

# 团体标准

T/GDWJ XXX—20XX

## 跨信任域医疗健康数据共享与流 通技术实施指南

Technical Implementation Guide for Cross-Trust Domain Medical and Health  
Data Sharing and Circulation

（征求意见稿）

20XX - XX - XX 发布

20XX - XX - XX 实施

广东省卫生经济学会 发布

所有

学会医疗标准分会版权所有

广东省卫生经济学会医疗标准分会版权所有

广东省卫生经济学会医疗标准分会版权所有

广东省卫生经济学会医疗标准

广

## 目 次

前 言 .....	III
跨信任域健康医疗数据流通与共享 .....	1
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	2
3.1 个人健康医疗数据 (GB/T 39725-2020, 3.1) .....	2
3.2 健康医疗数据 (GB/T 39725-2020, 3.2) .....	2
3.3 信任域 .....	2
3.4 健康医疗数据控制者 .....	2
3.5 跨信任域流通 .....	2
3.6 数据共享 .....	2
4 安全目标 .....	2
5 流通与共享数据管理 .....	3
5.1 数据分级、分类与编码 .....	3
5.2 数据质量控制 .....	3
5.3 数据目录管理 .....	4
5.4 数据生命周期管理 .....	4
5.5 数据隐私保护 .....	5
5.6 数据流通与共享的接收方 .....	5
6 技术要求 .....	5
6.1 数据传输技术 .....	5
6.2 数据存储技术 .....	6
6.3 数据接口技术 .....	6
6.4 数据标识与溯源技术 .....	6
6.5 互操作性技术 .....	6
6.6 隐私保护计算技术 .....	7
6.7 区块链技术 .....	7
7 安全保障 .....	8
7.1 身份认证与授权管理 .....	8
7.2 数据加密技术 .....	8
7.3 安全审计与监测 .....	8
7.4 应急响应与数据恢复 .....	9
8 安全管理 .....	9
8.1 管理机构与职责 .....	9
8.2 监督检查机制 .....	9
8.3 投诉举报与处理 .....	9
9 附则 .....	10
9.1 标准的修订 .....	10
9.2 实施日期 .....	10

附 录 A （规范性附录） 团体标准先进性评价表..... 11

附 录 B 应用场景 ..... 12

    临床医疗协同..... 12

    模型训练 ..... 12

    医学科研合作..... 12

    公共卫生监测与管理..... 12

    商业化应用场景..... 13

参考文献 ..... 14



## 前 言

本标准推荐为团体标准，旨在为跨信任域医疗健康数据流通与共享活动提供技术和管理指引。本标准不替代或超越国家现行法律法规、强制性标准及行业管理规定的要求。各应用方应在本标准指导下，结合自身实际情况，制定符合法律要求的内部管理制度与操作流程。

本规范按照GB/T 1.1—2020给出的规则起草。

本规范由提出并归口。

本规范起草单位：南方医科大学南方医院（严静东、付敬）

参与单位（暂定）：中山大学附属口腔医院（高峰），  
暨南大学附属顺德医院（吴庆斌、鲁俊杰），  
广东省卫生经济学会（李永强），  
郑州市中心医院（李伟），  
密码与网络空间安全（黄埔）研究院（咸鹤群、张宇、宋哲），  
杭州数圭通科技有限公司（肖宇），  
深圳迈瑞生物医疗电子股份有限公司（王仁行），  
湛江中心医院（欧明霖），  
广州医科大学附属口腔医院（张亮鸣），  
东莞市谢岗医院（谢耀洪），  
杭州数圭通科技有限公司  
深圳迈瑞生物医疗电子股份有限公司  
广东省电信

本规范主要起草人：后期根据沟通补充确定

本规范为首次发布。

所有

学会医疗标准分会版权所有

广东省卫生经济学会医疗标准分会版权所有

广东省卫生经济学会医疗标准分会版权所有

广东省卫生经济学会医疗标准

广

# 跨信任域健康医疗数据流通与共享

## 1 范围

本标准规定了跨信任域健康医疗数据流通与共享的基本原则、数据管理、技术要求、安全保障、应用场景及监督管理等方面的内容，旨在确保健康医疗数据在不同医疗卫生机构（包括医院、社区卫生服务中心、疾病预防控制机构、妇幼保健机构及政府主导的区域医疗协同平台等）之间安全、高效、合规地流通与共享。

本标准适用于各级各类医疗卫生机构之间，以及医疗卫生机构与政府卫生健康主管部门、区域健康信息平台之间的跨信任域数据流通与共享活动。

## 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。

《中华人民共和国数据安全法》

《中华人民共和国个人信息保护法》

《中华人民共和国网络安全法》

《中华人民共和国保险法》

《网络数据安全管理条例》

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 39725-2020 信息安全技术 健康医疗数据安全指南

GB/T 41479—2022 信息安全技术 网络数据处理安全要求

GB/T 42460—2023 信息安全技术 个人信息去标识化效果评估指南

GB/T 43697—2024 数据安全技术 数据分类分级规则

GB/T 45574—2025 数据安全技术 敏感个人信息处理安全要求

GB/T 45577—2025 数据安全技术 数据安全风险评估方法

GB/T 46903—2025 数据安全技术 个人信息保护合规审计要求

GB/T 37932—2025 数据安全技术 数据交易服务安全要求

GM/T 0111—2021 区块链密码应用技术要求

T/GDNS 002—2023 健康医疗数据合规流通标准

GM/T 0135—2024 多方安全计算 技术框架

YD/T 4690—2024 隐私计算 多方安全计算产品安全要求和测试方法

YD/T 6420—2025 隐私计算 技术应用合规指南

YD/T 6659—2026 基于差分隐私的用户个人信息保护技术要求

ISO/IEC 18033-6:2019 IT安全技术 — 加密算法

### 3 术语和定义

下列术语和定义适用于本文件。

#### 3.1 个人健康医疗数据 (GB/T 39725-2020, 3.1)

单独或者与其他信息结合后能够识别特定自然人或者反映特定自然人生理或心理健康的相关电子数据。

#### 3.2 健康医疗数据 (GB/T 39725-2020, 3.2)

包括个人健康医疗数据以及由个人健康医疗数据加工处理之后得到的健康医疗相关电子数据。

#### 3.3 信任域

在本标准中,特指受特定法律法规和技术措施或信任协议约束,实现共同的数据保护和管理目标的数据管理范围。

注 1:信任域因业务或数据保护管理目标的细分不同,可包含多个子信任域。

注 2:信任域可跨越不同通讯网络、机构和部门、以及地理区域的边界。

注 3:信任域通常由统一责任主体(如医院和其他健康服务机构)负责制订数据保护和管理的目标、规程和过程,并建立、维护、完善相应的技术体系,监控、应对和处理违反数据保护和管理的的事件。

#### 3.4 健康医疗数据控制者

在本标准中,特指某一信任域中能够决定健康医疗数据处理目的、方式及范围等的组织或个人。

注1:一个信任域通常具有一个健康医疗数据控制者,统一管理、监控和应对本信任域内健康医疗数据,并保障数据安全。

#### 3.5 跨信任域流通

健康医疗数据在不同信任域之间的传输、交换和共享过程,包括数据的推送、拉取、整合等操作方式。

#### 3.6 数据共享

在本标准中,特指不同信任域之间基于特定目的和授权机制,允许特定的健康医疗数据在授权范围内被另一信任域中个人或机构访问和使用的行为。

注 1:数据共享的目的可以由信任域之间事先约定的商业或业务目的,也可以是公共卫生、公共利益或国家安全等目的。

### 4 安全目标

健康医疗数据控制者针对健康医疗数据跨信任域流通和数据共享,应在本信任域内采取合理和适当的管理与技术保障措施,以达到以下目标:

- a) 合法性: 健康医疗数据跨信任域流通与共享应严格遵守国家相关法律法规,如《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等,确保数据来源合法、传输合法、使用合法、授权合法。
- b) 安全性: 保障健康医疗数据在跨信任域流通与共享过程中的保密性、完整性和可用性,防止数据泄露、篡改和滥用,保护个人信息安全和隐私。
- c) 知情同意: 在健康医疗数据跨信任域流通与共享前,应明确告知患者数据的流通与共享的目的、范围、接收方等信息,并获得患者或其法定代理人的有效知情同意,尊重患者的隐私权和选择权。
- d) 最小必要: 仅传输或共享满足特定业务需求或公共卫生目的的最小限度数据,避免过度共享和数据滥用。
- e) 可追溯: 健康医疗数据跨信任域的流通与共享过程中,对数据来源、流向、内容、使用情况等可全程记录、追溯、审计。
- f) 隐私保护: 健康医疗数据在跨信任域流通与共享过程中,应采取去标识化或其它技术手段,保障患者的个人隐私。

## 5 流通与共享数据管理

### 5.1 数据分级、分类与编码

#### 5.1.1 数据分级

健康医疗数据控制者应依据健康医疗数据的重要程度、风险级别以及对患者可能造成的损害和影响等因素,建立统一的分级体系,便于按照数据等级制订和执行适宜的数据保护措施。

注1: 可参照GB/T 39725-2020 6.2等标准的建议,对健康医疗数据进行分级。

#### 5.1.2 数据分类与编码

健康医疗数据控制者应依照健康医疗数据的类型,建立数据分类体系和编码规则,便于数据的管理、检索和共享,并确保数据在不同信任域之间具有一致性和可识别性。

注1: 例如,可将医疗数据分为患者基本信息类、诊断类、检查检验类、治疗类、医学影像类等,并为每类数据制定相应的编码规范。

### 5.2 数据质量控制

健康医疗数据控制者应制定数据质量标准和评估指标，包括数据的准确性、完整性、一致性、时效性等方面，确保用于跨信任域流通与共享的数据质量可靠。

注 1：例如，规定病历记录中关键信息的必填项、检查检验结果的正常参考范围等。

健康医疗数据控制者宜建立数据质量监测和反馈机制，定期对数据进行质量检查和评估，及时发现并纠正数据质量问题。对不符合质量标准的数据，应采取相应的处理措施，如数据清洗、补充完善或拒绝共享。

### 5.3 数据目录管理

健康医疗数据控制者应建立健康医疗数据目录，详细记录本信任域内可用于跨信任域流通或共享的数据资源信息，包括数据名称、数据格式、数据来源、更新频率、共享条件等内容，并向其它信任域或相关管理部门公开。

健康医疗数据控制者数据目录应保持动态更新，确保信息的及时性和准确性，以便其它信任域或相关管理部门能够快速了解和获取所需的数据资源。

### 5.4 数据生命周期管理

健康医疗数据控制者对健康医疗数据的采集、存储、传输、使用、共享、销毁等全生命周期进行规范管理。明确每个阶段的数据管理责任人和操作流程，确保数据在整个生命周期内的安全。

在数据采集阶段，健康医疗数据控制者应遵循合法、必要、准确的原则，采用标准化的采集方式和数据格式。

在存储阶段，健康医疗数据控制者应采取安全可靠的存储技术和措施，保障数据的长期保存、可访问性和安全性。

在传输阶段，健康医疗数据控制者应采用加密等安全技术确保数据传输安全，并保证和定期检查传输链路与设备的安全性。

在使用和共享阶段，健康医疗数据控制者应严格按照授权范围和规定用途使用数据

在数据不再具有使用价值或达到规定保存期限时，健康医疗数据控制者应按照安全规范进行销毁处理，确保数据无法被恢复；同时，健康医疗数据控制者应确保数据的接收者也按照安全规范进行销毁处理，确保数据无法被恢复。

健康医疗数据控制者对健康医疗数据的全生命周期管理应按照数据的不同分级，制订和执行适宜的管理机制，平衡数据安全隐私保护和数据的可用性。



## 5.5 数据隐私保护

在不影响跨信任域数据流通与共享的目的和业务需要的情况下，健康医疗数据控制者应对流通与共享的数据进行去标识化操作，保护患者的个人隐私。数据去标识化的过程和采用的技术应满足相关法律法规和数据安全标准的要求。

当数据去标识化影响跨信任域数据流通与共享的目的和业务需要时，健康医疗数据控制者宜采用差分隐私、同态加密等隐私保护计算技术，限制数据接收方对数据中隐私信息的访问和使用，在不影响流通与共享业务需要的情况下，最大限度保护患者隐私。

## 5.6 数据流通与共享的接收方

健康医疗数据控制者应确保健康医疗数据跨信任域流通与共享的接收方为有相应资质的单位或个人。

在未获得政府行业主管或监管部门批准同意的情况下，健康医疗数据控制者不得通过跨信任域的流通与共享的方式，使得健康医疗数据被境外单位（含外国组织和个人以及在我国注册的外商独资企业和中外合资、合作企业）使用。在未获得政府行业主管或监管部门批准同意的情况下，健康医疗数据不得出境。

健康医疗数据向香港特别行政区、澳门特别行政区和台湾地区相关单位或个人的流通与共享，参照本标准中关于健康医疗数据出境的相关规定执行，在未获得政府行业主管或监管部门批准同意的情况下，不得进行数据流通与共享。

# 6 技术要求

## 6.1 数据传输技术

采用安全可靠的传输协议和技术，如 TLS、IPSEC 等安全传输方式，防止数据在传输过程中被窃取或篡改。不允许使用未通过审批流程的对外端口进行数据传输，不允许改变已经审批通过的对外服务端口。

对于保护等级较高的数据，在传输前应进行加密，保证传输过程中数据的安全、隐私和完整性。加密技术的选择应符合相关法律法规和信息安全标准的要求。

支持断点续传、数据校验等功能，确保数据传输的完整性和准确性。在网络故障或传输中断时，能够自动恢复传输并保证数据的一致性。

如通过数据共享平台等方式实现医疗健康数据的跨信任域共享，则应对平台的对外服务端口进行安全审批，不允许使用未通过审批流程的对外端口提供数据访问或共享服务。对平台访问者进行多因素的身份认证，并根据访问者的身份和业务需要，对其登录访问平台，以及访问、浏览、修改数据进行控制（包括允许、限制或禁止等）。

## 6.2 数据存储技术

选用符合安全标准的存储设备和技术，对健康医疗数据进行存储。针对保护等级较高的数据，应进行加密存储，并实行加密数据与密钥分开存储。加密技术的选择应符合相关法律法规和安全标准的要求，并满足数据保护的需要。

采用冗余存储、备份恢复等措施，防止数据丢失。例如，采用分布式存储技术，将数据分散存储在多个节点上，提高数据的可靠性和可用性。

对存储的数据进行分类管理和访问控制，根据数据的敏感程度和授权级别设置不同的存储区域和访问权限，确保数据存储安全。

## 6.3 数据接口技术

制定统一的数据接口规范，包括接口格式、数据传输方式、接口调用方式等，确保不同医院的信息系统之间能够实现高效、准确的数据对接和交互。例如，采用基于 HL7 FHIR 等标准的接口规范，实现医疗数据的标准化交换。

数据接口应具备良好的兼容性和扩展性，能够适应不同医院信息系统的技术架构和数据格式差异，方便后续的系统升级和功能扩展。

## 6.4 数据标识与溯源技术

利用区块链、数字水印等技术为健康医疗数据添加唯一标识和溯源信息，实现数据的全程可追溯。通过数据标识，能够快速定位和识别数据的来源、流转路径和使用情况。

在数据流通和共享过程中，确保溯源信息的完整性和不可篡改，以便在出现数据安全问题或纠纷时能够准确追踪责任主体和数据流向。

## 6.5 互操作性技术

推动不同信任域间的健康医疗数据的互操作性，采用标准化的数据格式和接口规范，实现健康医疗数据在不同信息系统之间的无缝共享和协同应用。例如，支持不同电子病历系统之间的数据共享和集成，促进医疗服务的连续性和协同性。

建立互操作性测试和认证机制，对医院信息系统的互操作性进行评估和验证，确保系统之间能够稳定、可靠地进行数据交互和业务协同。



## 6.6 隐私保护计算技术

当无法利用数据去标识化手段保护患者个人隐私时，应利用差分隐私、同态加密、多方安全计算等隐私保护技术限制数据接受和使用方获取数据中的隐私信息。

**6.6.1 差分隐私：**在数据流通或共享前，利用差分隐私算法对数据进行适度扰动，添加一定的噪声，使得数据使用者或攻击者难以从发布的数据中推断出个体的敏感信息，同时又能保持数据的统计特征和可用性。例如，在统计患者疾病发病率时，对每个患者的数据进行微小的随机扰动，使得总体统计结果不受显著影响，但个体数据的隐私得到保护。

使用差分隐私技术时，应合理设置差分隐私的隐私预算，平衡数据隐私保护和数据可用性之间的关系。根据数据的应用场景和敏感程度，确定适当的隐私预算值，确保在保护隐私的前提下，最大限度地发挥数据的价值。同时，应对采用的差分隐私算法进行评估和验证，确保其能够满足数据隐私保护的要求。通过理论分析和实际测试，验证算法的隐私保护效果和数据可用性损失，不断优化算法性能。

**6.6.2 同态加密：**利用同态加密技术，使健康医疗数据以密文形式流通和共享，并允许授权接收方和使用方在不解密原始数据的前提下进行分析和计算<sup>[1,5]</sup>。在既定安全模型和密钥管理条件下，该技术可使计算方无需接触原始明文，从而降低隐私信息泄露风险<sup>[1,5]</sup>。

使用同态加密技术时，应综合考虑计算开销、数据规模以及密文膨胀所导致的存储和传输成本<sup>[1,5,6]</sup>。不同同态加密方案在支持的数据类型、密文编码、噪声管理和实现接口等方面存在差异，可能增加系统互操作和迁移成本<sup>[1]</sup>。

使用同态加密技术时，可根据应用场景与差分隐私、多方安全计算等隐私保护技术组合使用，形成互补的隐私保护能力<sup>[6-8]</sup>。

同态加密主要用于在数据计算或使用过程中保持密文状态并完成运算<sup>[4]</sup>；多方安全计算则侧重多个持有私有输入的参与方在不泄露各自输入的情况下联合计算，二者应根据参与方结构、信任模型和计算任务区分应用场景<sup>[5,6]</sup>。

**6.6.3 多方安全计算：**当数据跨信任域的流通与共享被用来支持临床医疗协同和医学研究合作等多方参与场景式，多方安全计算技术允许各参与方在不泄露各自数据的情况下，协助完成某个计算任务（如对医疗人工智能训练、保险公司和医疗机构协作计算保险理赔费用等），并获得正确的结果。各参与方仅能获得最终结果，而无法获得其它各方的数据，从而保证数据的隐私性，防止数据泄露。

使用多方安全计算时，应充分考虑计算的复杂度和数据规模的平衡，多方频繁交换数据带来的额外传输开销、各参与方计算能力和网络条件的异质性，参与方间的密钥分发和身份认证的安全性等。在使用多方安全计算技术时，应结合其它隐私保护技术，增强隐私保护整体能力，更具业务场景选择适宜的多方安全计算协议，采用数据预处理技术降低计算和传输开销，并确保计算全过程中数据搜集、传输、计算和存储的合规性。

## 6.7 区块链技术

数据存证：利用区块链的不可篡改特性，对医疗数据的采集、传输、整合和使用等关键环节进行存证，确保数据的完整性和真实性。每一个数据操作都记录在区块链上，形成完整的数据溯源链条，一旦数据出现问题，可以快速追溯到问题源头。

身份认证与授权：基于区块链的数字身份技术，实现对数据参与方的身份认证和授权管理。通过区块链上的智能合约，自动执行身份验证和授权规则，确保只有合法授权的用户才能访问和操作数据，提高身份认证和授权的安全性和效率。

数据共享与协同：构建基于区块链的医疗数据共享平台，促进不同信任域之间的数据共享和协同工作。通过区块链的分布式账本和共识机制，实现数据的安全共享和同步更新，避免数据孤岛和数据不一致问题。

## 7 安全保障

### 7.1 身份认证与授权管理

建立严格的身份认证机制，对参与数据流通与共享的医院、医护人员、数据管理人员等进行身份验证，确保其身份合法有效。采用多因素认证、数字证书等技术手段，提高身份认证的安全性。

基于角色和权限的访问控制策略，根据用户的角色和业务需求，为其分配相应的数据访问权限。权限管理应实现动态调整，及时根据用户角色变化或业务需求变更更新访问权限。例如，医生只能访问其诊疗范围内患者的相关数据，且访问权限应根据其科室、职称等因素进行细粒度划分。

### 7.2 数据加密技术

对健康医疗数据进行全生命周期的加密保护，包括数据存储加密、传输加密和使用加密。应优先采用国家密码管理局认可的商用密码算法（如 SM2/SM3/SM4 等）进行加密，确保数据的保密性。当与其他国际通行系统、算法兼容或业务场景有特殊要求时，可采用 AES、RSA 等国际标准加密算法，但需通过合规评估与审批。

定期更新加密密钥，加强密钥管理（保护密钥分发和存储），防止密钥泄露导致数据安全风险。同时，建立密钥备份和恢复机制，确保在密钥丢失或损坏时能够及时恢复数据的加密保护。

### 7.3 安全审计与监测

构建完善的安全审计机制和保障技术，对数据流通与共享过程中的所有操作行为进行实时审计和记录，包括数据访问、传输、修改等操作。审计记录应包括操作时间、操作人、操作对象、操作内容等详细信息，以便事后追溯和分析。

设立安全监测机制，通过实时监测数据流量、系统日志、网络连接等信息，及时发现和预警潜在的数据安全威胁和异常行为。一旦发现安全事件，应立即启动应急预案，采取相应的处置措施，降低安全风险。

#### 7.4 应急响应与数据恢复

制定数据安全应急响应预案，明确在数据泄露、系统故障、网络攻击等安全事件发生时的应急响应流程和措施。应急响应预案应包括事件报告、应急处置、数据恢复、调查评估等环节，确保能够快速、有效地应对安全事件。

建立数据备份和恢复机制，定期对健康医疗数据进行备份，并将备份数据存储在安全可靠的位置。在发生数据丢失或损坏时，能够及时利用备份数据进行恢复，保障数据的可用性和完整性。

### 8 安全管理

#### 8.1 管理机构与职责

明确健康医疗数据跨信任域流通与共享的监督管理机构，如卫生健康行政部门或相关专业机构，负责制定政策法规、监督标准执行、协调各方关系等工作。

健康医疗数据控制者是数据跨信任域流通与共享的责任主体，应建立数据跨域流通与共享安全管理部门（可作为数据安全管理部门的一部分），负责管理、监督、改进本信任域内数据跨域流通与共享的工作。

数据跨域流通与共享安全管理部门应在本信任域内建立完善的组织保障体系，明确相关人员的职责，制订相关规划和过程，管理、检查、改进数据跨信任域流通与共享工作，应对处置数据跨域流通与共享过程中出现的安全事件。

数据跨域流通与共享安全管理部门应建立健全监督管理机制，加强对数据跨信任域流通与共享行为的日常监督检查，定期评估数据安全和合规情况，及时发现和纠正存在的问题。

#### 8.2 监督检查机制

制定详细的监督检查计划和流程，采用定期检查与不定期抽查相结合的方式，对健康医疗数据跨信任域流通与共享安全管理制度建设、技术措施落实、数据流通与共享操作规范等方面进行检查。

建立监督检查结果公示制度，对检查结果进行公开通报，对存在严重问题的部门和个人进行督促整改，并依法依规追究相关责任人的责任。

#### 8.3 投诉举报与处理

建立投诉举报渠道，鼓励内部人员、患者或其他相关方对数据流通与共享过程中的违法违规行为进行投诉举报。管理机构应及时受理投诉举报，并按照规定的程序进行调查和处理。

对投诉举报人的信息进行严格保密，保护举报人合法权益。对查证属实的投诉举报，给予举报人适当奖励，提高公众参与监督的积极性。

## 9 附则

### 9.1 标准的修订

本标准应根据国家法律法规的变化、技术发展的进步以及实际应用中的反馈，适时进行修订。修订程序应遵循相关规定，确保修订过程的公开、透明和科学。

### 9.2 实施日期

本标准自发布之日起〔具体实施日期〕实施，各医院应在规定时间内完成相关系统的改造和制度建设，确保符合本标准的要求。在实施过程中，应加强对医院的培训和指导，帮助医院顺利过渡到新的标准体系。

以上草案内容仅供参考，可根据实际情况和进一步的研究讨论进行完善和细化。在制定过程中，需充分征求医疗行业专家、医院信息管理人员、法律专业人士等多方面的意见和建议，确保标准的科学性、实用性和可操作性。

附 录 A  
(规范性附录)  
团体标准先进性评价表

表A.1 团体标准先进性评价表

被评团体标准			参照物				先进性
指标名	指标值	证明材料 编号	名称	级别	相应指标值	证明材 料编号	



## 附录 B

### （资料性附录）

### 应用场景

#### 临床医疗协同

支持不同医院之间的远程会诊、转诊转院等医疗协同业务。在远程会诊中，经患者授权后，会诊医生能够安全地获取患者在转出医院的病历、检查检验结果等数据，为患者提供准确的诊断和治疗建议。

在转诊转院过程中，实现患者医疗数据的无缝交接，确保接收医院能够全面了解患者的病情历史，减少重复检查和医疗风险，提高医疗服务效率和质量。

#### 模型训练

支持医疗人工智能（AI）等模型的开发与训练业务，如医学影像辅助诊断、疾病风险预测、个性化治疗推荐等。通过跨信任域的数据流通与协同，医疗机构、科研院所及 AI 研发企业可在合规授权范围内，利用多中心、大规模的真实世界健康医疗数据联合开展模型训练，从而有效打破“数据孤岛”，提升人工智能模型的准确性、鲁棒性与泛化能力。

在模型训练的协作过程中，应严格落实患者隐私保护与数据安全。由于涉及多方参与场景，可充分结合同态加密、多方安全计算等隐私保护计算技术，允许各参与方在不泄露各自原始数据的前提下，协助完成医疗人工智能训练等计算任务。以此确保各参与方仅能获得最终的模型训练结果或参数，而无法获取他方的底层明文数据，在实现数据“可用不可见”的同时，保障全过程数据收集、传输、计算和存储的合规性。

#### 医学科研合作

促进医院之间在医学科研领域的合作，科研人员可在授权范围内获取多中心临床研究所需的数据资源，开展大规模的医学研究项目。例如，针对某种疾病的流行病学研究、药物临床试验等，通过整合不同医院的病例数据，提高研究的样本量和代表性，加速医学科研创新进程。

建立科研数据管理和共享平台，对科研数据的使用进行规范管理，确保数据的使用符合科研伦理和法律法规要求，保护患者隐私和数据安全。

#### 公共卫生监测与管理

助力公共卫生部门及时获取各医院的相关医疗数据，如传染病疫情信息、疾病监测数据等，实现对公共卫生事件的实时监测、预警和分析。通过对多源医疗数据的汇聚和分析，能够更准确地掌握疾病的流行趋势、传播路径和防控效果，为公共卫生决策提供科学依据。

医院应按照公共卫生管理要求，及时、准确地向指定的公共卫生信息平台上传相关数据，并确保数据的质量和安全性。公共卫生部门对获取的数据进行严格的管理和使用，保护数据提供医院和患者的权益。

### 商业化应用场景

**风险评估与定价：**保险机构可依据合法获取的医疗数据，对投保人的健康风险进行精准评估，从而实现更合理的保险产品定价。例如，通过分析投保人的既往病史、体检数据及家族疾病史等信息，确定其患病概率及潜在赔付风险，为制定个性化的保险费率提供数据支撑，使保险定价更贴合实际风险状况，保障保险市场的公平性与稳定性。

**理赔服务优化：**在保险理赔环节，利用医疗数据协助快速核实理赔申请的真实性与合理性。当被保险人提出理赔请求时，保险公司可通过与医疗机构的数据共享，获取相关医疗记录和诊断证明，加速理赔审核流程，提高理赔效率，减少欺诈行为的发生，同时为被保险人提供更便捷的理赔服务体验。

## 附 录 C参考文献

[1] 河人华, 李冰, 杜一博, 等. 基于容错学习问题的全同态加密算法和硬件优化综述[J]. 计算机研究与发展, 2025, 62(7): 1738-1753. DOI:10.7544/issn1000-1239.202331022

[2] 王志伟, 赵路坦, 程佳豪, 等. 基于同态加密的隐私保护神经网络研究综述[J/OL]. 信息安全学报, [网络首发日期][引用日期]. DOI:10.19363/J.cnki.cn10-1380/tn.2025.04.01

[3] 刘芬, 李永强, 王明生. 同态友好的对称密码算法研究综述[J/OL]. 信息安全学报, [网络首发日期][引用日期]. DOI:10.19363/J.cnki.cn10-1380/tn.2025.04.06

[4] 中国信息通信研究院. 隐私保护计算技术研究报告(2020年)[R/OL]. (2020-11-10)[引用日期]. 获取和访问路径

[5] 中国信息通信研究院. 隐私保护计算与合规应用研究报告(2021年)[R/OL]. (发布日期)[引用日期]. 获取和访问路径