

# 团体标准

T/GDWJ XXXX—2026

## 医疗机构可信数据空间建设指南

Construction Guidelines for Trusted Medical Data Space in Medical Institutions

(征求意见稿)

2026-XX-XX 发布

2026-XX-XX 实施

广东省卫生经济学会 发布

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

广东省卫生经济学会医疗标准分会版权所有

学会医疗标准分会版权所有

# 目录

前言 .....	5
1 范围 .....	6
2 规范性引用文件 .....	6
3 术语和定义 .....	6
3.1 可信数据空间 Trusted Data Space .....	7
3.2 医疗机构可信数据空间 Trusted Data Space for Healthcare Institution .....	7
3.3 数据资源 Data Resource .....	7
3.4 数据产品 Data Product .....	7
3.5 数据目录 Data Catalog .....	7
4 缩略语 .....	7
5 建设原则 .....	8
5.1 合法合规原则 .....	8
5.2 安全可信原则 .....	8
5.3 数据可控原则 .....	9
5.4 开放共享原则 .....	9
5.5 价值共创原则 .....	9
6 空间建设架构 .....	9
6.1 总体架构 .....	9
6.2 参与主体 .....	10
6.3 架构组成 .....	11
7 基础设施建设 .....	12
7.1 网络基础设施 .....	12
7.2 算力基础设施 .....	12
7.3 存储基础设施 .....	13
7.4 容灾备份设施 .....	13
7.5 密码基础设施 .....	13
8 数据资源建设 .....	13
8.1 数据资源体系 .....	13
8.2 数据资源汇聚 .....	14
8.3 数据分类分级 .....	14
8.4 数据目录管理 .....	14
8.5 数据资源登记 .....	14
8.6 数据资产管理 .....	15
9 可信能力建设 .....	15
9.1 可信身份管理 .....	15
9.2 数据授权管理 .....	16
9.3 访问控制管理 .....	16
9.4 合约与规则管理 .....	16
9.5 全流程审计管理 .....	16
9.6 数据确权与存证 .....	17
10 数据流通利用建设 .....	17
10.1 数据共享交换 .....	17
10.2 数据产品管理 .....	17
10.3 数据服务管理 .....	17
10.4 数据开发利用 .....	18
10.5 数据开放应用 .....	18
10.6 数据交易流通 .....	18
10.7 数据价值实现 .....	18

11 安全保障建设 .....	19
11.1 安全管理体系 .....	19
11.2 数据安全保护 .....	19
11.3 个人信息保护 .....	19
11.4 隐私计算能力 .....	19
11.5 密钥管理 .....	20
11.6 安全监测与预警 .....	20
11.7 应急响应管理 .....	20
12 运营管理 .....	21
12.1 组织管理 .....	21
12.2 制度管理 .....	21
12.3 服务管理 .....	21
12.4 生态管理 .....	21
12.5 合规管理 .....	22
12.6 风险管理 .....	22
13 运行维护 .....	22
13.1 运维管理 .....	22
13.2 配置管理 .....	22
13.3 日志管理 .....	22
13.4 性能监测 .....	23
13.5 故障处理 .....	23
13.6 持续改进 .....	23
参考文献 .....	23



## 前言

本文件按照GB/T1.1—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。

请注意本文件的其他内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由广东省卫生经济学会提出并归口。

本文件起草单位：南方医科大学南方医院，联通数智医疗科技有限公司，广州医科大学附属口腔医院（广州医科大学羊城医院）等。

本文件起草人：严静东、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX、XXX。

# 1 范围

本文件规定了医疗机构可信数据空间建设的总体原则、总体架构、基础设施、数据资源管理、可信身份管理、数据授权与访问控制、数据流通利用、安全保障、运营管理以及评价改进等方面的要求。

本文件适用于各级各类医疗机构可信数据空间的规划、设计、建设、运营和管理，开展医疗健康数据资源共享与开发利用活动。

本文件面向医疗健康数据要素共享利用需求，规范医疗机构在数据资源汇聚、治理、目录编制、确权授权、可信共享、融合应用、开发利用、监管审计和安全防护等方面的建设要求，支撑医疗健康数据在医疗服务、医院管理、医学科研、公共卫生、药械研发、医保服务、人工智能训练与应用等场景中的合规流通、安全共享和可信利用。

本文件不涉及医疗业务流程管理、医疗卫生专业技术规范以及医疗信息系统功能建设要求，相关内容应遵循国家、行业和地方现行法律法规、标准规范及管理要求。

## 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 39560-2020 信息安全技术 零信任架构
- GB/T 39725-2020 信息安全技术 医疗数据安全指南
- GB/T 42490-2023 信息安全技术 网络安全等级保护基本要求
- TC609-6-2025-01 可信数据空间 技术架构
- T/CITIF 004-2023 信息技术云桌面技术要求
- WS/T 598-2018 卫生统计指标（所有部分）
- WS 599-2018 医疗机构人财物运营管理基本数据集（所有部分）
- T/GZBC 37-2020 医疗机构数据治理规范
- NDI-TR-2025-03 数据基础设施用户身份管理和接入规范

《可信数据空间发展行动计划（2024—2028 年）》

## 3 术语和定义

TC609-6-2025-01界定的以及下列术语和定义适用于本文件。

### 3.1 可信数据空间 Trusted Data Space

基于共识规则、可信身份、统一标准和技术架构构建的数据流通利用基础设施，通过可信管控机制实现数据资源安全共享、授权使用、流通交换和价值共创的运行环境。

### 3.2 医疗机构可信数据空间 Trusted Data Space for Healthcare

#### Institution

以医疗机构为主体构建的可信数据空间，面向医疗服务、医学科研、医院管理、公共卫生、药械研发和人工智能应用等场景，通过可信身份认证、数据授权控制、隐私保护计算、安全审计等机制，实现医疗健康数据的安全汇聚、可信流通和合规利用。

### 3.3 数据资源 Data Resource

具有开发利用价值、以电子形式记录并能够被采集、存储、加工、传输、共享和应用的数据集合。

### 3.4 数据产品 Data Product

以数据资源为基础，经治理、加工、分析、建模或封装形成，能够满足特定业务需求并可供共享、交换或使用的数据服务、数据集、模型、知识库等成果。

### 3.5 数据目录 Data Catalog

按照统一规则对数据资源进行分类、描述、登记和管理形成的信息集合，用于实现数据资源发现、检索和共享。

## 4 缩略语

下列缩略语适用于本文件。

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

CA: 证书颁发机构 Certificate Authority

DSS: 数据安全系统 Data Security System

EHR: 电子健康档案 Electronic Health Record

EMR: 电子病历 Electronic Medical Record

IDS: 身份管理系统 Identity System

KMS: 密钥管理系统 Key Management System

NLP: 自然语言处理 Natural Language Processing

PII: 个人身份信息 Personally Identifiable Information

SDK: 软件开发工具包 Software Development Kit

TEE: 可信执行环境 Trusted Execution Environment

TDS: 可信数据空间 Trusted Data Space

UI: 用户界面 User Interface

VPN: 虚拟专用网络 Virtual Private Network

## 5 建设原则

医疗机构可信数据空间建设应以促进医疗健康数据安全流通和价值释放为目标，遵循合法合规、安全可信、数据可控、开放共享和价值共创的原则，构建安全、高效、可持续的数据流通利用生态体系。

### 5.1 合法合规原则

医疗机构可信数据空间建设应遵循国家法律法规、行业监管要求和相关标准规范，建立覆盖数据采集、存储、治理、传输、共享、开发利用和销毁全过程的合规管理机制。

建设过程中应符合《中华人民共和国网络安全法》《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》等法律法规要求，落实数据分类分级管理制度，明确数据权责边界和使用规则，保障数据处理活动合法、正当、必要。

涉及个人信息、重要数据和敏感医疗健康数据处理活动时，应建立风险评估、授权审批、审计监督和责任追溯机制，确保数据流通利用全过程依法合规。

### 5.2 安全可信原则

医疗机构可信数据空间应构建覆盖身份认证、授权管理、访问控制、数据保护、行为审计和风险防控的可信体系，保障数据流通全过程安全可信。

应采用可信身份认证、数字证书、密码技术、隐私计算、可信执行环境等技术手段，实现参与主体可信、数据来源可信、使用过程可信和流通结果可信。

应建立安全监测、风险预警、应急响应和持续改进机制，及时发现和处置数据安全风险，保障医疗健康数据的机密性、完整性、可用性和可追溯性。

## 5.3 数据可控原则

医疗机构应始终保持对数据资源的管理权和控制权，确保数据提供方能够自主决定数据开放范围、授权方式、使用条件和流通规则。

可信数据空间应支持细粒度授权管理、动态权限控制、全过程审计追踪和数据使用监管，实现“数据可用不可见、数据不动价值流动”的流通模式。

数据使用活动应遵循最小必要原则，确保数据访问权限与业务需求相匹配，防止数据滥用、越权访问和未经授权的数据扩散。

## 5.4 开放共享原则

在确保数据安全和隐私保护的前提下，医疗机构可信数据空间应建立统一标准、统一接口和统一规则体系，促进不同机构、不同系统和不同区域之间的数据互联互通。

应推动医疗健康数据资源目录化管理和服务化供给，提高数据资源发现、共享和利用效率，降低数据流通成本。

应支持跨机构、跨区域、跨行业的数据协同应用，促进医疗服务、医学科研、公共卫生、医保管理和产业创新等领域的数据融合应用。

## 5.5 价值共创原则

医疗机构可信数据空间建设应坚持共建共享、合作共赢的发展理念，推动数据资源、技术能力、应用场景和生态伙伴协同发展。

应建立多主体参与机制，鼓励医疗机构、科研院所、高校、企业和政府部门共同参与数据空间建设与运营，形成开放协同的数据生态体系。

应通过数据资源开发利用、数据产品创新和数据服务供给，充分释放医疗健康数据要素价值，促进医疗服务能力提升、科研创新发展和数字健康产业培育，实现社会效益与经济效益协同提升。

# 6 空间建设架构

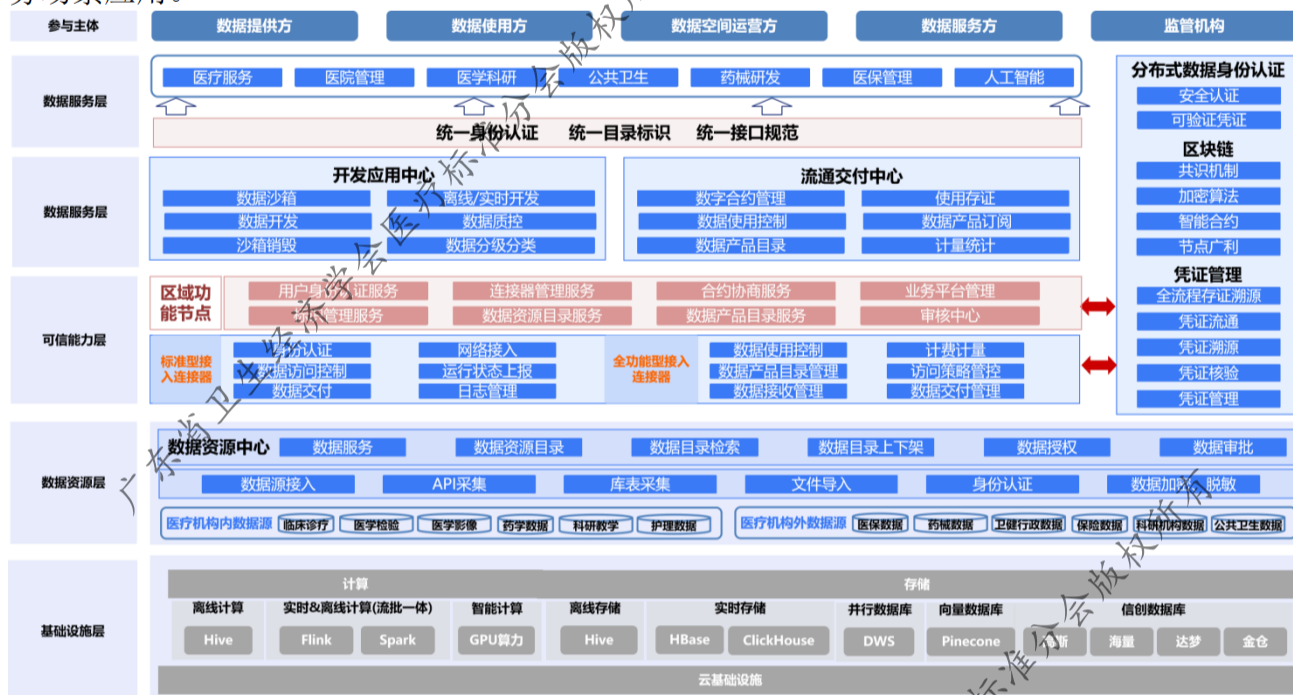
## 6.1 总体架构



医疗机构可信数据空间应围绕医疗健康数据要素安全流通与高效利用需求，遵循统一标准、互联互通、数据可控、安全可信和开放协同的建设理念，构建覆盖数据资源汇聚、治理管理、流通共享、开发利用和运营服务全过程的空间架构。

可信数据空间总体架构由参与主体、基础设施层、数据资源层、可信能力层、数据服务层和应用生态层构成。各层之间通过统一标准和接口实现协同运行，共同支撑医疗健康数据资源的安全流通和价值释放。

其中，参与主体是数据空间建设与运行的核心力量；基础设施层提供网络、算力、存储和安全运行环境；数据资源层负责医疗健康数据资源的汇聚和管理；可信能力层为数据流通提供身份认证、授权控制和安全保护等基础保障；数据服务层提供数据共享交换、数据产品开发和数据服务供给能力；应用生态层支撑医疗服务、医学科研、公共卫生和产业创新等业务场景应用。



## 6.2 参与主体

医疗机构可信数据空间参与主体主要包括数据提供方、数据使用方、数据空间运营方、数据服务方和监管机构。各参与主体依据统一规则开展协同合作，共同构建开放共享、互信互认、合作共赢的数据流通生态体系。

### 6.2.1 数据提供方

数据提供方是指依法拥有医疗健康数据持有权、管理权或者授权处置权，并向可信数据空间提供数据资源的组织。数据提供方主要包括医疗机构、公共卫生机构、医学检验机构、医学影像机构以及其他依法持有医疗健康数据的组织。

数据提供方应按照相关法律法规和管理要求，对提供的数据资源进行治理、分类分级、质量控制和授权管理，确保数据来源真实可靠、内容准确完整，并持续维护数据资源的时效性和可用性。

### 6.2.2 数据使用方

数据使用方是指依据授权规则获取数据资源、数据产品或者数据服务并开展相关业务活动的组织或个人。数据使用方主要包括医疗机构、科研院所、高等院校、药械研发机构、人工智能研发机构以及其他依法获得授权的主体。

数据使用方应严格按照授权范围和使用目的开展数据利用活动，不得超范围使用、擅自复制传播或者违规处理相关数据，并承担相应的数据安全保护责任。

### 6.2.3 数据空间运营方

数据空间运营方是指负责可信数据空间规划建设、运行维护、规则管理和生态运营的组织。运营方负责建立数据空间运行规则和管理机制，协调各参与主体关系，保障平台稳定运行，组织开展安全管理和风险防控，推动数据资源流通利用和生态体系建设。

运营方应建立完善的运营管理制度和服务体系，持续提升数据空间服务能力和运营水平。

### 6.2.4 数据服务方

数据服务方是指为可信数据空间建设和运行提供技术支撑、产品支撑和专业服务的组织。数据服务方可提供数据治理、数据开发、数据分析、隐私计算、安全防护、模型训练、数据产品开发等服务。

数据服务方应遵循统一技术标准和安全规范，确保服务过程合法合规、安全可靠，并接受运营方的统一管理和监督。

### 6.2.5 监管机构

监管机构是指依法对医疗机构可信数据空间建设和运行活动实施监督管理的政府部门及其授权机构。监管机构负责制定监管要求，组织开展监督检查、安全评估和风险监测，对数据流通利用活动进行全过程监督管理。

监管机构应建立协同监管机制，推动医疗健康数据安全治理和行业规范发展，保障数据空间健康有序运行。

## 6.3 架构组成

### 6.3.1 基础设施层

基础设施层是医疗机构可信数据空间运行的基础支撑层，为数据资源管理和流通利用提供网络、算力、存储和安全运行环境。基础设施层应具备高可靠性、高可用性和可扩展性，能够满足医疗健康数据大规模存储、高并发访问和复杂计算处理需求。

基础设施层主要包括网络设施、算力设施、存储设施、云平台设施、密码基础设施、安全监测设施以及容灾备份设施等，为可信数据空间安全稳定运行提供基础保障。

### 6.3.2 数据资源层

数据资源层是医疗机构可信数据空间的数据基础，负责医疗健康数据资源的汇聚、治理、组织和管理。数据资源层应建立统一的数据资源管理体系，实现数据资源的分类分级、标准化治理、目录编制、资源登记和质量管理。

数据资源范围包括电子病历数据、电子健康档案数据、医学影像数据、检验检查数据、公共卫生数据、医院运营管理数据、科研数据以及医疗设备运行数据等医疗健康相关数据资源。

### 6.3.3 可信能力层

可信能力层是医疗机构可信数据空间实现安全流通和可信协同的核心能力层，为数据流通过程提供身份可信、行为可信、数据可信和环境可信保障。

可信能力层应具备可信身份认证、授权管理、访问控制、数据加密、隐私计算、可信执行环境、电子签名、可信存证、全流程审计以及风险监测预警等能力，实现数据流通全过程可验证、可控制、可追溯和可审计。

#### 6.3.4 数据服务层

数据服务层面向数据资源开发利用需求，提供标准化、服务化和可扩展的数据服务能力。通过统一服务接口和服务管理机制，实现数据资源发现、共享交换、开发利用和价值转化。

数据服务层应具备数据目录服务、数据检索服务、数据共享交换服务、数据产品服务、数据开发服务、模型服务、知识服务以及运营服务等能力，为数据流通利用提供支撑。

#### 6.3.5 应用生态层

应用生态层是医疗机构可信数据空间价值实现的重要载体，通过汇聚多方资源和应用能力，推动医疗健康数据在医疗服务、医院管理、医学科研、公共卫生、药械研发、医保管理和人工智能等领域的创新应用。

应用生态层应支持跨机构、跨区域和跨行业协同应用，促进数据资源共享和业务协同创新，推动医疗健康数据要素价值释放，形成开放、合作、共赢的数据空间生态体系。

## 7 基础设施建设

医疗机构可信数据空间应建立安全可靠、弹性扩展、自主可控的基础设施体系，为数据资源汇聚治理、可信流通、开发利用和运营管理提供稳定支撑。基础设施建设应统筹网络、算力、存储、安全和灾备等资源，满足医疗健康数据高安全、高并发、高可用和持续运营的要求。

### 7.1 网络基础设施

网络基础设施应为医疗机构可信数据空间提供安全、稳定、高效的网络通信环境，满足数据汇聚、共享交换、协同计算和跨机构互联互通需求。

网络建设应采用分层分域架构，合理划分业务区、数据区、管理区和安全区，实现网络边界隔离和访问控制。应支持IPv6、虚拟专用网络（VPN）、专线网络以及安全接入服务，保障不同参与主体之间的数据传输安全。

网络基础设施应具备网络访问控制、入侵检测、防病毒、防拒绝服务攻击、流量监测和异常预警等安全防护能力，并能够满足医疗健康数据跨机构流通和高并发访问需求。

### 7.2 算力基础设施

算力基础设施应满足医疗机构可信数据空间数据处理、数据分析、人工智能训练、隐私计算和模型推理等业务需求，为数据流通利用提供计算资源保障。

算力资源应支持集中部署与分布式协同相结合的建设模式，能够根据业务规模动态扩展计算能力。宜采用云计算、容器化、虚拟化和分布式计算等技术，提高资源利用效率和服务弹性。

对于医学影像分析、人工智能模型训练、联邦学习和多方协同计算等场景，应提供高性能计算资源支持，保障计算任务高效稳定运行。



## 7.3 存储基础设施

存储基础设施应满足医疗健康数据全生命周期管理需求，支持结构化数据、非结构化数据和半结构化数据的统一存储和管理。

存储系统应具备大容量、高可靠、高性能和可扩展能力，能够满足电子病历、医学影像、检验检查、科研数据等海量数据存储需求。应支持分布式存储、对象存储、数据库存储以及冷热数据分级存储等模式。

存储基础设施应建立数据备份、完整性校验、访问控制和加密保护机制，确保数据存储安全和长期可用。对于重要数据和核心业务数据，应采取多副本存储和异地保存措施，提高数据保护能力。

## 7.4 容灾备份设施

容灾备份设施应保障医疗机构可信数据空间在设备故障、网络中断、系统异常、自然灾害等突发情况下持续运行和快速恢复。

应建立覆盖数据、应用和平台的容灾备份体系，明确恢复时间目标（RTO）和恢复点目标（RPO），定期开展容灾演练和恢复验证。

重要业务系统宜采用同城双活、异地灾备或多中心容灾架构，实现关键业务连续运行。备份数据应与生产环境隔离存储，并采取加密和访问控制措施，防止数据泄露和篡改。

## 7.5 密码基础设施

密码基础设施是医疗机构可信数据空间实现身份可信、数据可信和传输可信的重要支撑，应符合国家密码管理相关法律法规和技术标准要求。

密码基础设施应支持数字证书管理、身份认证、电子签名、数据加密、密钥管理和安全通信等功能，实现数据传输、存储和使用全过程密码保护。

应建立统一的密钥管理机制，对密钥生成、分发、使用、更新、备份、恢复和销毁等环节进行规范管理。涉及重要数据、敏感个人信息和跨机构数据流通活动时，应采用符合国家要求的商用密码技术进行保护。

密码基础设施应与可信身份认证、授权管理、访问控制和审计追踪等能力协同运行，为医疗机构可信数据空间提供持续、可靠的安全保障。

## 8 数据资源建设

医疗机构可信数据空间应建立覆盖数据资源汇聚、治理、管理、流通和利用全过程的数据资源体系，推动医疗健康数据标准化、规范化和资产化管理，提升数据资源质量和开发利用水平，为数据要素价值释放提供基础支撑。

### 8.1 数据资源体系

医疗机构应围绕医疗服务、医院管理、医学科研、公共卫生和健康产业发展需求，构建统一规范的数据资源体系。数据资源体系应覆盖医疗机构业务运行和管理活动产生的各类数据资源，形成层次清晰、结构合理、分类科学的数据资源组织架构。

数据资源体系宜包括电子病历数据、电子健康档案数据、医学影像数据、检验检查数据、护理数据、药学数据、公共卫生数据、医院运营管理数据、科研数据、医疗设备数据以及互联网医疗数据等。数据资源应按照统一标准进行组织管理，实现跨系统、跨部门和跨机构的数据协同共享。

医疗机构应建立统一的数据标准体系，规范数据编码、数据格式、数据交换和数据管理要求，保障数据资源的一致性和互操作性。

## 8.2 数据资源汇聚

医疗机构应建立统一的数据资源汇聚机制，实现多源异构医疗健康数据的规范接入和集中管理。

数据汇聚范围应覆盖医疗机构内部业务系统以及依法授权接入的外部数据资源，包括医院信息系统、电子病历系统、检验信息系统、医学影像系统、护理系统、公共卫生系统、医保系统及其他相关业务系统产生的数据。

数据汇聚过程中应建立统一的数据采集标准和接口规范，确保数据来源清晰、内容完整、传输安全和过程可追溯。对于跨机构数据汇聚活动，应按照授权规则和安全要求开展数据接入和资源共享。

医疗机构应建立数据资源动态更新机制，保障数据资源的及时性、完整性和连续性。

## 8.3 数据分类分级

医疗机构应依据国家和行业有关数据分类分级要求，建立医疗健康数据分类分级管理制度。

数据分类应根据业务属性、应用场景和管理需求，对医疗健康数据进行科学分类。数据分级应综合考虑数据的重要程度、敏感程度、影响范围以及潜在风险等因素，对数据实施差异化保护和管理。

分类分级结果应作为数据授权、访问控制、安全防护、共享开放和流通利用的重要依据。数据类别和等级发生变化时，应及时进行动态调整和更新。

涉及个人信息、重要数据和国家规定重点保护数据的，应按照相关法律法规要求实施重点保护。

## 8.4 数据目录管理

医疗机构应建立统一的数据目录管理体系，对数据资源进行规范化描述、登记和发布。

数据目录应全面反映数据资源基本信息、数据来源、数据内容、数据标准、数据质量、共享属性、开放属性、安全等级和使用条件等内容，实现数据资源可发现、可查询和可管理。

数据目录应采用统一编码规则和元数据标准进行管理，并支持目录动态更新和版本维护。医疗机构应定期开展目录核查和更新工作，保证目录信息准确有效。

数据目录宜支持跨机构目录互联互通和统一检索，为数据资源共享流通提供支撑。

## 8.5 数据资源登记

医疗机构应建立数据资源登记管理机制，对纳入可信数据空间管理的数据资源进行统一登记。

数据资源登记内容应包括资源名称、资源提供方、资源描述、数据规模、数据分类分级情况、数据质量状态、授权方式、更新周期以及责任主体等信息。

登记过程应确保信息真实、准确和完整，并形成统一的数据资源登记台账。对于新增、变更、暂停使用或者退出管理的数据资源，应及时更新登记信息。

数据资源登记结果应作为数据授权流通、产品开发和价值评估的重要依据。

## 8.6 数据资产管理

医疗机构应建立数据资产管理机制，推动数据资源向数据资产转化，实现数据价值的有效管理和持续释放。

数据资产管理应覆盖数据资源识别、资产登记、价值评估、运营管理、收益管理和风险管理等环节。医疗机构应明确数据资产管理责任主体，建立资产台账和动态管理机制。

对于具备流通利用条件的数据资源，应结合业务需求开展数据产品开发、数据服务供给和价值运营，提升数据资源利用效率和资产价值。

数据资产管理活动应遵循合法合规、安全可控和价值导向原则，确保数据资产开发利用与安全保护协调发展，实现医疗健康数据资源的可持续运营和价值创造。

## 9 可信能力建设

可信能力是医疗机构可信数据空间实现数据安全流通、可信共享和合规利用的核心保障。医疗机构应建立覆盖身份认证、授权管理、访问控制、规则执行、行为审计和可信存证等全过程的可信能力体系，实现参与主体可信、数据资源可信、流通过程可信和使用结果可信，为数据要素流通利用提供技术和管理支撑。

### 9.1 可信身份管理

医疗机构可信数据空间应建立统一的可信身份管理体系，对参与主体、用户、设备以及相关数字身份进行统一认证和管理，实现身份真实可信、行为可追溯、权限可管控。

可信身份管理应贯穿数据资源接入、服务调用、数据流通和运营管理全过程，并支持跨机构身份互认和可信认证。

#### 9.1.1 机构身份管理

医疗机构可信数据空间应建立机构身份管理机制，对参与数据空间建设和运行的各类组织进行统一身份标识和认证管理。

机构身份管理应对机构名称、统一社会信用代码、行业资质、业务范围、授权权限等信息进行登记和核验，确保机构身份真实、合法、有效。对于接入可信数据空间的医疗机构、科研机构、企业和其他组织，应建立准入审核和动态管理机制。

机构身份信息发生变更时，应及时更新相关信息，并重新进行身份核验和授权确认。

#### 9.1.2 用户身份管理

医疗机构可信数据空间应建立用户身份管理机制，对系统用户进行统一身份认证和权限管理。

用户身份管理应支持实名注册、身份认证、单点登录、多因素认证以及动态权限管理等功能。根据岗位职责、业务需求和安全等级要求，对用户实施分级分类管理。

用户身份信息、权限变更和登录行为应进行全过程记录，并具备可查询、可追溯和可审计能力。

#### 9.1.3 设备身份管理

医疗机构可信数据空间应建立设备身份管理机制，对接入数据空间的服务器、终端设备、网络设备、医疗设备以及其他智能设备进行统一身份标识和可信认证。

设备接入前应完成身份注册和安全认证，并建立设备身份档案。设备身份管理应支持设备状态监测、接入控制、安全评估和生命周期管理。

对于存在安全风险、身份异常或者不符合接入要求的设备，应限制或终止其接入权限。

#### 9.1.4 数字证书管理



医疗机构可信数据空间应建立数字证书管理体系，为机构、用户、设备以及系统服务提供可信数字身份凭证。

数字证书应支持身份认证、数字签名、数据加密、安全通信和可信存证等应用场景。证书管理应覆盖申请、签发、更新、吊销、归档和销毁全过程，并确保其真实性、唯一性和有效性。

数字证书管理应符合国家密码管理和电子认证相关要求，并支持跨机构可信互认。

## 9.2 数据授权管理

医疗机构可信数据空间应建立统一的数据授权管理机制，实现数据资源使用权限的规范化管理。

数据授权应遵循合法合规、最小必要、明确授权和动态管理原则，明确数据提供方、数据使用方和数据服务方的权利义务关系。

授权内容应包括授权主体、授权对象、授权范围、授权期限、使用目的、使用方式以及安全责任等信息。授权过程应形成完整记录，并支持授权审批、授权变更、授权撤销和授权到期管理。

数据授权应与数据分类分级管理要求相匹配，对重要数据、敏感数据和个人信息实施差异化授权控制。

## 9.3 访问控制管理

医疗机构可信数据空间应建立统一的访问控制机制，对数据资源、服务资源和系统资源实施精细化访问管理。

访问控制应基于身份认证结果和授权规则进行动态决策，实现用户、机构、设备和应用的访问权限控制。根据数据安全等级和业务需求，可采用基于角色、基于属性、基于策略或者多种方式组合的访问控制模式。

访问控制应支持访问申请、权限审批、权限分配、权限调整和权限回收等全过程管理，并实时监测访问行为，防止越权访问、违规操作和数据泄露。

## 9.4 合约与规则管理

医疗机构可信数据空间应建立统一的合约与规则管理机制，对数据流通活动中的权责关系、使用规则和执行过程进行规范管理。

合约应明确参与主体、数据资源范围、授权条件、使用方式、安全要求、收益分配和违约责任等内容，并能够在数据流通过程中自动执行和验证。

规则管理应覆盖数据接入、资源登记、授权共享、访问控制、开发利用、审计监督和退出管理等环节，实现规则统一发布、动态更新和持续优化。

对于跨机构数据流通活动，应建立规则协同和互认机制，保障数据流通行为规范有序开展。

## 9.5 全流程审计管理

医疗机构可信数据空间应建立覆盖数据全生命周期的审计管理机制，实现数据流通全过程可记录、可追溯、可核查和可问责。

审计范围应覆盖数据采集、汇聚、治理、存储、授权、访问、传输、共享、开发利用和销毁等活动。审计内容应包括操作主体、操作时间、操作行为、数据对象、授权依据和处理结果等信息。

审计记录应真实、完整、不可篡改，并按照规定期限保存。医疗机构应建立审计分析和异常预警机制，及时发现违规行为和安全风险，并采取相应处置措施。

对于涉及重要数据、敏感个人信息和跨机构流通的数据活动，应实施重点审计和专项监督。

## 9.6 数据确权与存证

医疗机构可信数据空间应建立数据确权与存证机制，保障数据来源真实、权属清晰、责任明确和过程可信。

数据确权应结合数据来源、数据贡献、授权关系和管理责任等因素，明确各参与主体在数据持有、管理、使用和运营过程中的权利与义务。数据确权活动应符合国家有关法律法规和政策要求。

数据存证应采用电子签名、时间戳、区块链存证或其他可信技术手段，对数据产生、授权、流通、使用和交易等关键活动进行记录和固化，形成可验证、不可篡改的证据链。

存证信息应支持查询验证、责任追溯和争议处理，为数据流通活动提供可信保障和法律依据。

## 10 数据流通利用建设

医疗机构可信数据空间应围绕医疗健康数据资源流通利用需求，建立覆盖数据共享交换、数据产品开发、数据服务供给、数据开放应用、数据交易流通和价值实现全过程的数据流通利用体系。在保障数据安全、个人信息保护和合法合规的前提下，促进医疗健康数据资源高效配置和价值释放，推动数据要素赋能医疗服务、科研创新、公共卫生治理和健康产业发展。

### 10.1 数据共享交换

医疗机构可信数据空间应建立统一规范的数据共享交换机制，实现医疗健康数据资源跨系统、跨机构、跨区域安全有序流通。

数据共享交换应遵循依法合规、授权使用、安全可控和最小必要原则，根据数据分类分级结果和授权规则实施差异化管理。共享交换过程应明确数据提供方、数据使用方和管理责任主体，确保共享范围、共享方式和使用目的清晰明确。

数据共享交换应支持目录发现、在线调用、批量交换、协同计算等多种模式，并实现全过程记录和可追溯管理。对于涉及个人信息、敏感数据和重要数据的共享交换活动，应开展风险评估并采取必要的安全保护措施。

### 10.2 数据产品管理

医疗机构可信数据空间应建立数据产品管理机制，对数据资源加工形成的数据产品实施全生命周期管理。

数据产品应以合法获取的数据资源为基础，通过数据治理、数据分析、知识加工、模型训练等方式形成能够满足特定业务需求的产品成果。数据产品形式可包括数据集、专题数据库、指标库、知识图谱、算法模型、分析报告和应用组件等。

医疗机构应建立数据产品设计、开发、测试、发布、运营和退出管理机制，明确产品责任主体、服务对象和应用范围。数据产品上线前应完成安全审查、质量评估和合规审核，确保产品质量和应用安全。

### 10.3 数据服务管理

医疗机构可信数据空间应建立统一的数据服务管理体系，为数据资源流通利用提供标准化、规范化和服务化支撑。

数据服务应围绕数据资源发现、共享交换、分析处理、模型训练和应用开发等需求开展，形成覆盖数据全生命周期的服务能力。服务内容可包括数据查询服务、数据检索服务、数据接口服务、数据分析服务、模型服务、知识服务和运营服务等。

医疗机构应建立服务目录管理、服务注册发布、服务质量监测和服务评价机制，持续提升数据服务能力和服务质量。数据服务调用过程应纳入统一监管和审计范围，实现服务行为可记录、可追溯和可评价。

## 10.4 数据开发利用

医疗机构可信数据空间应支持医疗健康数据资源的规范开发和创新利用，促进数据资源向知识成果和应用价值转化。

数据开发利用应在授权范围内开展，围绕临床诊疗、医学科研、医院管理、公共卫生、药械研发和人工智能等领域需求，推动数据资源深度融合应用。开发利用活动应采用标准化工具和技术平台，提高数据开发效率和利用水平。

医疗机构应建立数据开发利用管理机制，对开发过程中的数据使用、模型训练、成果输出和安全管理进行规范管理，确保开发利用活动合法合规、安全可控。

## 10.5 数据开放应用

医疗机构可信数据空间应按照国家有关法律法规和政策要求，稳步推进医疗健康数据开放应用。

数据开放应坚持安全优先、分类管理和风险可控原则，根据数据属性、开放条件和应用需求确定开放范围和开放方式。开放数据应经过脱敏处理、风险评估和合规审查，防止个人隐私泄露和数据安全风险。

医疗机构应建立开放数据目录和开放服务机制，为科研机构、社会组织、企业和公众提供依法合规的数据开放服务，促进医疗健康数据创新应用和社会价值创造。

## 10.6 数据交易流通

医疗机构可信数据空间应支持依法合规的数据流通活动，为数据资源价值转化提供支撑。

数据交易流通应遵循国家有关数据流通交易管理要求，坚持合法合规、公开透明、安全可信和权责明确原则。数据流通活动应明确数据来源、授权关系、使用范围、安全责任和收益分配机制。

在开展数据流通活动过程中，应通过可信身份认证、授权管理、访问控制、隐私计算和全过程审计等措施保障交易安全和数据权益。涉及重要数据、个人信息和敏感医疗健康数据的流通活动，应严格执行相关法律法规和监管要求。

## 10.7 数据价值实现

医疗机构可信数据空间应建立数据价值实现机制，推动医疗健康数据资源向数据产品、数据服务和创新应用成果转化。

数据价值实现应充分发挥医疗健康数据在提升医疗服务质量、优化医院运营管理、促进医学科研创新、支撑公共卫生治理和培育数字健康产业等方面的作用。通过数据资源开发利用、数据产品运营、数据服务供给和生态协同创新，实现数据资源价值持续释放。



医疗机构应建立数据价值评估和运营管理机制，探索符合医疗健康行业特点的数据价值实现模式，促进数据资源、技术能力和应用场景协同发展，推动形成多方参与、合作共赢的数据要素生态体系。

## 11 安全保障建设

医疗机构可信数据空间应建立覆盖组织管理、技术防护、运行监测和应急处置全过程的安全保障体系，坚持“安全与发展并重、保护与利用并举”的原则，统筹网络安全、数据安全和个人信息保护工作，确保医疗健康数据在采集、存储、传输、共享、开发利用和流通过程中的机密性、完整性、可用性和可追溯性。

安全保障建设应符合国家网络安全、数据安全、个人信息保护及医疗健康行业相关法律法规和标准规范要求，构建制度完善、责任明确、技术先进、运行可靠的安全管理体系。

### 11.1 安全管理体系

医疗机构应建立与可信数据空间建设相适应的安全管理体系，明确安全管理目标、组织架构、职责分工和管理流程，形成覆盖数据全生命周期的安全治理机制。

安全管理体系应包括安全组织管理、安全制度管理、安全风险管管理、安全运维管理、安全监督检查和持续改进等内容。医疗机构应明确主要负责人、安全管理部门、业务部门和技术部门的职责，建立协同联动的安全管理体系。

医疗机构应定期开展安全评估、安全审计和风险排查工作，持续提升可信数据空间安全管理能力和风险防控水平。

### 11.2 数据安全保护

医疗机构应建立数据分类分级保护机制，根据数据的重要程度、敏感程度和风险等级实施差异化安全管理措施。

数据安全保护应覆盖数据采集、汇聚、存储、处理、传输、共享、开放、流通和销毁全过程。对于重要数据、核心业务数据以及敏感医疗健康数据，应采取访问控制、加密保护、脱敏处理、水印标识、备份恢复和安全审计等措施进行重点保护。

医疗机构应建立数据安全责任机制，明确数据管理责任主体和使用责任主体，确保数据资源安全可控。数据流通利用活动应遵循授权管理要求，防止数据泄露、篡改、丢失和非法使用。

### 11.3 个人信息保护

医疗机构应按照个人信息保护相关法律法规要求，建立个人信息保护管理制度和技术保障机制。

个人信息处理活动应遵循合法、正当、必要和诚信原则，明确处理目的、处理方式和处理范围，并采取最小必要原则开展数据处理活动。涉及患者个人信息和敏感个人信息的数据流通活动，应依法取得授权或者符合相关法律法规规定。

医疗机构应建立个人信息风险评估、影响评估和监督检查机制，采取匿名化、去标识化、访问控制和加密保护等措施降低个人信息泄露风险。

在开展科研合作、数据共享和数据开发利用过程中，应确保个人信息主体合法权益得到有效保护。

### 11.4 隐私计算能力

医疗机构可信数据空间应建设隐私计算能力体系，在保障数据不出域、隐私不泄露和权属不转移的前提下，实现跨机构数据协同分析和价值挖掘。

隐私计算能力应根据应用场景和数据安全要求，综合采用联邦学习、安全多方计算、可信执行环境等技术，实现数据“可用不可见”和“数据不动价值流动”。

#### 11.4.1 联邦学习

医疗机构可信数据空间宜采用联邦学习技术支持跨机构协同建模和联合分析。

联邦学习应在原始数据不离开本地环境的情况下，通过模型参数交换和聚合实现联合训练。参与各方仅共享模型参数或中间结果，不直接共享原始数据。

联邦学习应用应建立模型管理、安全验证和效果评估机制，防止模型反演、参数泄露和数据推断等安全风险。

#### 11.4.2 安全多方计算

医疗机构可信数据空间宜采用安全多方计算技术支持多主体联合计算场景。

安全多方计算应在各参与方数据保持本地存储和独立控制的前提下，实现联合统计分析、联合查询和联合建模等功能，确保计算过程中无法获取其他参与方原始数据。

安全多方计算系统应具备参与方身份认证、计算过程验证、结果审计和异常监测能力，保障计算过程安全可信。

#### 11.4.3 可信执行环境

医疗机构可信数据空间宜建设可信执行环境，为敏感数据处理和联合计算提供可信运行环境。

可信执行环境应利用硬件隔离和可信计算技术，对计算过程和运行空间进行保护，防止数据在处理过程中被非法访问、窃取或篡改。

在涉及重要数据处理、模型训练和跨机构联合分析场景时，可采用可信执行环境增强数据保护能力和计算可信度。

### 11.5 密钥管理

医疗机构应建立统一的密钥管理体系，对数据加密、身份认证、数字签名和安全通信过程中使用的密钥进行全过程管理。

密钥管理应覆盖密钥生成、分发、存储、使用、更新、备份、恢复和销毁等环节，并建立严格的权限控制和审计机制。涉及重要数据和敏感信息的加密保护活动，应采用符合国家密码管理要求的密码技术和产品。

医疗机构应建立密钥生命周期管理制度，确保密钥安全、有效和可追溯。

### 11.6 安全监测与预警

医疗机构应建立安全监测与预警体系，对可信数据空间运行状态、数据访问行为和安全事件进行实时监测和分析。

安全监测范围应覆盖网络环境、系统平台、数据资源、用户行为和服务运行等关键环节。通过日志分析、行为分析、风险识别和异常检测等技术手段，及时发现潜在安全威胁和违规行为。

医疗机构应建立风险预警机制，对发现的异常情况进行分级预警和快速处置，并形成风险闭环管理体系。

### 11.7 应急响应管理



医疗机构应建立安全事件应急响应机制，提升可信数据空间突发安全事件处置能力。

应急响应管理应覆盖安全事件发现、报告、分析、处置、恢复和总结全过程，明确组织职责、响应流程和处置要求。针对数据泄露、系统入侵、恶意攻击、服务中断和隐私泄露等风险场景，应制定专项应急预案并定期组织演练。

发生安全事件时，应及时采取控制措施，降低影响范围，保护数据安全和业务连续性。事件处置完成后，应开展原因分析、责任认定和整改优化工作，持续提升安全保障能力和风险防范水平。

## 12 运营管理

医疗机构可信数据空间应建立规范化、体系化的运营管理机制，实现对数据空间运行全过程的组织协调、制度保障、服务支撑、生态协同、合规管理和风险控制，确保数据空间长期稳定、安全高效运行。

### 12.1 组织管理

医疗机构应建立与可信数据空间相适应的组织管理体系，明确数据空间运营管理的组织架构和职责分工。应设立专门的运营管理机构或岗位，负责数据空间的统一规划、统筹协调和日常管理。

组织管理体系应覆盖数据提供方、数据使用方、数据服务方及相关技术支持单位，形成多方参与、协同推进的管理机制。医疗机构应明确主要负责人及各部门职责，建立跨部门协同工作机制，保障数据空间建设与运营的持续推进。

### 12.2 制度管理

医疗机构应建立完善的数据空间运营管理制度体系，覆盖数据资源管理、数据流通管理、数据安全管

理、数据授权管理、服务管理及应急管理等方面。

制度体系应明确各类数据活动的管理要求、操作流程、审批机制和责任边界，确保数据空间运行有章可循、有据可依。制度应根据法律法规、标准规范及实际运行情况动态优化和更新。

### 12.3 服务管理

医疗机构应建立统一的数据空间服务管理机制，对数据资源、数据产品及数据服务进行标准化管理。

服务管理应包括服务目录管理、服务发布管理、服务调用管理、服务质量监测及服务评价机制，确保数据服务可发现、可调用、可监控和可评价。应持续优化服务能力，提升数据服务效率和用户体验。

### 12.4 生态管理

医疗机构应构建开放协同的数据生态体系，促进医疗机构、科研院所、企业及第三方服务机构等多主体协同参与。

生态管理应围绕数据资源共享、数据产品开发、技术能力协同及应用场景拓展开展，推动形成共建共治共享的数据空间生态体系。应建立生态伙伴准入机制、协同机制及退出机制，保障生态体系健康有序发展。

## 12.5 合规管理

医疗机构应建立覆盖数据空间全流程的合规管理体系，确保数据活动符合国家法律法规及行业监管要求。

合规管理应包括数据采集合规、数据使用合规、数据共享合规、数据流通合规及数据开放合规等内容。应建立合规审查机制、合规评估机制及合规整改机制，对数据活动进行全过程监督与管理。

对于涉及个人信息、重要数据及跨机构数据流通的活动，应开展专项合规审查，确保合法合规开展数据处理活动。

## 12.6 风险管理

医疗机构应建立数据空间风险管理体系，对数据安全风险、运营风险、合规风险及技术风险进行系统识别、评估与控制。

风险管理应覆盖风险识别、风险评估、风险预警、风险处置及持续改进全过程。应建立风险分级分类管理机制，对高风险事项实施重点监控与专项治理。

医疗机构应定期开展风险评估与安全检查，及时发现潜在风险隐患并采取有效措施加以控制，确保数据空间安全稳定运行。

## 13 运行维护

医疗机构可信数据空间应建立标准化、规范化的运行维护体系，保障系统持续稳定运行、性能可控及安全可靠，实现数据空间长期健康运营。

### 13.1 运维管理

医疗机构应建立统一的运维管理体系，对可信数据空间基础设施、平台系统、数据资源及应用服务进行统一监控与管理。

运维管理应包括日常运维、巡检维护、版本管理、容量管理及应急响应等内容，确保系统持续稳定运行。应建立运维责任体系和操作规范，提升运维效率与管理水平。

### 13.2 配置管理

医疗机构应建立配置管理机制，对数据空间涉及的系统配置、服务配置、网络配置及安全配置进行统一管理。

配置管理应确保配置项可识别、可追溯、可控制，并支持配置变更的审批、记录与回滚。应建立配置基线管理机制，防止未经授权的配置变更影响系统安全与稳定。

### 13.3 日志管理

医疗机构应建立统一的日志管理体系，对数据空间运行过程中的操作日志、访问日志、安全日志及审计日志进行集中管理。

日志管理应确保日志记录完整、准确、不可篡改，并支持日志查询、分析与追溯。应建立日志留存机制，满足监管合规与安全审计要求。

## 13.4 性能监测

医疗机构应建立性能监测机制，对数据空间系统性能、服务性能及资源使用情况进行实时监测与分析。

性能监测内容应包括系统响应时间、吞吐量、资源利用率及服务可用性等指标。应建立性能预警机制，及时发现性能瓶颈并进行优化调整，保障系统高效稳定运行。

## 13.5 故障处理

医疗机构应建立完善的故障处理机制，对系统故障、服务异常及安全事件进行快速响应与处置。

故障处理应包括故障发现、故障定位、故障隔离、故障修复及恢复验证等环节。应建立分级响应机制，确保关键故障能够及时处理，最大限度减少业务影响。

## 13.6 持续改进

医疗机构应建立持续改进机制，通过运行数据分析、用户反馈、审计结果及评估结果不断优化数据空间建设与运营能力。

持续改进应覆盖技术优化、流程优化、管理优化及服务优化等方面，推动数据空间能力持续提升。应形成闭环管理机制，实现发现问题、分析问题、解决问题和验证效果的持续迭代改进过程。

## 参考文献

- [1] GB/T 39725-2020 信息安全技术 医疗数据安全指南
- [2] GB/T 42490-2023 信息安全技术 网络安全等级保护基本要求
- [3] TC609-6-2025-01 可信数据空间 技术架构
- [4] 《数据安全法》（中华人民共和国主席令第 84 号）
- [5] 《个人信息保护法》（中华人民共和国主席令第 103 号）
- [6] 《医疗机构数据安全管理办法》（国卫办医函〔2023〕28 号）
- [7] 可信数据空间发展行动计划（2024-2028 年）（国数资源〔2024〕119 号）
- [8] 国家数据基础设施建设指引（发改数据〔2024〕1853 号）

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

广东省卫生经济学会医疗标准分会版权所有

学会医疗标准分会版权所有