

团 体 标 准

T/CGCPU XXX-20XX

疫苗临床试验电子源数据系统应用

Application of Electronic Source Data System in Vaccine Clinical Trial

(征求意见稿)

20XX-XX-XX 发布

20XX-XX-XX 实施

中关村玖泰药物临床试验技术创新联盟 发布

目次

前言 II

引言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 基本原则 3

5 职责 4

6 管理要求 6

7 系统基本要求 8

8 电子源数据管理 12

9 系统应用操作规范 13

参考文献 18

前 言

本部分按照 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》给出的规则起草。

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这些专利的责任。

本文件由中关村玖泰药物临床试验技术创新联盟提出并归口。

本文件起草单位：国新健康保障服务集团股份有限公司、北京思睦瑞科医药科技股份有限公司、河北省疾病预防控制中心、重庆智飞生物制品股份有限公司。

本文件主要起草人：李月红、曹诗琴、曹彩、刘英杰、王浩、刘加振、李小艳、莫雪梅、董瑞华、张黎、郝晓花、吴竞轩、付斌。

引 言

疫苗临床试验作为公共卫生安全与创新疫苗研发的关键环节，其数据质量、时效性及合规性直接影响研究结论的科学性与监管决策的可靠性。随着疫苗研发全球化、多中心化及数智化转型的深入推进，传统的人工数据采集模式在效率、管理、数据可靠性及风险控制等方面已经不能满足日益增长的数据质量需求，而电子源数据系统相比人工数据采集具有非常明显的优势，如数据及时录入、实时发现数据错误、数据全过程可溯源等，并显著提高临床试验数据质量，提升研究效率，加快研究进度等，已然成为了现代临床试验数据采集与管理的重要工具。然而，电子源数据系统的应用虽逐步普及，但尚缺乏统一的技术标准与管理规范，存在数据管理流程不一致、系统功能要求差异等问题，易出现合规隐患和跨机构协作壁垒，从而制约疫苗研发进程与国际竞争力。

在此背景下，为规范电子源数据系统的应用，制定统一的应用技术要求和操作规范，推动电子源数据系统在疫苗临床试验中的规范化、标准化和可信化应用，确保临床试验数据满足 ALCOA+原则，即可归因性、易读性、同时性、原始性、准确性、完整性、一致性、持久性和可获得性，进而提升疫苗临床试验数据质量的整体水平，为疫苗研发的科学性和监管决策的可靠性提供技术支撑，为行业自律提供指导。

本文件针对疫苗临床试验实施的特殊性，围绕电子源数据系统应用的全生命周期，从各方职责、信息化应用和管理要求、电子数据管理及操作规范等多个维度确立了统一要求，期望能够促进临床试验参与各方之间的协调合作，降低数据偏差风险，提高临床试验数据质量与可靠性，为监管申报与科学决策提供坚实的数据基础，推动疫苗研发的高效协同与创新发展。

此外，本文件亦致力于推动行业内最佳实践的形成，加强监管机构、申办者、研究者以及服务供应商之间的沟通与协作，促进各方对电子源数据系统应用的理解与共识，共同构建更加高效、透明和协同的疫苗研发环境。这不仅对于提升数据质量与可靠性具有重要意义，同时也为疫苗临床试验的全面信息化与数智化转型提供了有力支撑，为疫苗研发的科学性奠定坚实的数据与技术基础。

疫苗临床试验电子源数据系统应用

1 范围

本文件规定了疫苗临床试验中电子源数据系统的基本架构、功能规范及全生命周期管理要求，涵盖系统设计、部署、验证、运行、变更控制及退役等阶段。

本文件适用于疫苗临床试验中的下述组织：

- 申办者；
- 临床试验机构；
- 合同研究组织（CRO）；
- 系统服务供应商。

为其在电子源数据系统下述活动中提供必要的技术支持和工具：

- 开发设计；
- 应用实施；
- 维护管理；
- 系统退役等全生命周期。

无论是自主研发的电子源数据系统，还是采购的第三方（服务供应商）系统，在应用过程中均可遵循参考本标准的规定，确保系统建设与数据管理的规范性、可靠性和合规性。

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 19000—2016 质量管理体系 基础和术语

3 术语和定义

GB/T 19000—2016 界定的及以下术语和定义适用于本文件。

3.1

临床试验 clinical trial

以人为对象的临床干预研究

注：包括患者和健康受试者。临床试验意在发现或验证某种试验药物的临床医学、药理学、其他药效学作用、不良反应，或者试验药物的吸收、分布、代谢和排泄，以确定药物的疗效与安全性的系统性试验。本文件中的药物特指疫苗。

3.2

疫苗 vaccine

为预防控制疾病的发生、流行，用于人体免疫接种的预防性生物制品

注：包括免疫规划疫苗和非免疫规划疫苗。

3.3

源数据 source data

原始记录或者核证副本上记载的所有信息

注：源数据可包括临床发现、观测结果以及用于重建和评价临床试验所需要的其他相关活动记录。

3.4

电子源数据 electronic source data

使用电子采集工具记录的源数据（3.3）

3.5

权限控制 access control

允许、限制或禁止对系统的登录或使用，或对系统中某项信息资源项的访问、输入、修改、浏览能力的技术控制

3.6

审计追踪 audit trail

一系列从原始数据追踪到有关的记录、报告或事件，或从记录、报告、事件追溯到原始数据的活动

3.7

逻辑核查 edit check

对数据有效性的检查

注：这种核查可以通过系统的程序逻辑，子程序和数学方程式等方法实现，主要评价输入的数据域与其预期的数值逻辑、数值范围或数值属性等方面是否存在错误。

3.8

变更控制 change control

对变更过程的控制

注：变更的原因一般来自两个方面：系统更新或研究方案的修订所导致的数据采集发生变化。变更过程应事先严格规划，事后详细记录。规划中应明确变更的内容，指定具体实施的人员、方法和步骤；记录中应包括开始日期、变更实施过程中的规划偏离和应对措施以及最后的处理结果、结束日期，此即所谓的过程控制。变更控制的主要目的有两个方面：确保原有数据无损；变更后的系统满足预期的要求。

3.9

用户接受测试 User Acceptance Testing

电子源数据（3.4）系统用户实施的标准化测试流程

注：在招募受试者之前，由用户将模拟数据录入系统，测试系统是否按照设计要求对所有数据正确储存、逻辑核查正确执行、外部数据能与目标系统正确整合、接入的仪器设备正常使用等。

3.10

源数据审阅 Source Data Review

在临床试验（3.1）过程中，临床监查员对研究者提供的所有源数据、源文件和报告所做的查阅活动

4 基本原则

4.1 适用性

电子源数据系统应基于疫苗临床试验的实际需求进行功能配置与技术实现，其设计、部署及验证过程应遵循风险可控、灵活可扩展的原则，确保系统功能与临床试验方案设计、数据采集规范及监管要求的动态适配性。

4.2 实时性

电子源数据的采集应与观察、操作同步进行，以确保数据与真实情况保持一致，避免因延后录入产生记忆偏差导致数据记录错误，保障源数据记录的及时性、真实性与准确性。

4.3 可靠性

源数据采集、传输、处理、存储、归档、恢复等应符合《药物临床试验质量管理规范（GCP）》等法规要求，确保数据质量遵循ALCOA+原则，即可归因性、易读性、同时性、原始性、准确性、完整性、一致性、持久性和可获得性。

4.4 可控性

电子源数据的最终归属及管理权限应符合行业主管部门相关要求，参与试验各方应签订合规的法律文件，禁止系统提供方修改源数据。数据的采集方对数据负最终管理责任，应确保相关数据仅被临床试验相关方在职权范围内合理使用。试验过程中应密切关注受试者权益与隐私保护，并建立数据泄露应急响应机制，定期开展权限审计与安全影响评估。

4.5 安全性

电子源数据系统应具备完善的加密、备份、恢复等安全和保密措施，防止数据泄露、篡改或丢失，保障临床试验数据的安全性与保密性。

4.6 合规性

电子源数据系统的开发、应用、维护、退役等全生命周期应符合国家相关法律法规和行业标准，以确保源数据采集和管理的可靠性与合规性。

5 职责

5.1 总则

应用电子源数据系统的疫苗临床试验，申办者、临床试验机构及服务供应商应签订合同或协议，对电子源数据归属、使用、管理和维护等进行明确的职责划分，或在相关管理制度/SOPs中作出明确规定。

5.2 申办者

申办者应对其使用的电子源数据系统进行评估和选择，确保系统及数据的安全性、可靠性与合规性。

申办者应建立电子源数据系统使用全过程质量管理体系，对临床试验电子源数据系统应用的全生命周期进行监督管理。申办者可以委托合同研究组织（CRO）承担电子源数据系统应用管理的工作和任务，但仍对临床试验数据质量负有最终责任。

申办者或其委托的合同研究组织应与临床试验机构密切协作，协同完成电子源数据系统应用合同

约定的相关职责内容：

- a) 电子源数据采集表的设计及更新；
- b) 临床试验数据库的建立、更新及版本控制；
- c) 用户接受测试（UAT）的执行与确认；
- d) 临床试验数据库上线发布、锁定与解锁执行；
- e) 源数据审阅（SDR）等质量控制活动。

5.3 临床试验机构

临床试验机构应具备电子源数据系统应用所需的必要条件，包括提供可用的网络资源、数据存储设备（云服务器或本地服务器）等。临床试验机构还应建立电子源数据系统使用和管理相关的标准操作规程，对电子源数据系统应用的全生命周期进行组织管理与质量控制。

电子源数据系统应用过程中，临床试验机构应履行以下管理职责：

——系统应用管理：

- 组织系统和设备使用培训，协调研究团队规范操作系统；
- 组织实施用户接受测试；
- 用户权限审批与管理；
- 临床数据传输、迁移、锁定与解锁批准。

——数据安全的管理：

- 临床试验机构服务器部署及日常维护；
- 定期备份电子源数据。

——数据质量控制。

5.4 临床试验现场

临床试验现场应具备电子源数据系统应用所需的必要条件，以确保电子源数据系统的稳定运行。

包括：

- 提供可用的临床试验场所、稳定可靠的网络环境；
- 具备完善的电力及应急保障设施；
- 提供具备相应资质或专业背景的研究者。

电子源数据系统应用过程中，临床试验现场研究者应履行以下职责：

- 协助临床试验机构建立电子源数据系统使用的标准操作规程；
- 开展系统和设备使用培训；

- 建立仪器设备管理程序，定期检查并维护仪器设备；
- 规范执行电子源数据采集与更新。

5.5 系统服务供应商

系统服务供应商应按照申办者、研究者的要求，提供电子源数据系统的补充开发、安装和验证等服务。并应建立电子源数据系统开发、测试、验证、维护等标准操作规程。

系统服务供应商所提供的电子源数据系统应满足药品监督管理部门的管理要求和技术要求，保护受试者隐私，确保源数据的真实、完整、可靠、可追溯。

系统服务供应商需配备专业的技术支持人员提供全天候的技术支持，并与委托方签订具有法律约束力的技术服务协议。系统正式投入使用之前，技术支持人员应协助完成临床试验机构服务器部署。系统运行过程中应对系统运行、审计追踪、存储设备、备份数据的完整性和可用性等进行日常监控和检查，建立可追溯的监控日志记录。当出现系统故障时，技术支持人员应立即对故障进行诊断并进行相应的修复措施，确保系统连续稳定运行。

系统服务供应商应签署临床试验源数据防篡改承诺书，禁止对已采集的源数据实施非授权修改、删除或篡改。确因系统维护或数据纠错需要调整源数据的，需经主要研究者与申办者书面授权并完整记录操作轨迹。违反本条款导致数据完整性受损的，服务供应商应依据《中华人民共和国疫苗管理法》《药物临床试验质量管理规范》等相关法律法规承担相应责任。

6 管理要求

6.1 研究人员管理

电子源数据系统应具备完善的访问控制和用户权限管理功能，确保登录用户的唯一性与可追溯性。临床试验机构应指定系统权限分配负责人，根据参与临床试验的研究人员职责分工分配相应的操作权限。

临床试验项目启动前，参与系统使用的研究者应建立研究人员档案并及时更新，档案内容应包括：

- 授权任命文件；
- 个人简历；
- 资格证明文件；
- 保密约定；
- 电子系统账户及电子签名声明；
- 系统使用相关培训记录等。

6.2 受试者管理

电子源数据系统应建立受试者身份信息识别与隐私数据安全机制，确保受试者的可追溯性及隐私数据的安全。受试者信息管理应符合下列要求：

——为受试者分配唯一性标识符，确保临床试验全流程数据可追溯，标识符包括但不限于：

- 数字编码；
- 一维码；
- 二维码。

——隐私数据采集范围应限于临床试验目的必需的个人信息，并实施基于角色的最小化访问权限控制；

——临床试验机构应建立数据保密程序，包括：

- 保密约定；
- 账户安全措施；
- 操作人员保密培训。

——系统使用过程中，研究者应对涉及受试者身份信息的数据进行匿名化或去标识化处理，以最大程度减少个体识别风险。

6.3 试验全过程信息化管理范围

临床试验全过程均可以使用电子源数据系统进行源数据的采集与管理，包括：

- 知情同意；
- 筛选与体检；
- 随机入组；
- 样本采集与管理；
- 疫苗接种；
- 疫苗管理；
- 随访管理；
- 不良事件报告。

电子源数据系统应建立完善的逻辑核查校验程序，以确保数据的完整性、准确性与一致性。逻辑核查校验应符合以下要求：

- a) 自动化逻辑核查应对数据范围、格式、时间逻辑等要素进行合规性判定；
- b) 发现数据异常时触发提示功能，但不得限制研究者录入数据或干预数据内容；
- c) 操作日志完整记录数据修改轨迹及判定结果。

6.4 计算机系统管理规程

研究者、申办者及服务供应商应制定电子源数据系统相关的标准操作规程，确保系统开发至退役各环节操作合规、数据可靠。操作规程应明确各方职责并包含以下内容：

- a) 系统开发、验证、维护、变更及退役全生命周期管理规范；

- b) 数据库构建、测试、权限管理及系统关联仪器设备管理等系统应用全流程操作规范；
- c) 电子源数据采集、传输、迁移、销毁、备份与恢复等数据管理要求。

6.5 仪器设备管理

电子源数据采集专用计算机及接入设备应具有明确的技术规范与管理标准，确保系统运行安全符合试验质量要求。仪器设备应满足下列管理要求：

- 研究专用计算机应设置访问控制措施（如身份认证、密码策略），安装实时病毒防护软件，禁止安装非授权软件；
- 接入仪器设备应符合国家行业标准及系统兼容性要求；
- 仪器设备应实施唯一性编码标识，配备专人负责日常维护及异常报备；
- 仪器设备档案需完整记录交接、安装调试、校准维护及退役处置信息；
- 仪器设备运行期间应定期进行检查与维护。

电子源数据采集专用计算机及接入设备宜由服务供应商统一提供，设备采购及管理责任主体应在临床试验协议中作出明确规定。

6.6 质量管理

申办者及研究者应对数据管理与系统应用等各个环节实施有效管理和控制，建立包含常态化监控、审计追踪以及闭环管理机制的质量管理体系，确保系统运行合规、风险可控。电子源数据系统质量管理体系应符合下列要求：

- a) 体系设计应符合《药物临床试验质量管理规范（GCP）》及ALCOA+原则，覆盖数据采集、权限控制、备份恢复、审计追踪及系统变更等环节；
- b) 对数据采集设备、逻辑核查规则、用户操作行为实施常态化质量监控；
- c) 定期执行系统数据完整性、可靠性质量控制活动，问题项应闭环整改。

7 系统基本要求

7.1 系统可靠性

电子源数据系统架构设计、功能实现及运行管理等各环节均应严格遵循可靠性标准，以确保系统持续稳定运行，系统产生和管理的数据符合ALCOA+原则。具体要求如下：

- a) 系统架构应满足高可用性及时效性要求，并配备负载均衡及冗余容错机制，数据需实时备份，灾备恢复应支持全量恢复且恢复时间目标（RTO） ≤ 4 小时；
- b) 系统应具有完整的稽查轨迹和审计追踪功能，记录有关系统、应用程序及用户的所有操作记录，任何人不得删除、修改或关闭；
- c) 系统上线前需完成计算机系统验证，系统生命周期内应自始至终都保持被验证过的状态；
- d) 系统全年服务可用率不低于99.9%（即全年宕机时间应 ≤ 8.76 小时）；

- e) 系统应具备自动容灾切换机制及资源弹性扩容机制，硬件故障或流量激增时自动切换至备用节点并动态扩展计算资源，保障数据采集连续性。

7.2 系统安全

电子源数据系统应通过公安部网络安全等级保护第三级及以上认证，系统安全需符合《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》。安全管理要求如下：

- a) 基础设施安全：数据存储服务器应符合临床试验机构内部或外部管理的等级保护要求，本地服务器需配备防火、防潮等措施，云存储服务供应商应具备ISO 27001信息安全管理体和公安部网络安全等级保护第三级及以上认证；
- b) 访问安全：登录用户应经过授权，身份认证宜采用动态双因素验证，用户权限应遵循最小权限原则；
- c) 数据安全：数据存储应实施本地和异地双备份机制，隐私敏感数据应采用国密或AES-256等更高安全级别的加密算法进行存储；所有数据传输宜通过TLS 1.2及以上版本协议进行加密保护；
- d) 运维安全：系统供应商应建立数据安全管理体系及应急预案，实时监测网络攻击及异常访问行为，安全事件处置记录保存期限不低于10年。

7.3 备份与恢复

电子源数据系统应进行异地备份和本地备份，当发生不可抗力或不可控因素造成系统运行中断时，可以紧急启用或恢复，以确保系统运行的连续性和数据的安全性。备份与恢复应符合下列管理要求：

- a) 数据应实时备份，其中增量备份（ $RPO \leq 15$ 分钟），全量备份周期不得超过7天；
- b) 数据存储应同步异地灾备（地理隔离 ≥ 500 公里）；
- c) 数据灾难恢复时间目标（ $RTO \leq 4$ 小时）、恢复点目标（ $RPO \leq 1$ 小时），关键业务数据恢复时间目标（ $RTO \leq 4$ 小时）、恢复点目标（ RPO ） ≤ 15 分钟；
- d) 系统应用应制定分级应急预案，使系统在最短时间内恢复正常运行；
- e) 系统供应商应定期对硬件故障、网络攻击等场景执行灾难恢复演练，演练报告及恢复日志留存期限不低于10年。

7.4 权限控制

电子源数据系统应具备完善的权限管理机制，保障数据访问安全。权限控制应符合下列要求：

- a) 账户开通需经主要研究者书面授权，禁止共享账户、使用通用账户或转交他人使用；
- b) 用户身份认证宜采用双因素验证（密码+动态令牌/生物特征），密码长度 ≥ 8 位，包含大小写字母、数字及特殊符任意三种组合，至少3个月更换一次，更换的新密码不应与最近5次旧密码相同；
- c) 系统长时间空闲时或短时间暂停工作时实行自行断开连接，时长不超过15分钟；
- d) 权限控制应遵循最小权限原则，用户仅被授予完成工作所需的最小权限；监管账户仅能查阅数

据，不能对数据进行编辑、修改或删除；

- e) 系统操作日志应完整记录账户登录、权限变更及异常访问行为，日志存储期限不得低于临床试验数据留存时限。

7.5 电子签名

电子签名应符合下列要求：

——电子签名功能应符合《中华人民共和国电子签名法》；

——电子签名方式包括但不限于：

- 生物特征（如指纹/面部识别等）；
- 数字证书；
- 用户名及密码；
- 动态令牌（如短信验证码）。

——电子签名应能够追溯至签署者的个人身份，包括签署者、签署日期及时间，并与其签署的相应电子记录相关联；

——电子签名应具有唯一性，不可被篡改、删除或复制；

——电子记录变更时，系统应追加新签名并保留原始签名轨迹，变更记录需标注修改原因、时间及操作者；

——用户应在首次使用电子签名前签署电子签名法律效力声明，经签署者确认后生效，声明内容应符合《电子签名法》第十四条等效性认定要求。

7.6 数据审阅

电子源数据系统应具备源数据审阅（SDR）模块，支持审阅标记、批注及数据质疑生成功能。数据审阅应符合下列要求：

- a) 临床监查员审阅权限应遵循受试者隐私数据最小化原则；
- b) 临床监查员查阅受试者隐私信息需经主要研究者授权，且仅限临床试验现场查阅；
- c) 审阅日志应完整记录审阅人员、时间、内容及操作类型，保存期限不得低于临床试验数据留存时限。

7.7 数据质疑

电子源数据系统应具备数据质疑全流程管理模块，支持质疑生成、派发、答复、关闭及重开操作，质疑状态变更记录需与原始数据关联存储，数据质疑应符合下列要求：

- a) 系统用户经授权后，可以通过质疑管理模块将数据质疑发布给研究者；
- b) 研究者应及时完成数据复核，更正数据需追加电子签名并标注修改依据；
- c) 质疑处理日志应完整记录质疑内容、操作者、操作时间及最终结论，保存期限不得低于临床试验数据留存时限。

7.8 系统变更

电子源数据系统变更包括系统版本升级、功能修复、软件应用程序升级等，变更应严格遵循变更管理规程。系统变更应符合下列管理要求：

- a) 系统变更需确保前向兼容性，不得导致历史数据丢失、不可读或逻辑冲突；
- b) 应建立变更控制程序，明确变更申请、风险评估、测试验证、批准实施及文档归档流程；
- c) 变更实施前应评估系统变更对数据完整性及系统安全的影响，高风险变更需制定变更控制措施并确定再验证的范围；
- d) 变更后应执行全量回归测试，测试报告与变更记录保存期限不得低于10年；
- e) 系统版本迭代日志需标注变更内容、操作日期及操作人，供监管机构追溯审查。

7.9 系统验证

电子源数据系统上线运行前应经过计算机系统验证，且整个生命周期内应自始至终都保持着被验证过的状态，以确保系统开发、运行以及维护等环节能高度满足其预设的各种系统技术标准、使用目的和质量属性。系统验证应符合下列要求：

- 验证工作应由系统服务供应商或第三方独立机构实施；
- 验证范围应覆盖系统设计、安装确认（IQ）、运行确认（OQ）、性能确认（PQ）及变更控制等，验证计划需明确测试用例及验收标准；
- 验证过程应记录并形成验证文档，保存期限不得低于10年。验证文档应包括但不限于：
 - 验证计划书；
 - 验证文件；
 - 系统测试脚本；
 - 系统测试报告；
 - 系统测试结果；
 - 验证证书。
- 系统上线后应定期进行周期性回顾/审查，重大变更后需实施专项验证。

7.10 系统退役

电子源数据系统退役管理应符合下列要求：

- a) 系统停用前需完成全量数据备份、迁移或归档，备份、迁移或归档的数据应确保完整性与可读性，数据保存期限不得低于临床试验数据留存时限；
- b) 服务供应商应制定系统退役方案，明确数据迁移或归档路径、风险评估及应急措施；
- c) 退役操作日志应完整记录停用日期、数据处置方式及操作人员，日志保存期限与临床试验数据一致；
- d) 系统退役计划应提前30日书面通知临床试验相关方。

8 电子源数据管理

8.1 数据采集

电子源数据采集应严格遵循《药物临床试验质量管理规范（GCP）》及国际数据标准要求，确保数据采集质量。数据采集应符合下列要求：

- 人工录入数据应由授权研究者执行，系统需实时记录录入数据、录入者身份及时间，关键数据（如疗效终点、不良事件）应经过人工或计算机方式二次核查；人工录入的数据包括：
 - 受试者原始评估记录（如受试者日记卡、受试者自评报告）；
 - 研究者的实时操作；
 - 对不具备介入条件的仪器及设备的人工观察、巡检、结果判断及补充说明信息等。
- 自动采集的数据应不易被篡改、丢失或修改，数据采集与人工记录系统之间的接口传输应经过验证，并能正确显示时间戳；
- 数据修改需记录修改人、时间、原始值、修改后值及修改原因，修改轨迹应有完整记录；
- 数据格式应符合国际公认的数据标准和格式（如CDISC），数据字典应明确定义字段编码、逻辑规则及计量单位。

8.2 数据传输

临床试验中，通过人工/自动采集的外部数据（生命体征监测、受试者电子日记卡等）输入到电子源数据系统，或将电子源数据进行提取输出到其他采集系统中，应严格遵循《药物临床试验质量管理规范（GCP）》、《中华人民共和国网络安全法》及行业数据安全标准（如ISO 27001），确保数据传输从采集端到目标端的安全、可靠、可验证。数据传输应符合下列要求：

- a) 电子系统之间接口传输应经过验证；
- b) 数据传输前，临床试验参与各方应建立数据传输协议和流程，明确下列内容：
 - 1) 数据传输方法和频率；
 - 2) 外部数据结构与内容；
 - 3) 数据传输方式；
 - 4) 数据传输时间；
 - 5) 数据传输流程。
- c) 数据传输需进行全面且充分的测试，断点续传机制应保障数据零丢失与一致性；
- d) 传输日志保存期限不得低于临床试验数据留存时限，监管审查时需提供可追溯的传输链证据。

8.3 数据迁移

数据迁移过程应严格遵循《药物临床试验质量管理规范（GCP）》、《GB/T 20988-2007 信息系统灾难恢复规范》及行业数据管理标准，确保数据迁移的零风险、零丢失、可读写、可追溯。电子源数据迁移应符合下列要求：

- a) 数据迁移前完成全量备份并通过《GB/T 20988-2007 信息系统灾难恢复规范》完整性验证；
- b) 应制定迁移计划并明确数据结构变更项、风险评估结论及回退方案，经申办者及主要研究者书面批准后实施；
- c) 迁移过程中应暂停使用系统，恢复运行前需完成数据库检查；
- d) 迁移过程禁止覆盖或修改原始数据，迁移后数据一致性验证错误率应 $\leq 0.01\%$ ；
- e) 迁移审计日志应记录操作人员、时间节点、数据量及异常处理措施，日志保存期限不应低于临床试验数据保存时限。

8.4 数据销毁

数据销毁需严格遵循《药物临床试验质量管理规范（GCP）》、《中华人民共和国个人信息保护法》、《数据安全法》及《GB/T 35273-2020 信息安全技术 个人信息安全规范》等法律法规要求，确保数据彻底清除且操作全程可验证。电子源数据销毁应符合下列要求：

- a) 销毁前需经主要研究者及申办者充分评估并书面批准，明确销毁数据范围及执行人员；
- b) 销毁操作应由主要研究者和申办者授权的人员操作，全程视频监控并留存备查，保存期限与销毁记录一致；
- c) 销毁方式应采用《GB/T 35273-2020 信息安全技术 个人信息安全规范》中不可逆删除技术（如物理消磁、安全擦除方式），确保数据不可恢复；
- d) 销毁记录应包含数据清单、销毁方法、操作人员及时间戳等，保存期限不得低于临床试验数据留存时限。

9 系统应用操作规范

9.1 试验启动阶段

9.1.1 数据采集表设计

电子源数据采集表应由研究者与申办者（或合同研究组织）联合设计及更新，并符合下列要求：

- a) 数据采集项需完全覆盖临床试验方案要求的全部访视点和访视数据；
- b) 隐私数据字段应标注敏感标识，采集范围限定于方案必需的最小数据集；
- c) 符合国家药品监督管理部门管理规定的临床试验方案变更导致访视点和数据点更新的，应同步更新数据采集表。

9.1.2 数据库构建

临床试验数据库构建应由独立建库人员（非数据采集/管理人员）依据研究方案及电子源数据采集表设计及更新，数据库设计说明应预先对所需采集的数据点定义，定义内容包括但不限于：

- 数据集名称；
- 变量名称；

——变量类型；

——变量规则。

9.1.3 逻辑核查设计

电子源数据系统逻辑核查规则应由研究者或申办者（或合同研究组织）制定，经主要研究者及申办者书面批准后实施。逻辑核查的设计应符合下列要求：

- a) 逻辑核查范围通常覆盖必填项缺失、数值阈值超限、时间逻辑冲突、事件先后顺序及跨表单数据一致性等，逻辑规则应与临床试验方案规定相符；
- b) 临床试验进行过程中，如对核查规则进行更新，新规则不应追溯既往数据。

9.1.4 填写指南

数据填写指南由研究者或申办者（或合同研究组织）根据源数据采集内容及相关要求制定，填写指南需明确数据字段填写规则和数据修改规范，内容应清晰易懂。

9.1.5 人员培训

所有用户（含研究者、监查员）使用系统前应完成系统和设备使用培训，培训应符合下列要求：

- a) 系统用户培训内容应与用户角色职责匹配；
- b) 培训合格后才能获得系统使用权限，培训记录的保存期限不得低于临床试验数据留存时限；
- c) 系统功能变更、用户角色调整或标准操作规程更新后，适用范围内的人员应重新执行针对性培训。

9.1.6 用户接受测试

研究者和申办者（或合同研究组织）应在临床试验项目启动前完成用户接受测试，测试应符合下列要求：

- a) 测试计划书及测试报告需获得主要研究者与申办者的书面批准，测试完成后应进行书面确认；
- b) 测试场景应覆盖有效、无效、边界值、异常及不合理等输入场景，以充分验证数据库设计是否符合要求；
- c) 测试记录应存档，保存期限不得低于临床试验数据留存时限；
- d) 测试内容主要包括但不限于：
 - 1) 数据库测试：验证访视顺序、表单跳转逻辑、权限配置及数据字段属性与方案的一致性；
 - 2) 逻辑核查测试：模拟正常/异常数据输入，核查系统警示触发准确性及质疑闭环处理流程；
 - 3) 数据传输测试：依据传输协议验证数据格式（CDISC标准）、传输完整性及接口稳定性，数据结构变更后需重新测试；
 - 4) 设备使用测试：验证系统接入设备的兼容性与功能完整性。

9.1.7 上线使用

数据库上线使用前，研究者和申办者（或合同研究组织）应进行上线前核查确认，确认系统配置与临床试验方案及逻辑核查规则完全匹配后，由主要研究者和申办者书面批准上线。

9.2 试验进行阶段

9.2.1 权限管理

电子源数据系统权限管理应由非数据利益相关人员担任，且不得兼任数据采集或录入职责。权限管理员宜由临床试验机构主要研究者或授权的研究管理人员承担。权限管理应符合下列要求：

- a) 账户权限授予、变更、锁定与解锁需经主要研究者书面审批；
- b) 权限分配遵循最小权限原则，用户权限限于其临床试验职责必需的操作范围；
- c) 数据录入及修改权限仅授予经授权的研究者，申办者、合同研究组织及监管方不得持有数据编辑权限；
- d) 盲法临床试验，非盲态人员不得操作和访问电子源数据中的安全性及疗效评估等数据，盲态人员不能操作和访问受试者药物分组等盲态数据；
- e) 账户管理员宜每季度对账户使用状态进行核查，及时清理闲置账户。人员离职或调岗后应于24小时内注销权限。

9.2.2 数据采集

电子源数据采集人员需经主要研究者授权，完成系统和设备使用培训并签署账户声明后，方可开通数据采集权限。数据采集应符合下列要求：

- a) 数据录入需严格遵循《药物临床试验质量管理规范（GCP）》、临床试验方案及填写指南要求，源数据的采集应与观察、操作同步进行；
- b) 数据录入后如发现错误或不完整时，研究者宜在获得正确或完整数据后24小时内完成修改。数据修改权限仅限原始录入者或经同等授权的研究者，修改记录需包含修改人员姓名、原始值、修改后值及修改原因等；
- c) 临床试验中需要在临床试验现场采集的随访数据宜使用经物理网卡（MAC地址）白名单或VPN拨号认证绑定的研究专用计算机进行录入，以严格限定数据录入终端的物理位置，确保数据采集仅能在授权的临床试验现场完成；
- d) 研究者应对研究专用计算机进行源数据采集全过程影像记录（系统录制功能或安装第三方录屏软件等），影像视频应定期备份；
- e) 研究结束后，研究人员应对采集数据的研究专用计算机中window运行日志进行备份。

9.2.3 变更控制

电子源数据系统数据库变更应严格遵循变更操作规程，并确保原有数据完整无误。变更控制应符合

合下列要求：

- a) 关键数据库变更前，临床试验相关方应对数据库的变更进行评估，确定变更对数据可靠性产生的影响，经主要研究者和申办者批准同意后进行变更；
- b) 数据库变更后应对更改部分以及与更改内容相关的数据点进行全面测试，测试通过后再上线；
- c) 变更过程需严格控制，并详细记录变更内容、变更时间及变更人，变更记录应存档备查。

9.3 试验结束阶段

9.3.1 数据库锁定

试验结束后，经主要研究者和申办者的书面批准，系统管理员应对临床试验数据库进行锁定，数据库锁定前和锁定后应通知试验相关用户。

9.3.2 数据库解锁

数据库一般情况下不得随意解锁，如需解锁，应事先获得主要研究者和申办者书面批准，解锁条件和流程应严格遵循相应的标准操作规程，并将解锁记录存档备查。

9.3.3 文件归档

电子源数据系统文件归档应符合下列要求：

- 数据应归档在授权指定的安全区域或设备内，存档设备应具备防火、防盗、防潮等措施；
- 数据应专人管理并严格控制访问权限，档案管理员应定期对电子文档或设备进行检查；
- 数据归档要求和期限应不低于《药物临床试验质量管理规范（GCP）》及相关法规的要求；
- 电子源数据系统实施的临床试验中，除遵循《药物临床试验质量管理规范（GCP）》和《药物临床试验必备文件保存指导原则》对临床试验文件保存的要求外，还需保存以下的文档（但不限于）：
 - a) 系统技术支持服务协议或合同；
 - b) 系统验证文件；
 - c) 计算机系统应用和管理相关的SOP及应急预案；
 - d) 数据库构建的全套内容；
 - e) 逻辑核查文件；
 - f) 空白的电子源数据采集表（PDF格式）；
 - g) 系统用户手册；
 - h) 数据填写指南；
 - i) 申办者和研究人员的培训证明文件；
 - j) 用户接受测试文件；
 - k) 数据传输相关文件；
 - l) 账户及电子签名声明；

- m) 系统上线和再上线批准文件；
- n) 系统角色权限表、账户审批及权限管理记录；
- o) 系统相关设备记录（设备交接、安装与调试、维护等）；
- p) 研究专用计算机window运行日志；
- q) 临床试验影像记录（监控记录、影像录制视频等）；
- r) 研究过程中的系统的变更（如系统升级、项目数据库变更）的测试文件与再上线通告；
- s) 数据迁移相关文件；
- t) 每个受试者完整的电子源数据采集表（PDF格式）；
- u) 数据库锁定与解锁相关文件；
- v) 稽查轨迹；
- w) 研究过程中的应急计划的相关文件；
- x) 灾难恢复过程的相关文件。

参考文献

- [1] 《药物临床试验质量管理规范》国家药监局 国家卫生健康委（[2020]第 57 号，自 2020 年 7 月 1 日起施行）
 - [2] 《医疗卫生机构开展研究者发起的临床研究管理办法（试行）》 国家卫生健康委(2021 年 9 月 9 日发布)
 - [3] 《国务院办公厅关于加快推进重要产品追溯体系建设的意见》（国办发〔2015〕95 号）
 - [4] 《临床试验的电子数据采集技术指导原则》 食品药品监管总局（2016 年第 114 号）
 - [5] 《疫苗临床试验质量管理指导原则（试行）》 国家食品药品监督管理总局（食药监药化管〔2013〕228 号）
 - [6] 《药物临床试验数据管理与统计分析计划指导原则》 国家药品监督管理局（2021年第63号）
 - [7] 《临床试验数据管理工作技术指南》 国家药品监督管理局（2016年第112号）
 - [8] 《生物等效性试验电子化记录技术指南（征求意见稿）》 国家药品监督管理局食品药品审核查验中心(2024)
 - [9] GB/T 25069-2022 信息安全技术
 - [10] ICH. ICH E6(R3): Guideline For Good Clinical Practice E6(R3)（2025）
 - [11] FDA.《临床试验中使用的计算机化系统的指导原则》（2007）
 - [12] FDA.《临床研究中的电子系统、电子记录和电子签名：问与答》（2023）
-