ICS 11.020
CCS C 07

团　　体　　标　　准

T/CGCPU 031-2025

疫苗临床试验电子源数据系统技术要求与应用规范

Technical requirements and application specifications for electronic source data systems in vaccine clinical trials

2025-08-14 发布　　2025-08-15 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

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、高招、邵杰。

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增多，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技术要求与应用规范

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要求、功能规范及全生命周期应用和管理要求。

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）；

——系统服务供应商等。

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，均可参考本标准的规定，确保系统建设、应用及数据管理的规范性、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

GB/T 25069—2022 信息安全技术 术语

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

3 术语和定义

GB/T 19000—2016、GB/T 25069—2022 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

以人体（患者或健康受试者）为对象的临床试验

注：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

电子源数据 electronic source data

使用电子采集工具初次或从源头采集的、未经处理的电子化方式记录的数据

3.4

疫苗临床试验电子源数据系统 electronic source system for vaccine clinical trials

用于直接采集、存储和管理疫苗临床试验源数据的计算机系统

3.5

权限控制 access control

按照**临床试验**（3.1）计算机系统的用户身份及其归属的某项定义组的身份来允许、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

一系列有关计算机操作系统、应用程序及用户操作等事件的记录

注：包含记录数据的录入、修改、删除和访问历史，审计日志应包含时间戳、用户标识、操作类型和具体内容，用以帮助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。

3.7

逻辑核查 edit check

临床试验（3.1）数据输入计算机系统后对数据有效性的检查

注：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**电子源数据**（3.3）系统变更过程的控制

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（3.3）系统用户进行的一种检测方式

注：检测记录可用以证明所设计系统经过了相关的验证过程。用户应全面检测所有正确和错误数据组合，记录检测结果。

3.10

源数据审查 source data review

在**临床试验**（3.1）过程中，对源数据和源文件进行系统性审查的活动

3.11

电子表卡 electronic card

临床试验（3.1）中，以电子化形式设计，用于记录和管理研究数据的结构化数据收集表单

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 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。

4.3 可控性

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，并密切关注受试者权益与隐私保护。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，应具有源数据维护和保存权限，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，避免申办者或第三方独自控制源数据系统。

4.4 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。

4.5 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《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》《药物临床试验质量管理规范（GCP）》《疫苗管理法》等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。

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，需对 CRO 职责履行情况进行有效监管及评估。

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约定的相关职责内容，包括（但不限于）：

——电子表卡设计及更新；

——临床试验数据库建立、更新及版本控制；

——用户接受测试（UAT）的执行与确认；

——源数据审查（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，包括提供可用的终端设备、网络资源等。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：

a) 组织系统和设备使用培训，确保研究团队规范操作系统；

b) 组织实施用户接受测试；

c) 用户权限审批与管理；

d) 数据传输、迁移、销毁、锁定与解锁批准等。

——数据安全管理：

a) 本地服务器部署及日常维护；

b) 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，包括（但不限于）：

——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；

——接受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；

——备份电子源数据等。

5.5 伦理委员会

伦理委员会应依据《涉及人的生命科学和医学研究伦理审查办法》及相关法规对临床试验项目应用的电子源数据系统进行独立审查。审查内容包括（但不限于）：

——电子表卡设计，如知情同意书、日记卡、原始记录本等；

——系统验证及认证情况，如计算机系统验证情况、网络安全等级保护认证情况等；

——数据安全管理，如数据访问安全、使用范围、备份与恢复等；

——受试者隐私保护，如隐私数据收集、传输、存储、查阅等。

5.6 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，包括协助完成临床试验机构服务器部署、系统部署或配置、数据迁移/销毁等，并与委托方签订具有法律约束力的技术服务协议。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采取相应的修复措施，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，依据《中华人民共和国药品管理法》《中华人民共和国疫苗管理法》《药物临床试验质量管理规范（GCP）》等相关法律法规，服务供应商应承担相应责任。

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管理员，根据参与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；

——计算机系统账户及电子签名声明；

——计算机系统使用相关培训和考核记录；

——计算机系统盲态维持权限规定文件等。

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管理机制，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，确保临床试验全过程数据可追溯，标识符包括（但不限于）：

- 数字编码；
- 一维码；
- 二维码。

——隐私数据采集应遵循最小化且必要原则，采集范围限于临床试验目的必需的个人信息；

——隐私数据访问应建立权限控制机制，限制不必要的用户对隐私数据的访问；

——临床试验机构还应建立数据保密程序，包括（但不限于）：

- 保密约定；
- 账户安全措施；
- 操作人员保密培训。

6.3 试验过程信息化管理范围

疫苗临床试验实施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（但不限于）：

a) 知情同意：构建研究者与受试者在线知情同意全流程管理平台，完整记录知情宣讲、互动问答、知情同意书签署及身份核验等关键操作；

b) 随访流程管理：实现疫苗临床试验从入组到出组全流程随访记录的电子化，完整记录受试者基本信息、筛选与体检、随机入组、样本采集和疫苗接种等随访数据；

c) 电话访视管理：通过移动端进行电话访视，自动生成通话记录，并同步录入访视获知的信息；

d) 安全性信息收集与报告：为受试者提供数字化报告工具（如电子日记卡），实时填报接种后不良事件及合并用药情况；

e) 病例收集与报告：实现终点病例监测、收集、报告等关键环节的数据管理；

f) 样本/疫苗管理：实现样本/疫苗交接、存储及出入库等全流程操作的电子化记录。

6.4 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：

a) 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；

b) 接入仪器设备应符合国家行业标准及系统兼容性要求；

c) 仪器设备与电子源数据系统之间的接口需经过验证；

d) 仪器设备应具备唯一编码标识，运行期间应定期进行检查、维护及异常报备；

e) 仪器设备档案需完整记录交接、安装调试、校准维护及报废处置等信息。

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明确规定。

6.5 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（SOPs）或管理要求，确保系统开发至退役各环节操作合规、数据可靠。标准操作规程应明确各方职责并包括（但不限于）：

a) 计算机系统全生命周期：

- 系统开发、测试、验证、维护、变更及退役；
- 数据迁移、备份与恢复；
- 问题处理、安全管理制度、应急预案等。

b) 计算机系统应用生命周期：

- 数据库构建、上线使用、变更控制、锁定与解锁；
- 系统培训、用户接受测试、权限控制；
- 系统关联仪器设备安装与管理等。

c) 电子源数据管理：

- 数据采集、传输、迁移、销毁；
- 数据保存与归档等。

6.6 质量管理

申办者及研究者应对系统应用与数据管理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，确保系统运行可靠、应用合规、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，覆盖电子源数据系统评估与选择、数据库构建、用户接受测试、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) 建立系统应用及数据管理相关的标准操作规程（见 6.5），并不定期更新；

c) 对可能影响数据质量的环节，如数据采集设备、逻辑核查规则、权限管理及变更控制等实施常态化质量监控或检查；

d) 对临床试验电子源数据执行完整性、可靠性质量控制活动，发现问题应闭环整改。

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遵循《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》《GBT+29832-2013 系统与软件可靠性》等法规及行业标准，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实时性要求，配备负载均衡及冗余容错机制，全年服务可用率不低于 99.9%（即全年宕机时间应≤8.76 小时）；

b) 系统应具备可靠性灾备能力，数据异地实时备份，灾备恢复应支持全量恢复，恢复时间目标（RTO）≤4 小时；

c) 系统应具备自动生成且带有时间标记的审计追踪功能，任何人不得删除、修改、覆盖或关闭；

d) 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；

e) 系统上线前需完成计算机系统验证，并在整个生命周期内都保持其验证状态。

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》等法规及行业标准。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通过 ISO 27001 信息安全管理体系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：数据传输宜通过 TLS 1.2 及以上版本加密通道协议进行保护；数据存储应建立备份与恢复机制，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；

d) 运维安全：系统供应商应建立数据安全管理制度，实时监测网络攻击、异常访问行为及潜在安全威胁，安全事件处置记录应完整、准确，保存期限不低于 10 年。

7.3 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：

——计算机系统验证应由系统服务供应商或第三方独立机构实施；

——验证范围覆盖需求、设计、开发到退役全生命周期，验证阶段和内容包括：

a) 计划阶段：进行系统影响性评估及风险评估，制定验证计划；

b) 设计阶段：审核系统设计文档，执行设计确认（DQ），确保设计符合用户需求。系统设计文档主要包括：

- 用户需求说明（URS）；
- 系统功能说明（FS）；
- 系统设计说明（DS）；
- 系统配置说明（CS）。

c) 确认与测试阶段：按验证计划执行测试，测试过程需完整记录（如测试脚本、测试结果、测试报告），核心测试内容包括（但不限于）：

- 安装确认（IQ）；
- 运行确认（OQ）；
- 性能确认（PQ）；
- 单元测试/集成测试等。

d) 报告阶段：汇总验证结果，形成验证报告。

——系统上线运行过程中应定期进行周期性回顾/审查，确保系统持续保持验证状态；

——如发生系统变更，应基于风险评估变更对系统及数据的潜在影响，必要时进行再确认或再验证；重大变更后需实施专项验证。

7.4 备份与恢复

电子源数据系统应进行异地备份和本地备份，备份与恢复应遵循《GB/T 20988-2007 信息系统灾

难恢复规范》等法规及行业标准要求。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：

——备份机制

- 数据实时备份，其中增量备份恢复点目标（RPO≤15分钟），全量备份周期不得超过7天；
- 异地灾备中心与主中心应满足地理隔离≥500公里要求。

——灾备恢复能力

- 系统整体恢复时间目标（RTO≤4小时）、恢复点目标（RPO≤1小时）；
- 关键业务数据恢复时间目标（RTO≤4小时）、恢复点目标（RPO）≤15分钟。

——应急响应

- 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作；
- 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。

7.5 审计追踪

电子源数据系统应具有安全、完善的审计追踪功能，完整记录有关系统、应用程序、用户及数据的所有操作记录，审计追踪应符合下列要求：

a) 审计追踪功能在系统首次安装后自动开启，任何人不得删除、修改以及关闭审计追踪；审计追踪包括（但不限于）：
   - 数据创建、修改、删除、再处理、重新命名、传输、迁移、销毁；
   - 文件创建、修改、删除、重命名；
   - 用户每次登录时间、IP地址、操作内容和操作者，以及试图访问系统的行为；
   - 系统用户及权限的创建、变更、删除；
   - 对系统的设置、配置、参数及时间戳的变更或修改等；

b) 审计追踪由系统自动生成，并带有时间戳，可以追溯到个人；

c) 审计追踪记录需安全存储，任何记录的变更都不得掩盖先前记录的信息；

d) 审计追踪应记录系统操作的相关信息，至少包括操作者、操作时间、操作内容、操作过程、修改原因。数据的修改应完整记录修改时间、修改人、修改原因、修改前数据值、修改后数据值。

7.6 权限控制

电子源数据系统应具备完善的权限管理机制，并符合《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》等相关法规及行业标准，保障数据访问安全。权限控制应符合下列要求：

a) 开通电子源数据系统的账户，需经过授权，未经授权的人员不能访问系统；

b) 每个用户应有独立的账户，禁止使用通用账户、账户共享或转交他人使用；

c) 用户角色应分级管理，角色权限应预先定义并符合相关法规要求。常见的角色及权限包括（但不限于）：

- 系统管理员：系统维护、日志管理等；
- 权限管理员：负责角色和账户权限管理，不可操作试验数据；
- 主要研究者：最高数据操作权限，对权限管理进行监管；
- 现场研究者：数据录入和修改，处理数据质疑；
- 质控员：只读权限，对数据进行质控并发布质疑，不可操作试验数据；
- 申办者：只读权限，不可操作试验数据；
- 临床监查员：只读权限，审查数据并发布质疑，不可操作试验数据；
- 稽查/监管账户：只读权限，不可操作试验数据。

d) 用户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；

e) 用户身份认证宜采用双因素验证，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；

f) 系统应对非法登录次数进行限制，同一账号连续失败登录次数不得超过 5 次，超过后自动锁定账号；

g) 系统长时间空闲或短时间暂停工作时应实行自行断开连接，时长不超过 15 分钟；

h) 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。

7.7 电子签名

电子签名功能应符合《中华人民共和国电子签名法》《21 Code of Federal Regulations Part 11》等法规要求，具体要求如下：

——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；

——用户在首次使用电子签名前应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《中华人民共和国电子签名法》要求。

7.8 逻辑核查

电子源数据系统应具备完善的逻辑核查校验功能，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：

——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；

——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；

——操作日志应完整记录逻辑核查提示及数据修改轨迹。

7.9 数据审查

电子源数据系统应具备源数据审查（SDR）模块，支持审查标记及数据质疑生成功能。临床监查员可以现场或远程审查临床试验电子源数据（包括经医学编码后的数据），数据审查应符合下列要求：

a) 临床监查员应依据相关法规要求进行数据审查，发现异常问题可以通过数据质疑功能发布给研究者，并对异常问题进行跟踪处理；

b) 数据审查应实施基于角色的权限控制，确保仅授权人员可以审查数据；

c) 隐私数据应遵循最小化权限原则，仅访问与监查目的直接相关的隐私数据；

d) 审查日志应完整记录审查人员、审查时间、审查内容及审查结果，保存期限不得低于临床试验数据留存时限。

7.10 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并回复质疑，更正数据需追加电子签名并标注修改原因；

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。

7.11 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，变更应建立变更管理规程，包括变更申请、评估、审批、测试验证、批准实施及文档归档全流程。变更管理规程应严格执行，确保系统变更得到有效控制。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、篡改、不可读或逻辑冲突；

b) 变更实施前需进行风险评估，评估对系统功能、性能及数据安全与可靠性的潜在影响，基于风险制定变更控制措施并确定再验证的范围；

c) 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；

d) 变更实施过程应进行记录与监控，确保变更结果符合预期；

e) 变更后应及时告知系统使用人员，必要时更新文档和培训人员；

f) 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。

临床试验实施过程中，出现系统变更导致数据采集发生变化的风险或可能性时，变更前还应书面通知研究者和申办者，在获得研究者和申办者书面同意后方可进行变更。系统变更可能影响数据采集时，应提前30天书面通知系统采集方。

7.12 系统退役

电子源数据系统退役管理应符合下列要求：

a) 系统退役前应制定退役计划，明确退役方法、历史数据的处理要求、退役时间、风险评估及应急措施等；

b) 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；

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 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）》及数据质量标准要求，以确保数据真实、完整、准确。源数据应当记录或可呈现数据来源，主要包括人工录入和自动数据采集。人工录入数据应符合下列要求：

a) 人工录入数据由研究者、受试者或其他授权人员录入，必要时进行电子签名，系统应记录录入的详细信息、录入人身份和录入数据。常见的人工录入数据包括：

- 受试者原始评估记录（如受试者日记卡、受试者自评报告）；
- 对不具备接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。

b) 数据采集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；

c) 人工将纸质记录信息录入计算机系统时，应当可追溯到保留原记录数据的纸质记录；

d) 所有人工录入的关键数据应经过第二人核查或通过计算机系统进行逻辑校验；

e) 数据修改应完整记录修改前数据值、修改后数据值、修改原因、修改时间、修改人及修改人的电子签名（如有）。

自动数据采集通过仪器、设备或信息系统（如实验室信息管理系统（LIS））直接生成，并满足以下要求：

a) 接口验证：原始系统、数据采集与记录系统之间的接口应经过验证；

b) 数据记录：数据应实时、准确记录，并显示正确的时间戳；系统时间应与当前国家标准时间同步；

c) 数据存储：采集的数据应以不易被篡改、修改或丢失的格式存储，并符合长期存储要求。

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、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系统中，应严格遵循《药物临床试验质量管理规范（GCP）》等法规要求及行业数据安全标准，确保数据传输从采集端到目标端的安全、可靠、可追溯。数据传输应符合下列要求：

a) 计算机系统之间接口传输应经过验证，断点续传机制应保障数据零丢失与一致性；

b) 数据传输前，临床试验参与各方应制定数据传输协议，明确下列内容：

- 数据传输方法和频率；
- 外部数据结构与内容；
- 数据传输方式；
- 数据传输时间；
- 数据传输流程等。

c) 数据传输应事先定义数据传输所需的数据点及相对应变量，形成完整的变量列表；

d) 数据传输应采用统一的数据标准和格式，确保数据的一致性和可比性；

e) 数据传输需进行全面且充分的测试，外部数据库或数据库结构改变后，应重新进行测试；

f) 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

数据迁移应参照《GAMP®5: A Risk-Based Approach to Compliant GxP Computerized Systems》《GBT+37740-2019 信息技术 云计算 云平台间应用和数据迁移指南》等法规及行业标准，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) 数据迁移前应进行风险评估，根据评估结果制定迁移计划，迁移计划包括迁移数据范围、迁移目标、人员及时间、迁移工具、迁移方法以及回退方案等，经主要研究者及申办者书面批准后实施；

b) 迁移实施前应完成数据全量备份，备份数据需通过《GBT+30285-2013 信息安全技术 灾难恢复中心建设与运维管理规范》中完整性和一致性验证；

c) 迁移过程中应暂停使用系统，迁移后数据一致性验证错误率应≤0.01%；

d) 迁移审计日志应记录操作人员、操作时间、迁移数据内容及迁移位置，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

数据销毁应符合《药物临床试验质量管理规范（GCP）》《工业和信息化领域数据安全管理办法（试行）》及《GBT+31500-2024 网络安全技术 存储介质数据恢复服务安全规范》等法规及行业标准，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) 数据销毁应建立销毁操作规程，明确数据销毁流程、执行人员和销毁方式等要求；

b) 销毁计划应明确销毁数据范围、销毁方式及执行人员等，并经主要研究者与申办者书面批准；

c) 数据销毁应由授权的执行人员进行操作，监督人员全程监督并对销毁过程记录进行确认。销毁过程应全程视频监控，相关记录留存备查；

d) 销毁方式应采用不可逆删除技术（如物理消磁、安全擦除方式），确保数据不可恢复；

e) 销毁记录应包含数据清单、销毁方法、操作人员及操作时间等，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 电子表卡设计

疫苗临床试验中需要将每个受试者或某个试验模块的数据以规范化的格式进行收集的，应根据临床试验方案或项目要求设计电子表卡。常见的电子表卡包括（但不限于）：

a) 电子知情同意书；

b) 电子日记卡；

c) 电子原始记录本；

d) 安全性随访记录表。

电子表卡应由研究者与申办者（或合同研究组织）联合设计及更新，其设计和更新应符合下列要求：

a) 电子表卡内容应符合《药物临床试验质量管理规范（GCP）》《涉及人的生命科学和医学研究伦理审查办法》等法规要求；

b) 数据采集项需完全覆盖临床试验方案规定的全部访视点和访视数据，或覆盖临床试验操作全过程节点数据，确保临床试验全过程可追溯；

c) 隐私数据字段应标注敏感标识，采集范围限定于临床试验方案必需的最小数据集；

d) 临床试验方案变更导致电子表卡中访视内容、访视节点或数据点更新的，应同步更新电子表卡。

9.1.2 数据库构建

临床试验数据库由建库人员依据临床试验方案及电子表卡进行构建及更新，数据库构建应符合以下要求：

——数据库结构应符合 CDISC CDASH/SDTM 通用的数据格式标准；

——数据库构建前，应预先对所需采集的数据点进行定义，形成数据库设计说明。数据库定义内容包括（但不限于）：

- 数据集名称；
- 变量名称；
- 变量类型；
- 变量规则。

——数据库构建后，符合伦理委员会审查内容的电子表卡（包括但不限于电子知情同意书、电子日记卡）需递交伦理委员会审查批准/备案。获批后的任何变更应重新递交伦理委员会。

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：

——逻辑核查规则应与临床试验方案规定或项目要求相符；

——逻辑核查范围包括（但不限于）：

- 必填项缺失；
- 数值阈值超限；
- 时间逻辑冲突；
- 事件先后顺序；
- 跨表单数据一致性或逻辑性。

9.1.4 填写指南

数据库构建后，研究者或申办者（或合同研究组织）可以根据源数据采集内容及需求制定数据填写指南（如数据录入指南、系统在线帮助/提示等），明确数据填写规则、数据采集和数据修改规范等，内容应清晰易懂。

9.1.5 人员培训

所有用户（含研究者、临床监查员）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等更新后，适用范围内的人员应重新进行针对性培训。

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) 测试内容包括（但不限于）：
   - 数据库测试：验证访视内容和顺序、数据字段等与临床试验方案及项目需求的一致性；
   - 逻辑核查测试：模拟正常/异常数据输入，核查系统提示触发的准确性及质疑闭环流程；
   - 数据传输测试：依据传输协议验证数据格式、传输完整性及接口稳定性；
   - 设备使用测试：验证系统接入设备的兼容性与功能完整性。
d) 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。

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，确认数据库和逻辑核查设计符合需求并通过用户接受测试，所有设计和测试文档已完成签字后，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 角色和账户管理

电子源数据系统角色和账户权限管理应由主要研究者授权的非数据利益相关人员担任，权限管理员不得同时兼任数据采集或录入职责。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或主要研究者授权的管理人员书面批准；

b) 权限分配应遵循最小权限原则，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非盲态数据；

e) 权限管理员应定期（如每季度）对账户使用状态进行审查，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 源数据采集/录入

临床试验过程中，由研究人员在临床试验现场采集的电子源数据（如随访数据）应符合下列要求：

a) 数据采集的研究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开通数据采集权限；

b) 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；

c) 数据录入后如发现错误或不完整时，研究者应及时修正数据。数据修改权限仅限原始录入者或经同等授权的研究者；

d) 临床试验数据采集应在授权的临床试验现场完成，数据采集专用计算机宜采用物理网卡（MAC 地址）白名单或 VPN 拨号认证等措施来限定数据录入终端的物理位置；

e) 使用研究专用计算机进行源数据采集的，条件允许的前提下，宜对源数据采集全过程进行影像记录（如系统自动录制功能或安装第三方录屏软件等），影像视频应定期备份；

f) 临床监查员应对研究者录入的数据进行审查，确保源数据的产生和修改符合相关法规及ALCOA+质量标准。数据修改后应经临床监查员复核确认。

9.2.3 数据库变更控制

临床试验项目上线后，应对数据库变更（如数据库结构修改、逻辑核查更新等）进行严格控制，变更控制应符合下列要求：

a) 数据库变更应确保原有数据完整无误；

b) 数据库变更前，临床试验相关方应对数据库的变更进行风险评估，经主要研究者和申办者批准同意后执行变更；

c) 数据库变更后应对更改部分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；

d) 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，当试验数据完成录入和审查，质疑已被关闭，锁定清单所有任务均已完成，经主要研究者和申办者的书面批准后对临床试验数据库进行锁定，数据库锁定前应通知试验相关用户。

9.3.2 数据库解锁

数据库锁定后一般不得随意解锁，当发现错误时可以补充数据错误/不完整的说明文件。

如出现重要数据问题需解锁数据库，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，解锁记录应存档备查。

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：

a) 文件应归档在授权的安全区域或设备内，存储环境应受控，并做好防火、防盗、防潮等安全措施，确保符合长期保存要求；

b) 数据应以可检索和可读的方式存档，归档格式应符合《临床试验数据管理工作技术指南》等法规要求；

c) 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；

d) 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；

e) 使用电子源数据系统实施的临床试验，除符合《药物临床试验必备文件保存指导原则》规定的临床试验文件外，还需保存以下的文档（但不限于）：

1) 系统技术支持服务协议或合同；

2) 系统验证文件；

3) 系统应用和管理相关的 SOP 及应急预案；

4) 数据库构建的全套内容；

5) 逻辑核查文件；

6) 空白的电子表卡（PDF 格式）；

7) 系统用户手册；

8) 填写指南；

9) 申办者和研究者的培训证明文件；

10) 用户接受测试文件；

11) 数据传输、迁移、销毁相关文件；

12) 账户及电子签名声明；

13) 系统上线和再上线批准文件；

14) 系统角色权限表、账户审批及权限管理记录；

15) 系统相关设备管理记录（设备交接、安装与调试、维护等）；

16) 临床试验影像记录（如数据采集过程影像录制视频等）；

17) 研究过程中的变更控制的测试文件与再上线通告；

18) 每个受试者完整的电子知情同意书/日记卡/原始记录本等（PDF 格式）；

19) 数据库锁定与解锁相关文件；

20) 审计追踪；

21) 研究过程中的应急计划的相关文件；

22) 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》国家药品监督管理局 国家卫生健康委（ [2020]第 57 号）

[2] 《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）

[3] 《临床试验的电子数据采集技术指导原则》国家食品药品监督管理总局（2016 年第 114 号）

[4] 《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）

[5] 《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）

[6] 《临床试验数据管理工作技术指南》国家食品药品监督管理总局（2016 年第 112 号）

[7] 《药品记录与数据管理要求（试行）》国家药品监督管理局（2020 年第 74 号）

[8] 《涉及人的生命科学和医学研究伦理审查办法》国家卫生健康委、教育部、科技部、国家中医药局（国卫科教发〔2023〕4 号）

[9] 《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)

[10] 《ICH E6(R3)：Guideline For Good Clinical Practice E6(R3)》ICH（2025）

[11] 《21 Code of Federal Regulations Part 11》FDA（1997）

[12] 《Guidance for Industry: Computerized Systems Used in Clinical Investigations》FDA（2007）

[13] 《GAMP®5: A Risk-Based Approach to Compliant GxP Computerized Systems》ISPE（2022）

[14] 《Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Questions and Answers》FDA（2023）