|  |  |
| --- | --- |
| ICS | 11.120.99 |
| CCS | C25 |

|  |
| --- |
| 32 |

江苏省地方标准

DB XX/T XXXX—XXXX

基于区块链技术的多中心药物临床试验

管理系统开发指南

Multiregional drug clinical trials based on blockchain technology

guidelines for management system development

XXXX - XX - XX发布

XXXX - XX - XX实施

江苏省市场监督管理局  发布

目次

[前言 II](#_Toc150161635)

[引言 III](#_Toc150161636)

[1 范围 1](#_Toc150161637)

[2 规范性引用文件 1](#_Toc150161638)

[3 术语和定义 1](#_Toc150161639)

[4 缩略语 1](#_Toc150161640)

[5 总体技术要求 2](#_Toc150161641)

[6 系统架构要求 2](#_Toc150161642)

[7 临床试验模块功能要求 4](#_Toc150161643)

[8 数据上链规则 12](#_Toc150161644)

[9 数据加密要求 14](#_Toc150161645)

[10 系统安全要求 14](#_Toc150161646)

[参考文献 15](#_Toc150161647)

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。

本文件由江苏省药品监督管理局提出并归口。

本文件起草单位：江苏省药品监督管理局审核查验中心。

本文件主要起草人：徐厚明、胡晨希、马驰原、余洋、方萍、廖怡、刘春帅、田媛、陆丽珍、王欣欣、席晓宇。

1. 引言

在医药研发领域，申请人在申请药品上市注册前，应当完成药学、药理毒理学和药物临床试验等相关研究工作。临床试验是药物研发的重要环节，是确定药物疗效和安全性的重要手段。药物临床试验应当在符合相关规定的药物临床试验机构开展，并遵守药品管理法、药品注册管理办法、药物临床试验质量管理规范等相关要求。临床试验源数据获取、共享是当前临床试验过程的关键。目前我国药物临床试验数据管理还面临数据采集依靠人工转录，数据可靠性需要反复核对，监管部门和申办者较难对临床试验施行远程监管，临床试验源数据收集和共享存在壁垒等问题。同时，随着新版《药物临床试验质量管理规范》的实施，对临床试验的数据管理提出了新的挑战，如 “临床试验机构的信息化系统具备建立临床试验电子病历条件时，研究者应当首选使用，相应的计算机化系统应当具有完善的权限管理和稽查轨迹，可以追溯至记录的创建者或者修改者，保障所采集的源数据可以溯源”。

本文件拟基于区块链技术制定多中心药物临床试验管理系统开发指南，目的在于借助区块链技术的优势，实现多中心临床试验数据安全储存、可追溯、流程规范及监管便利。

基于区块链技术的多中心药物临床试验管理系统开发指南

* 1. 范围

本文件规定了多中心药物临床试验管理系统开发指南。

本文件适用于多中心药物临床试验管理系统的开发。单中心临床试验管理系统的开发、多中心医疗器械临床试验管理系统的开发可参照本指南。

* 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 37964-2019 信息安全技术 个人信息去标识化指南

GB/T 39725-2020 信息安全技术 健康医疗数据安全指南

GB/T 42570-2023 信息安全技术 区块链技术安全框架

GB/T 42571-2023 信息安全技术 区块链信息服务安全规范

* 1. 术语和定义

下列术语和定义适用于本文件。

多中心试验 Multiregional trial

按同一个试验方案，在一个以上试验单位实施，由多名以上研究者共同完成的临床试验。

稽查轨迹 Audit trail

从第一次的数据录入以及每一次的更改、删除或增加，都必须保留在临床试验数据库系统中。应包括更改的日期、时间、更改人、更改原因、更改前数据值、更改后数据值。

1. 稽查轨迹为系统保护，不允许任何人为的修改和编辑，稽查轨迹记录应存档并可查询。
   1. 缩略语

下列缩略语适用于本文件。

PoW：工作量证明机制（Proof of Work）

PoS：权益证明机制（Proof of Stake）

PKI：公钥基础设施(Public Key Infrastructure)

P2P：点对点技术（Peer to Peer）

AE：不良事件（Adverse Event）

SAE：严重不良事件(Serious Adverse Event）

SUSAR：可疑且非预期严重不良反应(Suspected Unexpected Serious Adverse Reaction)

AESI：特殊关注事件（Adverse Event of Special Interest）

DSUR：研发期间安全性更新报告（Development Safety Update Report）

ISF：智能安全金融服务（Intelligent Secure Finance）

IPFS：星际文件系统（Inter Planetary File System）

CID：内容标识符（Content Identifier）

* 1. 总体技术要求
     1. 系统

该系统是一种基于联盟链的临床试验数据存储和共享系统，应当具有完整的使用标准操作规程，应包括但不限于：

——系统设置/安装（包括对所使用的软件、硬件、物理环境及相互关联的描述）；

——系统操作手册；

——系统验证和功能测试；

——数据采集和处理（包括数据存储、稽查轨迹和风险评估）；

——系统维护（包括系统退役）；

——系统安全措施；

——变更控制；

——数据备份、恢复；

——系统的应急预案；

——备选记录方法（当系统不可用时）；

——用户培训、用户角色权限管理。

* + 1. 源数据

应当具有可归因性、易读性、同时性、原始性、准确性、完整性、一致性和持久性。

* + 1. 受试者信息

数据使用和受试者隐私保护应遵守《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》及《药物临床试验质量管理规范》的规定，在涉及到受试者的个人数据和健康医疗数据时，由数据上传方提前对受试者数据进行匿名化或去标识化处理，其过程应符合GB/T 37964-2019和GB/T 39725-2020的相关规定。

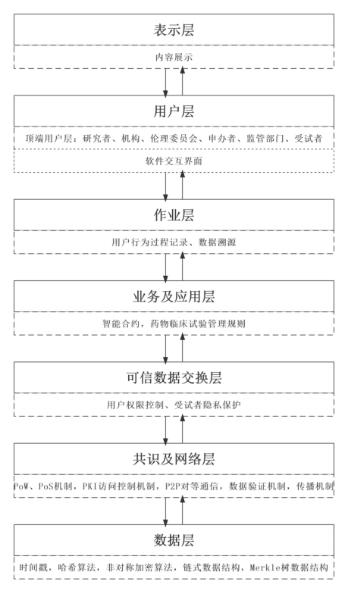
* + 1. 电子数据

电子数据的整合、内容和结构应当有明确规定，以确保电子数据的完整性；当系统出现变更时，如软件升级等，确保电子数据的一致性、完整性尤为重要。若数据处理过程中发生数据转换，确保转换后的数据与源数据语义保持一致和完整，和数据转化过程的可追溯性。

* 1. 系统架构要求

系统层次结构体系包含表示层、用户层、作业层、业务及应用层、可信数据交换层、共识及网络层、数据层等七个层次，分别对应不同的技术和实体组成，见图1。

1. 表示层：即对数据按照用户的需求进行展示，满足用户的使用需求。
2. 用户层：最顶端为用户层，是项目中各环节的实体个人和组织，用户包括研究者、机构、伦理委员会、申办者、监管部门、受试者等。
3. 作业层：指的是药物临床试验管理各环节中，操作人员的实际运作过程，它是溯源数据的源头。
4. 业务及应用层：该层涉及智能合约及药物临床试验管理规则等，其直接与实际业务挂钩，是业务逻辑与区块链系统运行的结合。
5. 可信数据交换层：指通过安全多方计算、智能合约、非对称加密等技术控制用户对数据的访问权限解决数据隐私安全和数据主导权等问题，包括用户权限控制、受试者隐私保护等。
6. 共识及网络层：包括POW、POS共识机制、PKI访问控制技术、P2P对等网通信技术，及数据验证机制和传播机制。区块链通过共识机制进行区块的生成和确认，通过P2P对等网技术实现节点之间的通信，通过外部添加的PKI技术实现访问权限管理。
7. 数据层：是区块链技术底层技术的集合。数据层主要包括哈希算法、Merkle树数据结构、链式数据结构、非对称加密算法、时间戳等。数据被打包记录入区块当中，实现数据的不可篡改化。



1. 基于区块链技术的多中心药物临床试验管理系统层次结构
   1. 临床试验模块功能要求
      1. 机构、研究者基本信息及项目管理模块
         1. 模块介绍

研究者和临床试验机构应当具有完成临床试验所需的必要条件。药物临床试验机构是按照《药物临床试验质量管理规范》（GCP）、《药物临床试验机构管理规定》和药物临床试验相关技术指导原则等要求，开展药物临床试验的机构。研究者，指实施临床试验并对临床试验质量及受试者权益和安全负责的试验现场的负责人。临床试验项目管理是根据GCP要求，在规定时限和预算范围内，有效利用各种资源，通过合理计划和执行，按照方案的规定完成符合质量要求的临床试验。

* + - 1. 模块主要内容

机构基本信息端口应包括但不限于：

1. 各中心临床试验管理部门基本信息；
2. 临床试验项目基本信息；
3. 临床试验备案网站备案信息；
4. 专业组备案信息；
5. 机构的执业证书；
6. 机构人员分工情况；
7. 研究团队人员信息；
8. 临床试验合同/协议签订及补充；
9. 研究经费管理；培训；
10. 样本检测实验室相应资质；
11. 实验室检测正常值范围；
12. 试验发起方的基本信息；
13. 申办者资质；
14. 临床试验批准告知书等。

研究者基本信息端口应包括但不限于：

1. 研究者备案信息；
2. 研究者执业信息，包括多点执业等；
3. 研究者简历；
4. 分工授权信息；
5. 培训；
6. 研究者GCP证书；
7. 研究者资格证等。

临床试验项目管理端口应包括但不限于：

1. 临床试验合同/协议签订及补充；
2. 研究经费管理；
3. 跟踪项目基本信息；
4. 项目进展；
5. 进行项目统计；
6. 按照日程提醒项目事务；
7. 研究团队及联系方式，包括已授权人、授权权限及授权有效期等。
   * + 1. 上链数据内容

应包括但不限于：

1. 各中心临床试验管理部门基本信息；
2. 临床试验项目基本信息；
3. 临床试验备案网站备案信息；
4. 机构的执业证书；
5. 研究团队人员信息；
6. 临床试验合同/协议签订及补充协议摘要；
7. 样本检测实验室相应资质摘要；
8. 实验室检测正常值范围、报价；
9. 研究者执业信息，包括多点执业等；
10. 研究者简历摘要；
11. 分工授权信息；
12. 研究者GCP证书等。
    * 1. 伦理委员会审核模块
         1. 模块介绍

伦理委员会，指由医学、药学及其他背景人员组成的委员会，其职责是通过独立地审查、同意、跟踪审查试验方案及相关文件、获得和记录受试者知情同意所用的方法和材料等，确保受试者的权益、安全受到保护。伦理委员会的职责是保护受试者的权益和安全，应当特别关注弱势受试者。伦理委员会通过独立地审查试验方案和试验方案修订版、知情同意书及其更新件、招募受试者的方式和信息、提供给受试者的其他书面资料；研究者手册；现有的安全性资料；包含受试者补偿信息的文件；研究者资格的证明文件；伦理委员会履行其职责所需要的其他文件。

* + - 1. 模块主要内容

资料上传端口应包括但不限于：

1. 试验方案及其修订版；
2. 知情同意书及其修订版；
3. 招募受试者的方式和信息；
4. 提供给受试者的其他书面资料；
5. 研究者手册；
6. 现有的安全性资料；
7. 包含受试者补偿信息的文件；
8. 研究者资格的证明文件；
9. 伦理委员会履行其职责所需要的其他文件；
10. 年度报告；
11. SAE/SUSAR/DSUR/AESI报告；
12. 偏离方案报告；
13. 研究完成报告；
14. 暂停或终止研究报告；
15. 人类遗传资源备案/审批信息等的上传；
16. 伦理委员会的委员组成；
17. 伦理委员会的委员伦理审查培训。

伦理委员会意见端口应包括但不限于：

1. 初始审查意见；
2. 跟踪审查意见；
3. 快速审查意见；
4. 备案资料接收确认等。
   * + 1. 上链数据内容

应包括但不限于：

1. 试验方案及其修订版；
2. 知情同意书及其修订版；
3. 招募受试者的方式和信息；
4. 研究者资格的证明文件摘要；
5. 伦理委员会的委员组成；
6. 伦理委员会的委员伦理审查培训等。
   * 1. 受试者信息管理模块
        1. 模块介绍

所有临床试验的纸质或电子资料应当被妥善地记录、处理和保存，能够准确地报告、解释和确认。应当保护受试者的隐私和其相关信息的保密性。

* + - 1. 模块主要内容

受试者信息端口应包括但不限于：

1. 受试者基本信息；
2. 监护人、法定代理人基本信息（如适用）；
3. 1年内参加过的临床试验；
4. 既往病史及记录，包括既往用药史及用药起止时间等；
5. 受试者补助及临床试验保险等保障信息等。

知情同意端口应包括但不限于：

1. 知情同意书过程管理；
2. 知情同意书的签订，应包括受试者本人签署、监护人签署、公平见证人见证等；
3. 知情同意书更新签署；
4. 安全性信息更新；
5. 质控端口等。
   * + 1. 上链数据内容

应包括但不限于：

1. 受试者基本信息，不应包含其个人隐私信息，同时对关键信息需加以脱敏处理；
2. 1 年内参加过的临床试验摘要；
3. 既往病史及记录摘要，包括既往用药史及用药起止时间；
4. 知情同意书的签署摘要；
5. 知情同意过程摘要。
   * 1. 病例报告表管理模块
        1. 模块介绍

病例报告表指按照试验方案要求设计，向申办者报告的记录受试者相关信息的纸质或者电子文件。病例报告表中的数据准确、完整、清晰和及时，与源文件一致。病例报告表中数据的修改，应当使初始记录清晰可辨，保留修改轨迹，必要时解释理由，修改者签名并注明日期。

* + - 1. 模块主要内容

应包括但不限于：

1. 筛选入选；
2. 随机化；
3. 第三方中心实验室、独立评估机构数据的自动抓取；
4. 试验数据的辅助分析、判断、预警、质疑；
5. 病例报告表的录入、审核、修改；
6. 合并用药记录；
7. 临床试验研究过程及医学处置管理；
8. 临床异常值的辨别及处理；
9. 质控端口；
10. 正常值范围，包括自动抓取或手动录入/修改等。
    * + 1. 上链数据内容

应包括但不限于：

1. 病例报告表摘要；
2. 合并用药记录；
3. 临床试验研究过程摘要；
4. 临床异常值处理摘要；
5. 过程性质控内容；
6. 正常值范围，包括自动抓取或手动录入/修改等。
   * 1. AE/SAE/SUSAR/AESI处理模块
        1. 模块介绍

研究者的安全性报告应当注明受试者在临床试验中的鉴认代码，而不是受试者的真实姓名、公民身份号码和住址等身份信息。应完整记录AE、SAE，与药物相关性判断标准符合试验方案规定和医疗常规。研究者应确保发生AE、SAE的受试者得到及时合理的观察与治疗。药物临床试验期间发生的可疑且非预期严重不良反应、研发期间安全性更新报告，申办者根据《药物临床试验期间安全性数据快速报告的标准和程序》中按有关程序和规范要求向药品审评部门、伦理委员会等进行报告。

* + - 1. 模块主要内容

应包括但不限于：

1. 临床异常值的辨别及提醒；
2. AE/SAE/SUSAR/AESI的自动生成、处理及判断；
3. SAE/SUSAR/AESI的上报、跟踪及反馈；
4. 涉及死亡事件的报告；
5. 安全性信息更新；
6. 紧急揭盲程序；
7. 质控端口等。
   * + 1. 上链数据内容

应包括但不限于：

1. 临床异常值提醒数据记录；
2. SAE/SUSAR/AESI的过程摘要；
3. 涉及死亡事件的报告摘要；
4. 紧急揭盲记录。
   * 1. 试验用药物管理模块
        1. 模块介绍

试验药物的制备应当符合临床试验用药品生产质量管理相关要求。试验药物的使用应当符合试验方案。试验用药品在临床试验机构的接收、贮存、分发、回收、退还及未使用的处置等管理应当遵守相应的规定并保存记录。试验用药品的贮存应当符合相应的贮存条件。研究者应当确保试验用药品按照试验方案使用。

* + - 1. 模块主要内容

应包括但不限于：

1. 药品说明书/研究药物手册；
2. 检验报告；
3. 试验用药品记录，包括接收、贮存、分发、使用、回收、退还、未使用药品的处置、销毁等环节；
4. 试验用药品库存管理的记录，包括出入库管理、项目号、项目名称、运单号、物流公司、物流单号、日期、数量、批号/序列号、有效期、温湿度记录、按规则生成药品编号，满足临床试验药品管理的特殊性，包括最大包装单位和最小单位、签名等；
5. 药品的贮存条件；
6. 运输条件，应注明是否需要避光；
7. 药物的配制方法和过程；
8. 药物给药方法或装置的要求；
9. 受试者日记卡使用药物情况；
10. 质控端口等。
    * + 1. 上链数据内容

应包括但不限于：

1. 试验用药品记录；
2. 药品说明书/研究药物手册摘要；
3. 检验报告摘要；
4. 试验用药品库存管理的记录；
5. 药品的贮存情况记录；
6. 药品运输情况记录；
7. 药物的配制方法和过程记录；
8. 药物给药记录；
9. 受试者日记卡使用药物情况。
   * 1. 生物样本及信息管理模块
        1. 模块介绍

生物样品采集、处理、储存、转运等各环节的管理遵守相应的规定并保存记录。生物样品的采集、处理、储存和转运的条件符合临床试验方案的要求。样本容器的标识易于识别和具有唯一性，且不泄露受试者隐私及制剂种类生物样品管理各环节的异常情况及时评估、处理、记录。临床试验中采集标本的管理、检测、运输和储存应当保证质量。

* + - 1. 模块主要内容

机构部分应包括但不限于：

1. 生物样本采集、处理、储存、转运、销毁等环节；
2. 生物样本管理的记录，应包括：日期、数量、仪器、唯一编码、签名等内容；
3. 样本的储存条件；
4. 运输条件；
5. 质控端口等。

中心实验室部分应包括但不限于：

1. 样本的储存条件；
2. 运输条件；
3. 待测样本管理的记录，包括接收、处理、检验检测、储存、归还（如适用）、销毁等过程；
4. 复测样本的审核及处理；
5. 检测结果的确认；
6. 危急值处理流程；
7. 方法学确认、验证；
8. 仪器设备管理的记录，包括使用、维护、校准等；
9. 环境温度和湿度监测等。

独立评估机构部分包括：

如独立影像学评估中心、终点事件裁定委员会、终点病例判定委员会、数据安全监查委员会等机构，应包括但不限于：

1. 资质；
2. 评估流程；
3. 数据记录及修改等。
   * + 1. 上链数据内容

应包括但不限于：

1. 生物样本采集、处理、储存、转运、销毁等环节记录；
2. 生物样本管理的记录；
3. 样本的储存条件记录；
4. 待测样本管理的记录；
5. 复测样本的审核及处理摘要；
6. 环境温度和湿度监测记录；
7. 独立评估机构资质摘要；
8. 独立评估机构评估流程记录等。
   * 1. 查询统计分析模块
        1. 模块介绍

对临床试验过程中的数据进行分析利用，包括查询统计分析、数据运行分析等。

* + - 1. 模块主要内容

本模块需要可进行查询统计和动态试验结果统计。推荐实现：数据库锁定管理。

* + - 1. 上链数据内容

应包括但不限于：最终数据统计记录。

* + 1. 监查、稽查模块
       1. 模块介绍

本模块主要包括监查和稽查两部分，其中：

1. 监查是为了保证临床试验中受试者的权益，保证试验记录与报告的数据准确、完整，保证试验遵守已同意的方案、药物临床试验质量管理规范和相关法规。其范围和性质取决于临床试验的目的、设计、复杂性、盲法、样本大小和临床试验终点等。
2. 稽查是对临床试验相关活动和文件进行系统的、独立的检查，以评估确定临床试验相关活动的实施、试验数据的记录、分析和报告是否符合试验方案、标准操作规程和相关法律法规的要求。

在试验各个阶段产生的必备文档，可自动形成数字ISF、数字受试者文件夹等，便于远程监查或稽查；远程监查应可动态查阅相应受试者在医院相关系统内的源数据，但应符合安全管理要求，如智能化脱敏、实时抓取信息、不可保存、打印等。

* + - 1. 模块主要内容

监查应包括但不限于：

1. 监查计划管理，包括监查策略、方法、职责和要求等；
2. 监查报告管理；
3. 数据监查委员会端口（如涉及）。

稽查应包括但不限于：

1. 稽查规程 包括：目的、方法、次数等内容；
2. 稽查员管理；
3. 稽查报告管理；
4. 稽查证明管理。
   * + 1. 上链数据内容

应包括但不限于：

1. 监查计划记录；
2. 监查报告摘要；
3. 稽查规程摘要；
4. 稽查报告摘要；
5. 稽查证明摘要。
   * 1. 检查模块
        1. 模块介绍

药品监督管理部门对临床试验的有关文件、设施、记录和其他方面进行审核检查的行为，检查可以在试验现场、申办者或者合同研究组织所在地，以及药品监督管理部门认为必要的其他场所进行。

* + - 1. 模块主要内容

应包括但不限于：

1. 临床试验许可与条件；
2. 伦理运行情况；
3. 临床试验过程；
4. 药品管理；
5. 生物样本管理及检测；
6. 中心实验室及独立评估机构；
7. 临床试验数据采集与管理；
8. 委托研究；
9. 生物样品分析条件与合规性；
10. 生物样品分析实验的实施等；
11. 临床试验必备文件管理。
    * + 1. 上链数据内容

应包括但不限于：检查报告摘要。

* + 1. 药物临床试验项目质量控制模块
       1. 模块介绍

质量控制是在临床试验质量保证系统中，为确证临床试验所有相关活动是否符合质量要求而实施的技术和活动。

* + - 1. 模块主要内容

应包括但不限于：

1. 临床试验项目跟踪情况记录；
2. 质量检查记录；
3. 问题反馈记录；
4. 整改情况记录；
5. 项目层面重要SOP（如有）等。
   * + 1. 上链数据内容

应包括但不限于：

1. 临床试验项目跟踪情况记录；
2. 质量检查记录；
3. 问题反馈记录；
4. 整改情况记录；项目层面重要SOP（如有）等。
   * 1. 数据补登及勘误模块
        1. 模块介绍

数据的补登及勘误应当具有完善的权限管理和稽查轨迹，可以追溯至记录的创建者或者修改者，修改过程应当完整记录，原数据（如保留电子数据稽查轨迹、数据轨迹和编辑轨迹）应当保留。若数据处理过程中发生数据转换，确保转换后的数据与原数据一致，和该数据转化过程的可见性。

* + - 1. 模块主要内容

应包括但不限于：

1. 用户账号权限；
2. 补登端口；
3. 勘误端口；
4. 补登及勘误说明等。
   * + 1. 上链数据内容

应包括但不限于：

1. 用户账号权限；
2. 补登端口；
3. 勘误端口；
4. 补登及勘误说明等。
   1. 数据上链规则
      1. 信息采集

将采集到的研究者和临床试验机构关键信息打包并同时录入数据库与机构所维护的区块链节点，经过平等的共识过程把信息摘要写入区块，写入成功的信息会返回区块链中一条交易的哈希值，它是检索区块链中数据的索引，并将该返回值存储到数据库中。

* + 1. 智能交互

智能合约层与系统进行交互，其中：智能合约层主要负责将逻辑层的数据处理结果锚定到区块链层的存储区内。系统智能合约主要由若干的结构体组成，并以此结构方式存储电子数据的关键信息。

* + 1. 去中心化

在智能合约的编写过程中，定义文件、记录、成员和用户等多个结构体变量，分别存储电子数据文件的关键信息、电子数据文件分片的关键信息、用户资料和电子数据文件的所有关系。基于上述变量，依次编写电子数据信息的上传、电子数据信息的查询、电子数据的授权、用户信息的更新和用户信息的查询。考虑到数据写入的速度较慢，容易影响用户体验，宜采用异步请求方式执行事务，以此来加快电子数据的查询传输速率。同时，可引入两个或以上监管部门，利用区块链平等共识、数据多点备份、分布式的特性，消除了原来的追溯系统中核心机构的中心化问题。在这样的机制下，数据实现了不可篡改，系统实现了去中心化。

* + 1. 访问权限

所有信息都存储在区块链中并且支持被授权的节点对其进行访问。信息存取的权限又取决于参与者在链中的角色与职能。此外，区块链的运行规则由代码定义并存储在区块链中，无法被区块链中的某一参与者所修改，从而保证数据的真实性与有效性。若要改变区块链运行规则，则同数据存储一般，需要向全部节点进行广播并且由重点部门核实确认。

* + 1. 系统授权

在被授权参与者维护试验信息文档及数据时，需要私钥登入，信息及数据录入和改动均需通过智能合约的审核和验证，信息及数据被打包成区块信息录入系统，通过授时服务器，避免了区块信息访问或交易时发生矛盾。此外，数据信息在“交易”时，需要两个节点达成统一协议并数字签字，确保了数据信息传输的安全性和可靠性。同时由于非对称加密和全网广播技术的存在，两个节点的身份信息无需公开，但交易信息会被记录在区块链中。一旦交易完成，系统授权对象会从一个节点转移到另一节点，后者可继续维护并补充试验信息。从信息录入修改到系统授权转移，整个过程信息可溯源并无法被篡改。

* + 1. 数据格式

临床数据格式存在多样性，主要有以下几类：

1. 试验机构、研究者、项目管理模块中的相关法律文件信息、试验项目相关的文件信息；
2. 受试者信息管理模块中的医疗文本信息、表格化数据、格式化量表数据等；
3. 临床试验中模块中的药物信息、治疗流程信息、生物样本检测信息等；
4. 统计分析模块中的量化数据、定性分级数据、统计摘要数据等。以上数据存在不同模块中，数据上链前是从各个模块中将不同类型数据统一上传至IPFS，然后转换成符合CID数据，再上传至区块链。
   * 1. 监督

临床试验机构将试验过程采集到的信息录入数据库，并记入区块链。在这个过程中，监督管理单位对各单位的行为进行监督。在系统中不承认区块链发生的分叉行为，一旦数据写入区块链就不可通过分叉的形式进行更改。

* + 1. 审核

监督管理单位可通过序列号从数据库中查询出对应的详细流程信息，若要对信息的完整性进行检验，再通过区块链中保存的消息摘要与数据库查询出的信息进行对比，若两者相同说明数据在录入系统后就未再更改，数据完整。

* 1. 数据加密要求
     1. 加密方式

支持同态加密的方式对数据进行加密。智能合约去中心化处理数据，掌握数据执行权，控制加密数据的访问和执行权限，加密数据用后置空销毁，使用方只有密文结果的使用权，互相监督，互相制约，实现数据权的分离解耦。

* + 1. 加密需求

加密需求包含传输加密需求和加密算法需求，其中：

1. 传输加密需求：网络通讯中应全面采用安全通讯协议或加解密技术，禁止对业务信息、用户帐号等数据进行明文传输。
2. 加密算法需求：系统需采用中国国产密码SM系列的密码算法标准，对称密码算法需使用分组密码算法SM4和流密码算法ZUC；非对称密码需使用SM2和SM9算法；哈希密码算法需使用SM3。
   * 1. 签名人数字证书

签名人数字证书的私钥应由签名人唯一控制。

* 1. 系统安全要求

用于多中心药物临床试验管理系统开发的系统安全应符合GB/T 42570-2023和GB/T 42571-2023规定的安全要求。

参考文献

[1] 《药物临床试验质量管理规范》（GCP）

[2] 《药物临床试验机构管理规定》

[3] 《区块链信息服务管理规定》

[4] 《中华人民共和国数据安全法》

[5] 《中华人民共和国个人信息保护法》