ICS 35.240.80
CCS L 79

团　　体　　标　　准

T/CI 857—2024

医疗保障数据安全可信流通技术要求

Technical requirements for secure and trustworthy flow of healthcare security data

2024-12-30 发布　　2024-12-30 实施

中国国际科技促进会　发　布
中国标准出版社　出　版

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。

本文件由重庆电子科技职业大学提出。

本文件由中国国际科技促进会归口。

本文件起草单位：重庆电子科技职业大学、重庆国家应用数学中心大数据与最优化研究所、智慧医保实验室、电子科技大学、贵州大学、杭州锘崴信息科技有限公司、重庆药品交易所股份有限公司、重庆瑞研信息科技有限公司、中国电信股份有限公司数据要素技术创新(海南)中心、广州广电运通信息科技有限公司。

本文件主要起草人：许磊、肖山、董昊、肖蒲、张莉、李帜、陈甫、李艳、朱刚令、高超、汪文勇、张方红、李林、李法平、陈明、樊小平、黄健强、周政成、黄程杰、胡红雨、张海宁、张承业、林誉、吴卫增。

引　言

《“健康中国 2030”规划纲要》《“十四五”国民健康规划》《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》《中共中央、国务院关于构建数据基础制度更好发挥数据要素作用的意见》《“十四五”全民医疗保障规划》《关于印发“十四五”全民健康信息化规划的通知》《可信数据空间发展行动计划(2024—2028 年)》等国家一系列重要战略规划与政策文件强调了数据这一新型生产要素的重要地位。医疗保障数据的量大、覆盖面广、更新频率高且潜在价值巨大,对公共医疗卫生服务和智慧医疗的发展具有重要作用,但其包含个人数据和企业数据,涉及隐私,对其明确安全可信流通技术要求,可促进医疗保障数据价值的激活和释放。

医疗保障数据安全可信流通技术要求

1 范围

本文件规定了医疗保障数据流通过程中，确保数据安全、合规和可信性的技术要求。

本文件适用于医疗保障数据合法有序流动的场景。

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 7408 数据元和交换格式 信息交换 日期和时间表示法

GB 11643 公民身份号码

GB/T 39786 信息安全技术 信息系统密码应用基本要求

医疗服务项目分类与代码（国家医疗保障局）

定点医疗机构代码（国家医疗保障局）

定点零售药店代码（国家医疗保障局）

医疗服务项目分类与代码（国家医疗保障局）

医保系统单位分类与代码（国家医疗保障局）

医保药品分类与代码（国家医疗保障局）

医保医用耗材分类与代码（国家医疗保障局）

3 术语和定义

下列术语和定义适用于本文件。

3.1

医疗保障数据 healthcare security data

与医疗保障制度运行相关的各种数据。

3.2

数据流通 data flow

通过开放、共享和交易等方式，实现数据在不同主体间流动的过程。

3.3

数据安全可信流通 data secure and trustworthy flow

在确保数据安全的基础上，确保数据可信度的数据流通。

4 缩略语

下列缩略语适用于本文件。

HIS：医院信息系统（Hospital Information System）

TEE:可信执行环境(Trusted Execution Environment)

5 流通总体要求

5.1 医疗保障数据流通总体要求如图1所示。

5.2 医疗保障数据的流通应遵循“原始数据不出域,数据可用不可见”原则。数据流通可借助平台完成。平台企业应为中华人民共和国境内合法注册的企业,具有企业统一社会信用代码。

5.3 医疗保障数据的流通类型主要包括数据开放、数据共享和数据交易。

5.4 医疗保障数据的流通宜以数据应用服务、数据终端、数据接口服务形式展开。

5.5 医疗保障数据流通的主要参与体包括各级医疗保障机构、数据使用方、数据监管方、数据经纪人和生态服务方。

5.6 医疗保障数据的采集和传输通过专网进行,TEE下应保证通信信道安全。

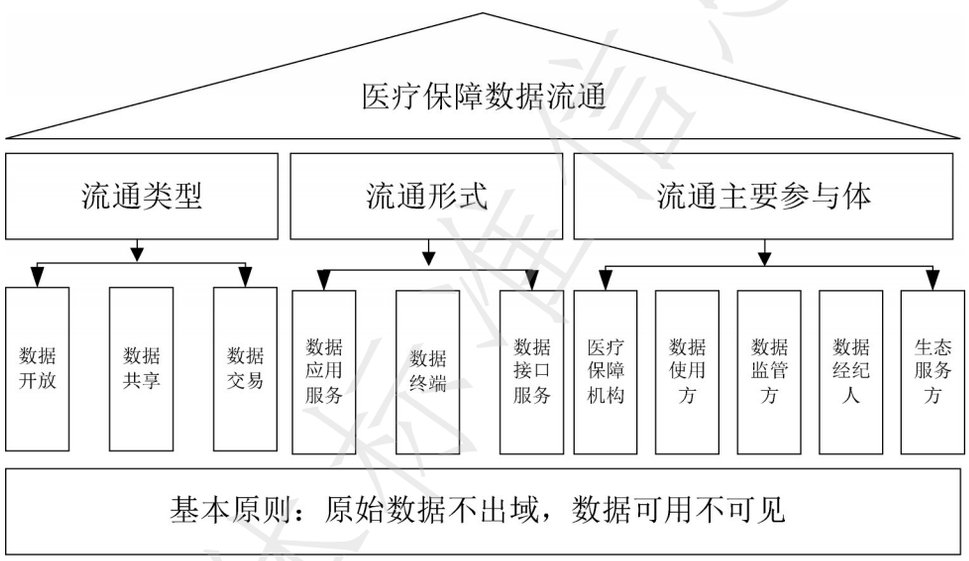

图1 医疗保障数据流通总体要求

6 流通前的安全可信技术要求

6.1 数据采集

6.1.1 医疗保障信息系统通过规范的程序和技术手段,按照既定的格式从HIS系统和定点医药机构等信息系统采集数据,应遵循合法、正当、必要的原则。

6.1.2 HIS系统和定点医药机构信息系统对数据的真实性和完整性进行管理。

6.2 数据分类分级

6.2.1 医疗保障数据的分类分级宜符合GB/T 43697、GB/T 39725和国家医疗保障局发布的《医疗保障数据分类分级管理规范》的规定,为其数据流通提供基本遵循。

6.2.2 医疗保障机构宜编制数据资源目录,包括数据名称、数据类型、数据格式、数据所有者、数据更新频率等基本信息。

6.2.3 医疗保障机构宜建立分类分级保护措施。

6.2.4 医疗保障数据的安全可信流通应参考数据分类分级结果、区分流通主体及应用目标,区别实现数据的开放、交易和共享。

6.3 数据存储

6.3.1 医疗保障信息系统应采用安全可靠的数据存储设备进行数据的分类存储，合理规划存储空间和存储设备，定期备份、更新、盘点数据，确保数据存储的安全性，防止数据损坏、丢失、泄露和篡改。

6.3.2 医疗保障信息系统宜采用加密技术对数据进行保护，数据加密技术应符合 GB/T 39786 的规定。

6.3.3 医疗保障机构宜建立合理的密码使用和密钥管理技术规范和制度。

6.4 数据访问控制

6.4.1 医疗保障数据中的个人数据和企业数据应设置访问控制规则。

6.4.2 对于被授权访问个人信息的人员，应建立最小授权的访问控制策略，确保其只能访问职责所需的最小必要个人信息，且仅具备完成职责所需的最少数据操作权限。若出现超权限处理授权信息，应经个人信息保护责任人或个人信息保护工作机构进行审批，并记录留档。

6.4.3 医疗保障数据中的个人数据和企业数据操作应设置内部审批流程，尤其是进行批量修改、拷贝和下载等重要操作。

6.5 数据脱敏

6.5.1 医疗保障数据中涉及大量个人数据和企业数据，应加强数据脱敏技术要求。

6.5.2 医疗保障机构宜建立数据脱敏技术规范和制度，明确不同安全级别数据脱敏规则、脱敏方法和脱敏数据的使用限制。

6.5.3 医疗保障信息系统对数据的脱敏过程宜留存日志记录，用于审核违规使用和脱敏的完整性。

6.5.4 医疗保障数据的处理符合以下规定：

a） 日期和时间应符合GB/T 7408的规定；

b） 公民身份证号码应符合GB 11643的规定；

c） 医疗目录编码应符合国家医疗保障局发布的《医疗服务项目分类与代码》规定；

d） 机构编码应符合国家医疗保障局发布的《定点医疗机构代码》《定点零售药店代码》《医保系统单位分类与代码》规定；

e） 医保药品及医用耗材编码和分类应符合国家医疗保障局发布的《医保药品分类与代码》《医保医用耗材分类与代码》规定。

6.6 数据产品登记

6.6.1 医疗保障机构应审核流通数据产品的使用范围、交易方式和使用权限。

6.6.2 医疗保障数据产品的登记宜经医疗保障机构审核后，根据数据流通平台的要求开展。

6.6.3 医疗保障数据产品的登记信息宜包含产品适用范围。产品适用范围的登记信息可分为通用信息和个性信息。通用信息包括但不限于登记编号、数据产品名称、描述关键词、产品简介、适用场景、禁用场景、授权情况、时间跨度、数据规模等；个性信息包括但不限于数据应用、数据接口、相关数据产品等。

6.7 数据监管

数据监管方应对数据分类、访问技术和合规管理实施监管。

7 流通中的安全可信技术要求

7.1 流通管理要求

7.1.1 医疗保障数据的流通应采用加密、访问控制、数据权限控制、个人数据去标识化等技术手段，确保数据流通过程中的安全。

7.1.2 医疗保障数据流通应遵循最小化原则，不应超范围、超用途传输医疗保障数据。

7.1.3 数据流通平台应对流通数据产品的描述和样本的准确性、真实性进行审核，对数据分类分级结果进行审核，对数据的安全风险进行评估。

7.1.4 医疗保障数据的流通管理应结合数据管理方式进行合理规划设计。

7.2 可信数据空间

7.2.1 可信数据空间应包括数据空间安全边界和数据空间身份认证和授权两部分内容，具体规定如下：

a) 数据空间安全边界：应明确定义和划分数据空间的逻辑边界并在数据空间边界设置访问控制机制；宜支持多方安全计算协议在信任域内的实施；支持基于区块链的去中心化信任机制；

b) 数据空间身份认证和授权：应支持服务器硬件的部署预认证，保证硬件设备的可信性；应支持通过TEE获取硬件码和操作系统的度量值；应支持算法在监管平台上的注册和认证；宜支持计算任务的动态证书机制，任务完成后即时受理证书；宜支持全方位的计算要素（硬件、软件、算法、数据）统一认证流程；宜支持认证过程的实时监控和异常检测；可支持基于区块链的全局认证机制，提高认证过程的透明度和不可篡改；可支持认证结果的跨空间互认和共享。

7.2.2 数据空间理念下，数据流通管理分为数据空间内部流通管理和跨数据空间的流通管理，具体规定如图2所示，其内容包括：

a) 数据空间内部流通管理：包括但不限于内部数据目录管理、权限控制管理、内部流通机制管理、内部审计与监管等；

b) 跨数据空间流通管理：包括但不限于不同数据空间之间的目录对接、身份认证与授权、数据审计等。

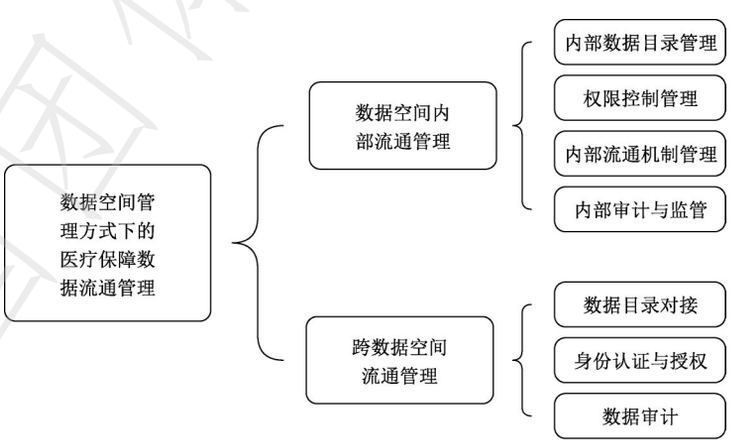

图2 数据空间管理方式下的医疗保障数据流通管理

7.2.3 内部数据目录管理主要包括：

a) 应支持建立统一的数据资产目录，包括数据名称、数据类型、数据格式、数据所有者、数据更新频率等基本信息；

b) 宜支持数据使用情况的统计和分析功能，包括访问频率、使用用途等信息；

c） 可支持数据目录的版本管理，记录数据结构和属性的变更历史；

d） 可支持与外部数据目录系统的对接和数据交换能力，促进跨空间的数据流通。

7.2.4 权限控制管理主要包括：

a） 应支持基于角色的访问控制，根据用户的角色分配相应的数据访问权限；

b） 应支持权限的动态调整机制，能够根据需求快速调整用户或角色的权限；

c） 可支持权限审计日志，记录所有的权限变更操作，便于追溯和审计。

7.2.5 内部流通机制管理主要包括：

a） 应支持数据流通申请与审批流程，规范数据流通的操作过程；

b） 应支持数据流通全过程的追踪，记录数据的流转路径和使用情况；

c） 宜支持数据加密传输机制，保障数据在传输过程中的安全性；

d） 可支持数据流通异常自动报警机制，及时发现并处理流通过程中的问题。

7.2.6 内部审计与监管主要包括：

a） 应支持全面的数据操作日志记录，包括数据访问、修改、删除等操作；

b） 应支持定期的合规性审计，确保数据使用符合相关法律法规和内部政策；

c） 可支持与外部监管系统的对接，便于满足外部监管要求。

7.2.7 跨空间数据目录对接主要包括：

a） 应支持跨空间数据目录的定期同步机制，保证各数据空间能及时获取其他空间的最新数据目录信息；

b） 应支持对跨空间共享的数据资源进行统一编目和分类，便于跨空间数据的检索和使用；

c） 宜支持跨空间数据目录的版本管理，记录数据结构和属性的变更历史；

d） 宜支持跨空间数据目录的访问控制机制，根据不同数据空间的权限设置限制数据目录的可见范围；

e） 宜支持跨空间数据目录的质量评估指标，帮助使用者了解其他空间数据的质量状况；

f） 可支持跨空间数据目录的语义映射，解决不同数据空间在数据描述上的语义差异。

7.2.8 跨空间身份认证与授权主要包括：

a） 应支持统一的身份认证标准，确保不同数据空间之间可以互相认可用户身份；

b） 应支持细粒度的跨空间授权管理，可以精确控制用户对不同数据空间资源的访问权限；

c） 宜支持多因素认证，提高跨空间访问的安全性，特别是对于敏感数据的访问；

d） 可支持基于区块链的去中心化身份认证，增强跨空间身份认证的可信度和安全性；

e） 可支持跨空间的角色映射机制，实现不同数据空间之间角色的对应和转换。

7.2.9 跨空间数据审计主要包括：

a） 应支持全面的跨空间数据操作日志记录，包括数据访问、传输、使用等各个环节；

b） 应支持跨空间数据流通的合规性审计，确保数据流通符合相关法律法规和行业标准；

c） 宜支持实时的跨空间数据流通行为分析，及时发现潜在的安全风险和违规操作；

d） 可支持跨空间审计的协同机制，允许不同数据空间的审计人员进行协作审计；

e） 可支持基于区块链的跨空间审计日志存储，确保审计记录的不可篡改性和可追溯性。

7.3 安全监管

7.3.1 医疗保障数据流通过程中应加强数据监控安全事件管理。

7.3.2 医疗保障数据流通过程应设计一套完善的安全事件处理流程，包括但不限于事件上报、事件评估、事件隔离和恢复、事件溯源和分析、事件处置和防范、事件总结和报告。

7.3.3 医疗保障数据流通过程应设计应急安全事件处理流程，并给予安全管理员应急处理权限。

8 流通后的运维要求

8.1 变更管理

8.1.1 医疗保障数据安全可信流通相关环节的规范应结合技术进步和法律法规的更新进行变更。

8.1.2 医疗保障数据安全可信流通环节的变更应符合变更流程，提出变更提案，由专家进行变更评估和评审，在接到变更评审结果反馈后展开实施。

8.1.3 医疗保障机构应建立变更监督机制，定期审查变更管理流程。

8.2 技术更新与维护

8.2.1 医疗保障数据流通平台及基础设施开发企业应响应技术进步和行业变化，在确保医疗保障数据安全前提下开展相应的技术更新和维护工作。

8.2.2 医疗保障机构宜建立机制监控技术发展趋势，评估技术更新与维护工作的风险。

参 考 文 献

[1] GB/T 39725 信息安全技术 健康医疗数据安全指南
[2] GB/T 43697 数据安全技术 数据分类分级规则
[3] ZT-T02—2020 医疗保障信息平台通用术语规范
[4] 医疗保障数据分类分级管理规范(国家医疗保障局)

中国国际科技促进会
团 体 标 准
医疗保障数据安全可信流通技术要求
T/CI 857—2024
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1　字数 15 千字
2025 年 2 月第 1 版　2025 年 2 月第 1 次印刷
*
书号:155066·5-10833　定价 31.00 元

T/CI 857-2024