据应用行为进行相应控制和监测。

5.4 数据披露

数据披露应符合GB/T 35273－2020中第9.4条要求。隐私控制者应在经过隐私主体同意或法律法规允许的前提下，仅在必要的范围内以密文形式披露经过脱敏的隐私数据。

5.5 数据删除

对于链上数据，可通过在新的区块中添加数据删除标记、删除密钥等技术手段确保隐私数据不可用。

6 隐私保护方法

6.1 权限控制

实施严格的权限控制，确保只有经过授权的用户才能访问特定的数据和功能。区块链智能合约可以用于自动执行访问控制策略。可采用基于属性基加密的权限控制方法。

6.2 去标识化

隐私主体在区块链上的交易和数据记录应匿名，不直接与他们的身份相关联。

6.3 加密保护

根据隐私数据的需求设计加密保护方案，确保隐私数据在存储和传输过程中，不被未授权用户获取明文信息，宜使用国密算法对隐私数据进行加密。

6.4 物理分割

可将隐私数据碎片化，并存储在不同的物理存储上。

6.5 链外存储

音视频等类型隐私数据上链时，宜通过安全技术手段将原数据存储于链外系统，只在链上存储数据对应的摘要信息。链外系统宜使用IPFS存储原数据。

7 隐私保护监管要求

7.1 日常管理要求

7.1.1 隐私数据全周期监管

隐私控制者应制定相应的隐私保护管理制度和流程，建立完善的信息安全管理体系和风险评估机制，对隐私数据收集、存储、应用、披露、删除等环节加以控制和监督。

7.1.2 隐私保护检查和审计

隐私控制者应配合监管机构进行隐私保护检查和审计。

7.2 应急管理要求

隐私控制者应建立并实施应急预案，必要时开展应急演练。