|  |  |
| --- | --- |
| ICS  | 35.220.01 |
| CCS  |

|  |
| --- |
| D:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T.pngD:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T后面的反斜杠.png XZBX |

L 78 |

西安市质量与标准化协会团体标准

T/XZBX 0106—2025

影像临床数据与护理数据融合的大数据

智能存储与管理规程

Code of practice for big data intelligent storage and management of clinical imaging data and nursing data integration

2025 - 09 - XX发布

2025 - 09 - XX实施

西安市质量与标准化协会  发布

目次

[前言 III](#_Toc207825459)

[引言 V](#_Toc207825460)

[1 范围 1](#_Toc207825461)

[2 规范性引用文件 1](#_Toc207825462)

[3 术语和定义 1](#_Toc207825463)

[4 数据存储与管理架构 3](#_Toc207825464)

[5 数据处理与分析 5](#_Toc207825465)

[6 数据安全与隐私保护 7](#_Toc207825466)

[7 数据共享与互操作性 9](#_Toc207825467)

1. 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。

本文件由西安市质量与标准化协会提出并归口。

本文件起草单位：九江市第一人民医院。

本文件主要起草人：胡俊松。

1. 引言

随着信息技术的迅速发展和医疗健康行业的数字化转型，医疗数据的种类和数量呈爆炸性增长，尤其是在影像数据和护理数据的生成和管理方面。影像数据，如CT、MRI、X光片等，成为临床诊断和治疗中不可或缺的部分，而护理数据则涵盖了患者的护理记录、病情变化、护理方案等重要信息。这两类数据的融合对于全面了解患者的健康状况、提供个性化治疗和提高医疗服务质量具有重要意义。

然而，影像数据和护理数据的管理面临着一系列挑战。影像数据通常具有大容量、高复杂性和高更新频率等特点，而护理数据则分散在多个系统和平台中，数据格式、存储要求和处理方式差异较大。因此，如何有效地融合这两类数据，并通过大数据技术实现智能存储、管理和分析，已成为现代医疗领域的亟待解决的问题。

本文件旨在为医疗机构提供一套完整的影像临床数据与护理数据融合的大数据智能存储与管理方案。通过建立数据融合架构、智能化存储系统和高效管理机制，本文件帮助医疗机构提升数据管理效率、实现数据共享与互通，并为临床决策支持系统的建设奠定基础。此外，本文件还特别强调数据安全和隐私保护，确保医疗数据的安全性和合规性。

本文件适用于各类医疗机构，尤其是大型医院、综合性医疗服务平台及相关医疗数据处理单位。其内容涵盖数据存储架构、数据融合处理流程、智能化管理技术、数据安全与隐私保护等方面，为医疗机构提供智能化、大规模的数据管理和分析支持，促进医疗服务的精准化、个性化发展。

影像临床数据与护理数据融合的大数据

智能存储与管理规程

* 1. 范围

本文件规定了影像临床数据与护理数据融合的大数据的数据存储与管理架构、数据处理与分析、数据安全与隐私保护以及数据共享与互操作性等内容。

本文件适用于医疗机构内的各类数据管理平台，包括但不限于医院信息系统（HIS）、影像存储与传输系统（PACS）、电子病历系统（EMR）及护理信息系统等。通过本文件的实施，旨在为医疗机构提供高效的数据融合与智能化存储管理方案，促进数据互联互通与资源共享，提升临床治疗效果和护理服务质量。

本文件不适用于非医疗领域的影像数据管理与大数据应用，也不包括医疗设备或数据采集终端的具体技术要求。其内容主要聚焦于数据的存储、处理与智能管理。

* 1. 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 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

GB/T 31916.1—2015 信息技术 云数据存储和管理 第1部分：总则

GB/T 39725—2020 信息安全技术 健康医疗数据安全指南

GB/T 42204—2022 临床医疗设备通信规范 影像设备

GB/T 43431—2023 信息技术 云数据存储和管理 基于对象的云存储应用接口测试方法

GB/T 44792—2024 健康管理 远程医疗平台信息接入与数据交换

* 1. 术语和定义

下列术语和定义适用于本文件。

影像数据 imaging data

指通过医学影像设备（如X光、CT、MRI等）获取的患者身体内部或外部的图像数据，通常包括二维和三维图像。影像数据用于诊断、治疗规划及患者健康监测。

护理数据 nursing data

指与患者护理过程相关的各种信息，包括但不限于护理记录、病情变化、治疗方案、药物管理、生命体征监测数据等。这些数据反映了护理人员对患者的照料过程及其健康状况。

数据融合 data fusion

指将来自不同来源、不同格式的影像数据与护理数据进行集成、处理和分析，以便为临床决策提供全面的支持。数据融合过程中，需要解决数据格式差异、数据缺失、数据冗余等问题。

大数据存储 big data storage

指通过分布式存储架构、云计算技术等手段，将海量的医疗数据（如影像数据、护理数据）存储于数据仓库、数据库等存储平台，以便快速、安全地访问、查询和处理。

智能存储系统 intelligent storage system

指基于人工智能（AI）、机器学习、自动化管理等技术的存储系统，能够根据数据的访问频率、重要性等自动优化存储策略，提高数据的处理效率和安全性。

数据管理平台 data management platform

指用于统一管理、监控和分析影像数据、护理数据及其他临床数据的系统平台。数据管理平台实现数据存储、数据共享、数据安全等功能，为医疗机构提供全方位的数据支持。

数据安全与隐私保护 data security and privacy protection

指在数据存储、传输、访问和处理过程中，采取一系列技术和管理措施，确保患者隐私信息和敏感数据的安全性，防止数据泄露、篡改或丢失，确保符合相关法规要求。

医疗数据交换标准 healthcare data exchange standards

指医疗数据在不同医疗系统或机构之间传输、共享时，所采用的统一数据格式、协议和规范。常见的标准包括HL7、DICOM等，用于确保数据在不同系统间的互操作性。

电子病历 electronic medical record; EMR

指记录患者诊疗过程中的所有医疗信息的数字化系统，涵盖患者的病史、治疗过程、检验结果、药物使用等。电子病历系统能够高效管理患者信息，支持临床决策、患者管理等。

影像存储与传输系统 picture archiving and communication system; PACS

指用于医学影像数据的存储、管理和传输的系统。PACS允许影像数据在医院内各部门之间快速共享和传输，优化影像数据的管理流程，支持医生和护理人员进行快速、精准的临床决策。

* 1. 数据存储与管理架构
		1. 数据存储架构设计

数据存储架构是实现影像数据与护理数据融合的重要基础。为确保数据存储的高效性、可靠性和安全性，必须设计科学的存储架构。建议采用分布式存储架构、云存储和本地存储相结合的方式，构建灵活可扩展的存储体系。存储架构应具备以下特性：

1. 高可用性：通过多节点冗余、故障转移机制等手段，确保存储系统具备高可用性，避免因硬件故障或系统崩溃导致数据丢失或服务中断；
2. 高性能：采用高速存储设备，如固态硬盘（SSD）和大容量硬盘阵列（RAID），以提高数据读写效率，满足影像数据的快速访问需求；
3. 可扩展性：存储架构应具备可扩展性，能够根据数据量的增长，灵活扩展存储容量和计算资源，支持大数据时代医疗数据的快速增长；
4. 数据备份与恢复：应定期对影像数据与护理数据进行备份，并设计合理的数据恢复机制，确保在数据丢失或损坏时能够快速恢复，确保数据安全。
	* 1. 数据管理平台架构

数据管理平台是实现数据存储、访问、管理和分析的核心工具。平台架构应满足以下要求：

1. 多层次架构：数据管理平台应采用多层次的架构，包括数据采集层、数据存储层、数据处理层、数据应用层等。每一层都有明确的功能和任务，确保数据流动的高效性和安全性；
2. 数据集成与融合：平台应能够实现影像数据与护理数据的高效集成与融合，支持不同格式、不同来源的数据进行统一处理和存储。数据集成时，应遵循标准化协议，如HL7、DICOM等，确保数据的互操作性；
3. 智能化管理与分析：平台应采用人工智能（AI）、机器学习等技术，实现对数据的智能管理与分析。通过对数据的自动化分类、标注、归档和处理，提高数据管理的效率和准确性；
4. 数据共享与协作：平台应具备良好的数据共享功能，支持医疗机构内部不同部门之间的数据共享与协作。平台可提供安全的数据接口，支持与其他医疗系统（如医院信息系统HIS、电子病历系统EMR等）进行数据交换与集成。
	* 1. 数据存储与传输协议

为了确保数据在存储和传输过程中的安全性与高效性，应制定统一的数据存储与传输协议。常见的协议包括：

1. DICOM（数字影像和通信医学标准）：DICOM协议用于医学影像数据的存储与传输，确保影像数据在不同设备和系统之间的互通性和无损传输。影像数据存储系统（PACS）应遵循DICOM标准，实现影像数据的统一管理；
2. HL7（健康水平7标准）：HL7协议主要用于医疗信息的交换和共享，特别适用于护理数据、病历数据等信息的传输。HL7协议应在数据传输和集成过程中得到广泛应用；
3. IHE（集成医疗环境）：IHE标准通过制定数据交换的具体规范和技术要求，确保医疗信息系统在不同平台之间能够实现无缝集成和共享。IHE协议在大数据平台中起着数据标准化和集成化的关键作用；
4. RESTful API：RESTful API是现代数据存储和传输中广泛应用的技术，通过HTTP协议进行数据传输，能够实现快速、低延迟的数据访问和共享。数据管理平台应提供RESTful API接口，以支持与其他医疗系统和外部应用进行数据交互。
	* 1. 数据存储与访问控制

数据的安全性和隐私保护是核心要求之一。必须采用严格的数据存储与访问控制措施，以保障患者隐私和医疗数据的安全性。主要控制措施包括：

1. 数据加密存储：所有敏感数据（如患者身份、病历信息等）应进行加密存储。采用高强度加密算法（如AES-256），确保数据在存储过程中不被非法访问；
2. 访问权限控制：应设定严格的数据访问权限，根据用户角色和职能不同，分配相应的访问权限。只有授权人员才能访问、查看或操作相关数据。可以通过基于角色的访问控制（RBAC）机制来实现；
3. 审计与日志记录：所有数据访问行为应进行记录，并生成详细的审计日志。定期检查访问日志，及时发现并处理潜在的安全风险。审计记录应保留一定期限，以备后续检查；
4. 多因素身份认证：对于访问敏感数据的用户，尤其是医疗数据管理人员，要求实施多因素身份认证（MFA），例如结合密码、短信验证码、指纹等认证方式，确保身份的真实性和安全性。
	* 1. 数据备份与恢复策略

数据备份和恢复是保障数据长期可用性和安全性的关键环节。为确保系统的高可用性，应采取如下措施：

1. 定期数据备份：应根据数据的重要性和访问频率，制定定期备份策略。数据备份应涵盖影像数据、护理数据和系统配置等所有关键信息，备份数据应存储在异地或云平台中；
2. 灾难恢复计划：制定详细的灾难恢复计划，确保在系统故障或数据丢失时能够及时恢复数据。恢复过程应包括数据备份的检查、恢复操作的流程、恢复测试等内容，确保数据能够在最短时间内恢复到正常状态；
3. 冗余存储：采用冗余存储技术，如RAID、分布式存储等，确保数据在硬件故障或系统故障时不丢失。数据存储系统应具备自动故障转移和负载均衡的能力。
	1. 数据处理与分析
		1. 数据预处理
			1. 数据清洗

影像数据和护理数据通常包含噪声、缺失值、重复数据等问题。通过数据清洗技术，去除无效信息、填补缺失数据、删除重复记录，确保数据的准确性和完整性。特别是护理数据中可能存在的重复记录或错误标记，需要进行合理的校验和修正。

* + - 1. 数据标准化与格式化

在数据融合过程中，影像数据和护理数据往往来自不同的系统和设备，数据格式和单位差异较大。通过数据标准化技术，统一数据格式、单位和标准，使得不同来源的数据能够互通并进行有效分析。例如，将影像数据的分辨率和护理数据的时间戳进行统一，以便后续处理和分析。

* + - 1. 数据去噪与降维

对于影像数据，去噪处理是确保图像质量和提高诊断准确性的关键。使用图像处理技术（如滤波算法）去除图像中的噪点。对于护理数据中的高维特征，可以使用降维技术（如主成分分析PCA）减少数据的复杂性，提高计算效率。

* + 1. 数据融合与集成
			1. 多模态数据融合

影像数据与护理数据属于多模态数据，分别提供了不同的患者信息。影像数据能够提供患者的生理结构信息，而护理数据则反映了患者的护理过程、生命体征等动态信息。通过多模态数据融合技术，将这两类数据结合，形成一个更加完整的患者健康档案。

* + - 1. 数据同步与关联分析

在数据融合过程中，影像数据和护理数据通常是在不同时间点采集的。必须确保数据在时间上的同步，能够准确地对应患者的治疗、护理和影像检查历史。例如，将影像数据和护理数据中的时间戳进行匹配，使得医生能够清晰地了解患者的治疗过程与影像检查结果的关联。

* + - 1. 数据融合模型设计

采用机器学习和深度学习等技术，设计融合模型，对影像数据和护理数据进行联合建模，挖掘数据之间的潜在关系。例如，通过深度神经网络（DNN）对影像数据进行特征提取，同时结合护理数据中的生命体征信息，进行综合评估和预测患者的病情发展。

* + 1. 数据分析与智能化处理
			1. 数据挖掘与模式识别

在大量的影像数据和护理数据中，存在潜在的关联关系和模式。通过数据挖掘技术（如关联规则挖掘、聚类分析等），识别不同数据特征之间的关系。例如，分析患者的影像数据与其护理记录之间的关联，以预测疾病的进展或治疗效果。

* + - 1. 预测分析

利用护理数据中的历史信息（如病程记录、生命体征等）和影像数据的变化趋势，构建预测模型，预测患者病情的发展或治疗后的恢复情况。常用的技术包括回归分析、时间序列分析、机器学习等。

* + - 1. 临床决策支持

通过对影像数据和护理数据的综合分析，构建临床决策支持系统（CDSS），为医生提供实时的决策建议。例如，结合患者的影像结果和护理记录，自动识别出患者的风险点，并给出个性化的治疗建议。

* + 1. 人工智能与深度学习应用
			1. 影像数据的深度学习分析

深度学习技术，特别是卷积神经网络（CNN），能够自动从影像数据中提取有用的特征，识别影像中的病变区域。通过训练深度学习模型，能够实现影像的自动诊断和标注，为医生提供辅助诊断支持。

* + - 1. 护理数据的智能分析

对于护理数据，可以使用自然语言处理（NLP）技术对病历记录进行分析，提取患者的健康状态、护理需求等信息。通过机器学习算法分析护理数据中的模式，预测患者可能的病情变化或治疗反应，提供智能决策支持。

* + - 1. AI融合模型的开发

结合影像数据和护理数据，构建AI融合模型。深度学习模型可用于影像分析，而机器学习和其他数据挖掘技术可以应用于护理数据的分析。通过将这两类数据的分析结果结合，构建更为精确的患者健康评估系统。

* + 1. 数据可视化
			1. 影像数据可视化

对影像数据的可视化通常涉及图像的处理和增强，例如利用三维重建技术对CT、MRI等影像数据进行立体展示，帮助医生更好地进行诊断与分析。

* + - 1. 护理数据可视化

护理数据可视化将患者的生命体征、病历记录等数据转化为图表、趋势线等形式，提供实时健康监控，帮助护理人员识别潜在问题。通过仪表盘的方式，将多个患者的关键指标集中展示，便于护理人员进行日常监控和及时响应。

* 1. 数据安全与隐私保护
		1. 数据安全管理
			1. 数据加密存储

所有影像数据和护理数据在存储过程中必须进行加密处理。常用的加密算法包括AES-256（高级加密标准），以确保数据即使在存储介质被非法访问时，也无法被破解和使用。

* + - 1. 数据加密传输

在数据传输过程中，应使用加密协议（如TLS/SSL）保障数据的机密性和完整性。特别是在影像数据和护理数据在医疗系统之间传输时，必须确保数据在传输过程中的安全，防止数据被拦截或篡改。

* + - 1. 访问控制

数据的访问权限应根据不同的角色和职责进行细致划分，实施最小权限原则。仅授权的用户才能访问敏感数据。所有访问行为应被记录并进行审计，确保数据访问的可追溯性。

* + 1. 身份认证与访问控制
			1. 多因素身份认证（MFA）

对于所有涉及影像数据和护理数据的访问，特别是对于敏感信息的访问，应采用多因素身份认证。除密码外，采用短信验证码、指纹识别、面部识别等二次认证方式，以增强数据访问的安全性。

* + - 1. 角色访问控制（RBAC）

数据访问权限应根据用户的角色进行控制，确保不同角色的人员只能访问与其工作职责相关的数据。例如，临床医生可以访问患者的影像数据和相关护理记录，但无法查看系统的管理日志或其他非相关数据。

* + - 1. 定期审计与监控

应定期对数据访问进行审计，确保所有操作均符合规定，并及时发现异常访问行为。系统应能实时监控并记录所有用户的访问日志，若发生不正常访问时能够自动报警。

* + 1. 隐私保护
			1. 患者同意书

患者的隐私保护是医疗数据管理中的核心问题。影像数据和护理数据中包含了大量的个人健康信息，必须严格遵守相关隐私保护法律法规，确保患者的个人信息不被泄露或滥用。

在数据采集、存储和使用过程中，患者应明确知情并同意其数据的使用。医疗机构应在患者接受治疗或影像检查前，提供明确的隐私保护说明，并获得患者的书面同意。

* + - 1. 数据去标识化与匿名化

在进行数据分析、研究和共享时，尽量去标识化或匿名化患者的个人信息。去标识化处理可以去除患者的姓名、身份证号等信息，确保在数据分析和共享过程中不会泄露患者的身份信息。

* + - 1. 合法合规使用

医疗机构在收集、存储和使用患者数据时，必须遵循相关法律法规的要求。数据使用仅限于医疗服务、研究等合法目的，不得将数据用于未经患者同意的其他用途。

* + 1. 数据泄露与应急响应
			1. 数据泄露应急预案

在实际操作中，数据泄露或其他安全事件仍可能发生。因此，必须建立完善的应急响应机制，以便在发生数据泄露等安全事件时，能够迅速采取有效措施进行应对。

医疗机构应制定详尽的数据泄露应急预案，明确各部门的应急响应职责。应急预案应包括事件发现、确认、应对、调查、恢复等全过程的操作流程，确保在发生数据泄露事件时能够迅速响应，最大限度降低损失。

* + - 1. 事件报告与通报

一旦发现数据泄露或其他安全事件，相关人员应立即上报管理层，并在24小时内向患者、监管部门等通报。通报内容应包括事件发生的时间、泄露数据的类型、可能受到影响的人员及采取的补救措施。

* + - 1. 补救措施与责任追究

在数据泄露事件发生后，医疗机构应立即采取补救措施，如关闭受影响的系统、加密泄露的数据、加强访问控制等。同时，应进行内部调查，找出泄露原因，并根据调查结果对相关责任人进行追责。

* + 1. 数据安全与隐私保护的持续改进
			1. 安全技术更新

数据安全和隐私保护是一个持续的过程，随着技术的发展和新威胁的出现，安全措施和隐私保护策略也需要不断优化和改进。

随着网络安全技术的不断发展，医疗机构应定期评估现有的安全措施，更新和升级安全技术，如加强数据加密算法、引入新的身份验证技术等，以适应新的安全挑战。

* + - 1. 员工培训与意识提升

定期开展员工安全培训，提升医护人员和IT人员的数据安全意识。通过培训，使其了解数据保护的法律法规、安全操作流程及应急响应程序，避免人为操作失误导致的数据泄露或安全事件。

* + - 1. 定期安全审计与风险评估

定期进行安全审计，评估数据存储和传输过程中可能存在的安全漏洞，及时修补系统缺陷。通过定期的风险评估，确保数据安全措施能够应对新出现的安全威胁。

* 1. 数据共享与互操作性
		1. 数据共享的必要性

随着医疗信息化的发展，数据共享已经成为提高医疗服务质量、促进跨机构协作和提升整体医疗效率的重要手段。影像数据和护理数据作为患者健康信息的核心组成部分，其共享可以为多学科团队的协作、临床决策支持和个性化治疗提供重要依据。然而，数据共享也面临数据标准、数据隐私、安全等问题的挑战，因此，需要通过科学的管理措施和技术手段，保障数据共享的合规性和安全性。

影像数据和护理数据的共享能够促进不同医疗机构之间的协作，尤其是在患者转院、远程诊疗等场景中，医生能够基于完整的患者历史数据进行治疗决策，提升诊疗的准确性。

数据共享为医学研究提供了丰富的素材，通过对大规模数据的分析和挖掘，可以发现潜在的疾病规律，推动医学进步。此外，通过数据共享与互操作性，医疗机构能够参与全球医学数据联盟，推动医学大数据的研究与应用。

* + 1. 互操作性要求

互操作性指的是不同系统、平台或设备之间能够无缝交换和使用数据的能力。影像数据和护理数据的融合要求不同系统能够有效互联互通，保障数据在不同医疗信息系统之间的流动和使用。

为实现影像数据和护理数据的共享，必须采用国际或行业标准的数据格式，确保不同系统之间的数据交换不会因格式不兼容而产生问题。

数据共享系统需要提供统一的数据接口，支持不同系统之间的数据交换。使得医疗信息系统能够方便地与其他外部系统进行数据交互。

对于不同医疗信息系统之间的数据共享，可能存在数据格式或结构上的差异。因此，必须进行数据映射与转换，将不同系统的数据结构进行统一，以实现数据无缝流转。

* + 1. 数据共享模型
			1. 集中式共享模型

在集中式共享模型中，所有数据都存储在一个统一的数据库或云平台上，供所有授权用户访问。这种模型适用于需要高效管理、集中存储和快速访问的场景，但可能存在单点故障的风险。

* + - 1. 分布式共享模型

在分布式共享模型中，数据被分散存储在多个系统或节点中，数据的交换和访问通过互联互通的机制进行。这种模型适用于大型医疗机构或多机构协作的场景，能够提升数据冗余和系统容错能力。

* + - 1. 混合式共享模型

混合式共享模型结合了集中式和分布式模型的优点，能够根据不同类型的数据和不同业务场景的需求，灵活选择数据存储和共享方式。例如，影像数据采用集中存储，护理数据采用分布式存储。

* + 1. 数据共享的隐私与合规性保障
			1. 患者授权与同意

数据共享前，医疗机构必须获得患者的授权同意。患者应被明确告知其个人健康信息将如何被共享，并且只有在患者同意的情况下，数据才能进行共享。医疗机构应确保患者在充分知情的情况下签署同意书。

* + - 1. 数据去标识化

在进行数据共享和分析时，应对数据进行去标识化处理，确保患者的身份信息得到保护。去标识化处理包括去除姓名、身份证号、联系方式等个人识别信息，同时保留有助于分析的医疗数据。

* + - 1. 合规性审查

数据共享和交换的过程应遵循国家和地区的法律法规，确保数据共享过程中的隐私保护措施符合法律要求。医疗机构应定期进行合规性审查，确保数据共享活动不违反相关法律法规。

* + - 1. 数据访问监控与日志管理

在数据共享过程中，应对所有访问行为进行监控，记录详细的访问日志。日志内容包括访问时间、访问人员、访问数据类型等信息，确保数据的访问可追溯，并及时发现和阻止非法访问。

* + 1. 数据共享的技术支持
			1. 云计算平台

云计算提供了高效的数据存储和计算能力，能够支持大规模的影像数据和护理数据存储及分析。通过云平台，医疗机构可以方便地实现数据共享、访问控制和灾难恢复等功能。

* + - 1. 大数据分析技术

大数据分析技术能够帮助医疗机构从海量的影像数据和护理数据中提取有价值的信息，为临床决策提供支持。常见的技术包括机器学习、自然语言处理（NLP）、数据挖掘等。

* + - 1. 区块链技术

区块链技术在医疗数据管理中的应用逐渐增加，尤其在数据共享和隐私保护方面具有优势。通过区块链技术，可以确保数据在共享过程中的不可篡改性、透明性和安全性。

