# 药物临床试验计算机化系统和电子数据指导原则

# （征求意见稿）

国家药品监督管理局药品审评中心

2025 年 11 月

# 目 录

## 一、概述

### （一）背景

临床试验数据质量是科学评价临床试验结果的基础，随着临床试验的发展和科学技术的不断进步，包括计算机、网络、移动设备和软件等的发展为临床试验的规范化和现代化提供了新的技术支持，也推动了对临床试验新模式的积极探索。

2025 年 1 月，ICH 发布 ICH E6(R3)指导原则，其中新增了数据治理章节，并对各类计算机化系统提出了更新的要求，对应于质量源于设计的新理念，要求计算机化系统的使用切合临床试验的目的、设计、实施和管理。为了保证临床试验数据质量，监管机构有必要进一步明确临床试验计算机化系统的使用规范，并对试验中所产生的电子数据提出相应的技术要求。

### （二）适用范围

本指导原则在 ICH E6(R3)指导原则和中国药物临床试验质量管理规范（GCP）要求的基础上，主要阐述在药物临床试验中使用计算机化系统和电子数据的一般要求，旨在对我国临床试验相关工作的开展起到规范化和指导性作用。

本指导原则主要针对用于药物临床试验的计算机化系统，这些系统涉及临床电子数据的生成或采集，以及对可能影响试验参与者保护和试验数据可靠性的其他流程的控制，

例如，作为临床研究源数据的电子医疗记录，电子病例报告表（eCRF），以及用于保存、分析、处理、报告及管理与临床试验相关数据的其他计算机化系统。

本指导原则仅代表药品监管部门当前的观点和认识，不具有强制性的法律约束性。随着科学研究的进展，本指导原则中的相关内容将不断完善与更新。应用本指导原则时，还请同时参考 GCP、国际人用药品注册技术协调会（ICH）和其他国内外已发布的相关指导原则。

## 二、一般考虑

### （一）数据可靠性

数据可靠性是指以安全的方式收集、访问和维护数据，并满足 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、可获得性和可追溯性，从而使数据能够在全生命周期内充分支持稳健的结果和良好的决策。确保数据可靠性需要建立适当的质量和风险管理体系，包括遵循合理的科学原则和良好的文档规范。

### （二）职责划分

临床试验中，申办者和研究者可能使用各自的计算机化系统来保存/管理数据。一般情况下，申办者负责提供、存储和/或管理、运营计算机化系统以及它们生成的记录，研究者负责使用申办者或自己的计算机化系统生成并存储数据，形成记录。

在本指导原则中，“责任方”一般指申办者或研究者。对于用于数据保存和管理的计算机化系统，应以规范、合理的方式把实施职责分配给各参与方，明确界定各方的具体职责，建议参照 GCP 相关要求。若借助第三方服务供应商，其涉及临床试验数据采集、保存和管理等相关活动须一并纳入并书面约定。

（三）风险管理

建立基于风险的质量管理体系非常必要。风险管理应当与风险对试验参与者权益、安全和福祉，以及对试验结果可靠性影响的重要性相称，并确保数据在全生命周期的全流程中的风险都得到关注和控制。风险管理应从体系和项目执行两个层面来确定风险点。体系层面应涵盖标准操作规程（SOP）、计算机化系统和人员等相关的内容。项目执行层面应包括临床试验采集的数据、采集流程、数据采集工具及项目特定的系统设置和定制等内容。

使用计算机化系统时，涉及保障数据真实性相关的重大风险会直接影响到试验参与者的权益、安全、福祉和临床研究结果的可靠性。识别风险时应全面关注系统生命周期的各个阶段，并考虑所使用系统的用途、所采集和管理的数据特点、系统的复杂性、操作人员的经验等内容。

（四）数据采集

临床试验方案中应明确需要收集的数据内容和数据采

集的过程，如数据采集方、采集时间点和使用的工具。方案或相关文件中应包括电子数据传输的流程图和相关描述。

申办者应描述需要传输的数据及其来源、格式、接收方、数据权限，以及数据验证、核对、审阅等工作。在临床试验过程中将采集的数据录入计算机化系统时，应当附带相应的元数据，包括稽查轨迹。

申办者应当确保数据处理和分析过程中数据传输和导出的可追溯性。

数据采集工具应只采集临床试验方案中规定的数据，不能超出方案规定的内容。除需要依靠计算生成的数据，数据点录入一般不应设置为自动录入的形式。

**（五）系统验证**

临床试验中使用的计算机化系统应有确定系统始终处于被验证状态的流程，以满足其特定的使用要求。系统验证应确保计算机化系统在整个过程中准确、可靠并能稳定运行。

系统验证的流程应由责任方决定并记录。责任方应监督服务供应商，以确保其确立了恰当的验证规程并按照规程规定完成了系统验证工作。验证方法应在基于风险评估的基础上制定，应考虑到系统用途，对试验参与者的保护和试验结果的可靠性的潜在影响。

责任方应保存系统验证相关文件，以证明系统处于被验证状态。计算机化系统自身的验证和临床试验特定的配置都

应有相应的验证文档。

系统验证应确保临床试验特定的配置符合临床试验方案的要求并经过了全面严格的测试。

## 三、计算机化系统

### （一）应用规程

责任方应建立内部 SOP，以确保计算机化系统的正确应用。这些规程应由责任方管理与维护。

### （二）培训

参与开展临床试验的每位人员都应具备相应的教育背景、培训经历和实践经验，例如申办者、研究者或服务供应商。对于参与开发、编码、构建以及在临床试验过程中配置、定制、或管理临床试验计算机化系统的人员，应进行相关法规、指导原则的培训。

所有培训都应记录在案，并保留记录以供监查、稽查和检查。

### （三）安全性

为了保护试验参与者的权益和维护数据可靠性，临床试验中使用的计算机化系统应具有安全流程和功能，并覆盖数据全生命周期。为防止未经授权的访问和不必要的数据更改，应进行定期检查。应保存系统访问权限的记录，并清晰记录相应的访问权限级别、以及用户角色、访问权限的变更。应有关于安全重要性的培训记录，例如保护密码和保密的必要

性、安全系统和流程的执行、安全事件及网络钓鱼的识别和处理等。应当对计算机化系统产生的试验数据及时备份，并在系统故障时采取应急措施，防止数据丢失或无法访问。

（四）验证

1.一般原则

责任方应确保系统在整个生命周期的验证状态，并证明符合要求。如果责任方已评估系统供应商执行的验证活动及相关文件充分，则责任方可以依赖系统供应商提供的验证文件；但是，责任方需评估是否还需要开展额外的验证活动。责任方对临床试验中使用的计算机化系统的验证承担最终责任。

2.用户需求

应在用户需求或用例中描述临床试验中实施和使用的关键系统功能。关键系统功能中应涵盖所有所需功能，以确保试验符合 GCP 标准，并以确保数据可靠性的方式采集、分析、报告和归档临床试验数据。用户需求应包括但不限于操作、功能、数据可靠性、技术、界面、性能、可用性、安全性和法规要求。以上内容独立于责任方的采购策略或系统开发流程。在相关的情况下，用户需求应构成系统设计、购买、配置和定制的基础；但无论如何，它们都应构成系统验证的基础。责任方应采纳并完全负责用户需求，无论这些需求是由责任方、供应商还是服务供应商记录的。责任方应审查并

批准用户需求，以验证其是否描述了用户在其特定临床试验中所需的功能。当系统功能发生变化时，应在整个系统生命周期内维护和更新用户需求。

3.试验特定配置与定制

用于特定临床试验的系统配置和定制需求应预先制定并详细记录，并验证其与临床试验方案、数据管理计划等其他相关文件的一致性。试验特定的配置和定制应在生产环境发布前进行质控与测试（如适用）。建议让用户参与相关测试活动。同样的流程也适用于方案修订所需的修改。如果需要开发新的功能或接口、或者添加新的代码，则应在使用前进行验证。

4.需求的可追溯性

应建立并维持每个用户需求与测试用例或其他文档（例如 SOP）之间的可追溯性（如适用）。这种可追溯性可以有多种形式，并且可以通过软件实现流程自动化。如果根据需求进行软件更新，更新内容应有相应测试和验证，并作风险评估后使用。

5.验证和测试计划

临床试验计算机化系统的验证活动应有相应的计划、记录和批准过程。验证计划应包括验证方法、所采取的基于风险的方法以及责任方与服务供应商之间的任务分工（如适用）的信息。在测试之前，风险评估应定义与关键系统功能相关

的需求与测试项。

测试用例应预先获得批准。可能有多种格式，包括文本文档组、电子表格、或者被设计并包含在专用的测试管理系统中、甚至可能是自动执行的测试用例。但是，对关键要素的要求是相同的。

测试用例应包括：1）测试的软件版本；2）进行测试前的任何先决条件；3)测试功能所采取的步骤(录入)的描述；4）预期结果（验收标准）。

测试用例应要求测试人员记录测试步骤中看到的实际结果、证据(如果相关)以及测试步骤的结论(通过/失败)。如果可能，应尽量避免测试用例的制定人员与实际测试人员为相同人员。如果测试失败，应评估潜在影响，并记录有关偏差评估情况以及后续决定。

6.测试执行与报告

临床试验计算机化系统测试的执行应遵循经批准的验证方案与测试用例，应记录被测试软件的版本，并且在执行测试用例的过程中保留证据（例如：屏幕截图）以记录测试步骤和结果。如相关，应记录测试人员使用的测试角色、或自动测试工具的身份。在系统验证过程中遇到的偏差应进行记录并在解决或者采取缓解措施后关闭。应评估系统发布时所有未解决的偏差和任何已知问题，后续决策应记录在验证报告中，验证报告应经责任方批准后再投入使用。

（五）系统发布

临床试验的计算机化系统在完成相关的验证测试后需完成责任方签署批准方可正式投入使用。同时，相关的培训材料、用户指南、以及用户使用所需的相关资料应在系统发布至正式环境时一并提供。

系统发布后，如有系统升级迭代，仍需遵循上述验证要求进行验证与测试后方可正式执行升级。

（六）系统故障

1.制定应急规程

责任方应制定应急规程，以防止对试验参与者安全性、试验决策或试验结果至关重要的数据丢失或缺乏访问。

应通过系统设计（如冗余配置、容灾备份）和预防性维护计划，最大限度降低系统故障风险。

必须制定书面化的应急计划（如业务连续性计划），明确系统故障时的备用流程（如临时使用经批准的替代记录方式）、数据恢复策略和沟通机制。

2.故障识别与报告

责任方应建立有效的系统故障识别机制，确保用户能够及时发现并报告故障情况，报告内容应包括故障发生的时间、具体表现、影响范围等详细信息。

应设立专门的故障报告渠道，如帮助台电话、在线故障报告系统等，方便用户随时提交故障报告。

3.故障分类与优先级划分

责任方应对系统故障进行分类，如硬件故障、软件故障、网络故障等，并根据故障类型和对临床试验的影响程度划分优先级，明确各优先级故障的响应时间和处理时限要求，优先处理可能影响数据准确性、完整性或危及试验参与者安全的高优先级故障。

4.故障处理规程

责任方应制定完善的故障处理规程，包括故障的初步诊断、问题定位、故障修复、数据恢复和系统测试等环节，确保故障处理过程有序进行。在故障处理过程中，如需对系统进行紧急修复或数据恢复操作，应遵循严格的变更控制规程，确保所采取的措施不会对系统的完整性和数据的可靠性造成新的风险。

故障恢复后，必须评估其对系统的完整性、数据的可靠性和试验参与者安全的影响。

关键系统故障后，必须重新验证受影响的系统功能或模块，确保其恢复后仍符合预期用途和 GCP 要求。

5.备份与恢复策略

责任方必须建立并定期测试可靠的备份与恢复规程，确保在故障或灾难情况下，关键试验数据可在可接受的时间内恢复至与故障前一致的状态。

应制定详细的系统恢复策略，明确在不同故障场景下的

恢复步骤和方法，定期进行备份数据的恢复测试，验证备份数据的有效性和恢复流程的正确性。

（七）技术支持

1.技术支持机制

责任方应设置适当的机制，如使用帮助台来报告、记录和管理计算机化系统的问题，并且应定期审查累积的问题，以识别重复和/或系统性的问题。

缺陷和问题应根据其关键性予以解决，关键性高的问题应被及时解决。

2.技术支持团队与职责

责任方应组建专业的技术支持团队，团队成员应具备计算机、信息技术、临床研究等相关专业知识和技能，明确各成员的职责分工，包括系统维护、故障排除、用户培训、问题解答等。确保能够为临床试验计算机化系统的正常运行提供全方位的技术支持。

应明确系统供应商和申办者/研究者各自的技术支持职责（如问题报告路径、响应时间承诺、升级流程等），并形成协议或 SOP。

3.技术支持内容与范围

责任方应提供计算机化系统的安装、配置和部署技术支持，确保系统能够按照预定的要求和标准正确安装和运行。负责系统的日常运行维护和技术支持，包括系统性能监控、

系统更新与升级、安全漏洞修复、用户权限管理等。

应对计算机化系统的使用进行培训和技术指导，根据用户的不同角色和权限，制定相应的培训计划和教程，包括系统功能介绍、操作规程演示、常见问题解答等，通过现场培训、在线培训、培训文档等多种方式，提高用户对系统的熟悉程度和操作技能，确保用户能够正确、高效地使用系统完成临床试验相关工作。

4.技术支持文档与资源

责任方应编写详细的技术支持文档，包括系统安装手册、配置指南、用户操作手册、故障排除手册等。

应建立技术支持资源库，收集和整理与计算机化系统相关的技术资料、常见问题解决方案、案例库等。

任何对系统的修改（包括补丁、升级、配置变更）必须遵循严格的变更控制规程(评估、批准、测试、验证、记录)，并评估其对数据可靠性和合规性的影响。

5.供应商管理

若使用供应商系统（包括但不限于如电子数据收集系统（EDC）、电子化临床结局评估工具、医院计算机化系统），申办者仍需承担最终责任，应通过合同或协议确保供应商符合 GCP 要求，并有权访问稽查报告和验证文档。

（八）用户管理

1.用户与权限管理

计算机化系统应当具备完善的用户管理、权限管理和稽查轨迹流程，确保在开始、更改和结束其临床试验项目管理和/或实施中，只有经授权的用户方可访问和使用系统，并且系统可以及时授予、更改和撤销系统访问权限。

只有在收到临床试验的所有必要批准并且所有文件都已到位（例如签署的方案和与研究者签署的协议），才应向经过培训的研究中心用户授予对系统的访问权限。这也适用于系统的任何更新。

用户访问权限的授予必须基于其完成系统使用和 GCP 相关培训的记录，以确保培训的效果。

2.用户权限审核

在任何给定时间，系统都应提供当前和既往访问权限、角色和权限的概览。应定期验证有关实际用户及其系统权限的上述信息，以确保只有已批准的用户才具有访问权限，并且他们的角色和权限是适当的。应及时删除不再需要或不再允许的访问。权限变更应有稽查轨迹或变更记录支持。

3.用户角色与权限分配

应根据职责分配、盲法设置和用户所属组织以及研究者和申办者的责任授予用户的系统访问权限。

具有特权或“管理员访问权限”的用户在系统中拥有广泛的权限，包括但不限于更改任何系统设置、定义或停用用户、激活或停用稽查跟踪功能以及更改稽查跟踪中未采集的数

据。为避免滥用权限，具有特权访问权限的用户应充分独立于临床试验的管理和实施，以及数据的生成、修改和审查，并且不参与其中。非盲信息应仅可供预先定义的用户角色访问。

4.最小权限分配规则

系统访问权限应根据最小权限规则分配，即用户应具有最少的权限和访问权限。

5.个人账户

所有系统用户都应具有个人账户，共享帐户（组帐户）被认为是不可接受的，并且违反了数据可靠性原则，因为数据应该是可归因的。

6.唯一可识别用户名

用户访问权限在系统内和系统的整个生命周期中应该是唯一的。用户名应可追溯到指定的账户所有者。并且账户的用户名和密码应仅使用于对应的计算机化系统，与计算机帐户区分开来。

7.认证与安全

应采用安全的认证机制(如强密码策略、双因素认证)。设置账户休眠期(如 90 天未使用自动停用)，定期审查账户列表。

（九）时间戳

1.时间戳的生成与记录

计算机化系统应具备自动产生时间戳的功能，时间戳应包含日期和时间信息，且时间的精度应能够满足临床试验数据记录和追溯的要求。在数据输入、编辑、保存、传输、报告等各个环节，系统应自动为相关操作记录添加时间戳。

2.时间戳的准确性与同步

责任方应定期对计算机化系统的时间进行校准和同步，采用可靠的时间同步协议和工具，使系统时间与标准时间保持一致。对于多用户、多终端的计算机化系统，应确保所有终端设备的时间同步。对于跨时区试验，系统应能记录事件发生的本地时间和/或转换为协调世界时（UTC），并明确标注时区信息，避免时间混淆。

3.时间戳的保护与完整性

时间戳记录应受到保护，防止未经授权的篡改或删除，确保时间戳的完整性和真实性。

## 四、电子数据

电子数据包括数据与元数据。申办者应确保用于采集、处理、报告和存储电子数据的计算机化系统经过充分验证，并实施适当的技术和组织控制措施。应遵守个人信息保护和数据安全的法律法规，按照其要求执行来确保临床试验数据的保密性。

### （一）数据采集

数据采集的主要目标是收集方案所需的所有数据点，所

有相关观察结果都应及时记录，不得包含非必要字段。每个试验都应明确将收集、修改、导入、导出、归档的电子数据和记录，以及如何检索和传输这些数据。在确保试验参与者身份及数据保密性的前提下，研究者、监查人员、稽查人员以及检查人员应能够直接访问原始电子记录，包括稽查轨迹。

数据采集应在受控环境下进行，确保数据录入者的身份可识别、操作时间可记录，并且系统配置可防止或检测未经授权或意外的数据修改。数据采集过程应遵循 ALCOA++原则。必须基于角色分配系统访问权限，确保只有经授权的人员才能录入或修改数据点。权限分配应有记录。

1.源数据

源数据应在其最初生成的系统或媒介中被采集和保留。必须清晰定义何为特定数据点的原始电子记录。在试验开始前明确指定所有源数据的位置，并在试验进行期间根据需要更新。

2.数据转录

纸质源数据，例如工作表、纸质病例报告表（CRF）、纸质日记或问卷，需要手动或通过验证过的录入工具转录到 EDC 系统或数据库中。当使用纸质源数据时，应建立清晰、受控的规程将其转录至计算机化系统，并确保转录的准确性和可追溯性。

在手动转录的情况下，应实施基于风险的方法以确保转

录数据的质量，如双重数据输入和/或数据监查。

3.逻辑核查

计算机化系统应验证手动和自动数据输入，以确保数据输入符合预定义标准。逻辑核查应与方案相关，并根据需要开发、修订、验证，并控制和记录单个逻辑核查的实施情况。如果在试验期间的任何时间变更或暂停逻辑核查，应记录并说明理由。逻辑核查可在数据输入时立即运行，也可以在规定的时间间隔（例如每天）自动运行，也可以手动运行。

逻辑核查应该以必要性为前提，不应导致偏倚，并且应该是可追溯的，例如因逻辑核查通知而发生的数据更正。

4.直接采集

鼓励使用电子数据输入设备和应用（如电子日记、eCRF）进行直接数据输入。也可通过与数据采集工具直接连接的自动化设备（如可穿戴设备、实验室或其他技术设备）进行。此类数据应附带有关所用设备的元数据，如设备版本、设备标识符、固件版本、最后校准、数据发起者、事件的时间戳等。

（二）稽查轨迹

所有电子数据的原始创建和后续修改都应启用稽查轨迹以独立记录与数据创建、修改或删除相关的操作。稽查轨迹应存储在系统内部，必须由计算机生成并带有时间戳。稽查轨迹记录本身必须受到充分保护，以防止更改、删除和访

问修改（例如编辑权限、可见性权限）。

稽查轨迹对于确保数据变更可追溯至关重要。稽查轨迹功能必须始终开启，仅“管理员用户”可操作该功能。如果可能，对于由“管理员用户”停用的稽查轨迹，应自动在日志文件中记录。

稽查轨迹应在实时系统中以数据点级别可见，并应能够将整个稽查轨迹导出为动态文件，包含自动处理功能且可支持与用户的交互操作，以便识别试验参与者、研究中心等数据中的系统性问题。用于内部报告和统计分析的数据提取或数据库提取不一定需要包含稽查轨迹信息。但是，数据库稽查轨迹中应该记录数据提取和导出的生成过程。对于数据库锁定后的解锁和重新分析，也应记录质量保证流程和对原始数据的任何更改。

稽查轨迹应记录所有因数据查询或澄清过程而产生的变更，其中应包含（至少）以下信息：修改或删除操作发生前的原始值，创建或修改操作发生后的新值；执行操作的时间（日期和时间戳）；执行操作的用户身份；操作的原因（对于修改或删除，应在操作时或通过受控流程强制/提示记录原因）。

对于某些类型的系统（例如电子化患者报告结局（ePRO）），输入的数据可能不会立即上传，但可能会暂时存储在本地内存中。在保存之前，未经数据创建者知晓，不

应编辑或更改此类数据。任何更改或编辑都应由数据创建者确认，应记录在稽查轨迹中，并应成为验证规程的一部分。收集工具(例如 eCRF)中数据输入的时间戳和保存到存储介质的数据的时间戳应作为元数据的一部分记录。从本地内存中的初始获取到上传到中央服务器之间的时间间隔不应过长且可追溯（即传输时间），尤其是在直接数据采集的情况下。

作为常规数据管理流程和质量控制的一部分，应定期审核稽查轨迹记录，以验证数据的可靠性，并检测潜在问题(如未经授权的修改、异常模式）。负责的研究者、申办者和检查人员应能够审查和理解稽查轨迹。稽查轨迹记录必须是可读的（例如，清晰的报告）并以电子形式保留，其保留期限应与相关电子记录(源数据和试验主文件)的保留期限一致。应确保稽查轨迹的可读性和可审核性，还应确保数据输入或传输的时间以带时区的时间戳或 UTC 等明确的方式自动记录。

应确保危及盲态保持的信息不会出现在盲态用户可以访问的稽查轨迹中。

（三）电子数据的审核

电子数据审核可确保试验用数据的质量与可追溯性，可用于（但不限于）识别缺失数据、检测数据操纵迹象、识别异常数据/离群值以及在非预期或不一致的时间和日期输入

的数据（单个数据点、试验参与者、研究中心）、识别不正确的数据处理（例如非自动计算）、检测未经授权的访问、检测设备或系统故障以及检测是否需要对试验参与者/研究者进行额外培训等。

1.数据审核

申办者应建立系统化、基于风险的规程和计划，利用计算机化系统的能力对采集的电子临床试验数据进行及时、持续的审核。并视试验过程中的情况进行调整审核范围和频率。

审核过程应能识别缺失数据、异常值、逻辑错误、与方案或预先定义规则的偏离以及潜在的数据趋势问题。确保数据与临床试验方案要求相符。

审核活动（包括审核人、审核日期和审核结果）应有记录。

2.元数据的审核

元数据的审核应成为申办者整体数据审核和质量控制流程的固定组成部分。

需要特别关注关键元数据，如那些用于计算派生数据、定义数据点含义或影响数据呈现方式的元数据。

应重点关注数据的准确性、完整性、一致性和版本控制状态，数据的采集、传输、存储和处理过程符合相关规定和SOP。元数据的变更也应有受控流程和记录，包括变更原因和批准。

元数据审核还包括稽查轨迹、访问日志、事件日志、质疑等的审核。访问日志（包括用户名和用户角色）在某些情况下被视为重要的元数据，因此应该是可查看的。例如，对于包含关键非盲数据的系统而言非常必要。稽查轨迹审核还可用于检测方案中已定义直接数据采集但未按规定进行的情况。研究者应当收到有关如何浏览所在中心的稽查轨迹的介绍，以便能够查看数据更改。

（四）数据更正

数据更正是维护数据可靠性的重要环节，数据错误应及时识别并更正，以减少错误对试验结果的影响。当数据创建者（例如研究者或试验参与者）发现错误地提交了不正确的数据并希望更正记录的数据时，应制定相应操作规程。如果数据发起人是试验参与者，则可能需要对数据澄清进行特殊考虑。

1.更正规程

必须建立清晰、受控、有文档记录的规程用于更正电子数据中的错误或遗漏。规程应确保更正操作的透明度和可追溯性。数据更正应能追溯做出该更正的主体，有原始记录来证明和支持，并应及时进行。

2.更正原则

执行数据更正时，必须强制记录更正的原因。原因说明应具体、清晰，并符合方案或数据管理计划的要求。

数据更正只能由经授权的人员执行。只有经授权的研究

者或操作人员才能对源数据中的数据进行更正。申办者不得更改研究者或试验参与者输入的数据，特殊情况需到研究者的授权并书面记录。

更正操作本身及其理由必须形成永久性记录，并与相关数据点关联，可供审查和稽查。对数据的任何更改都应注明日期、签名，并解释，且不应掩盖原始录入的数据。系统应通过以下方式实现：保留原始录入值；记录更正后的新值；清晰标识哪个是当前有效值；通过稽查轨迹自动记录更正操作（包括操作者、时间戳、更正原因）。

3.ePRO 的数据更正

ePRO 数据更正通常与其他数据采集工具的数据更正不同，因为试验参与者通常无法在应用程序中自主更改数据。因此，需要制定澄清规程，以便在有合理理由的前提下实施更正，不应禁止在合理的情况下更正试验参与者数据。

预计更正的可能性是基于合理的和特定于试验的风险评估来实现的，并且任何更正都由试验参与者或研究者及时启动，如果是后者，则基于研究中心的可靠来源，例如来自试验参与者的电话记录或电子邮件，记录了研究中心和试验参与者之间的通信在错误发生/发现后立即发生。

试验参与者直接输入数据可以让回忆偏倚最小化。因此，在没有充分理由的情况下，更正应及时进行。为了避免输入错误，ePRO 的设计既要适当地确保试验参与者正确理解，

又需要对试验参与者进行适当的培训。

（五）数据传输、交换和迁移

1.数据传输和交换

临床试验数据需要定期在不同的计算机化系统内部和系统之间传输和交换，所有数据传输和交换都需要预先规定。应建立规程并进行验证，采取安全加密等措施，确保数据和其元数据在传输和交换过程中保持可靠性和保密性，以及所有传输文件的完整性。从外部来源收集并通过开放网络传输的数据应有严格的保护措施，防止未经授权的更改，并应采取安全/加密措施，防止泄露机密信息。

验证应在临床试验开始时进行，包括恰当的压力测试，并确保该流程在整个临床试验运行过程中可用且正常运行（例如，确保申办者能够持续审查日记数据、实验室数据或安全委员会的不良事件数据等）。

数据传输和交换过程应有文档记录以确保可追溯性。传输或交换后的数据应进行系统间数据的一致性核查以避免数据丢失和被意外修改。被传输的数据和相应的稽查轨迹应被妥善保存并可以被随时查阅（根据其授权角色以及相应的访问权限）。试验参与者数据被传输到国外时应遵守跨境数据传输的各项规定，并告知试验参与者。

2.数据迁移

数据迁移与数据传输和交换不同，是指将现有数据和元

数据从一个计算机化系统永久迁移到另一个系统的过程。应制定详细的迁移规程并对此规程进行验证。迁移过程不应对现有数据和元数据产生不利影响。数据迁移过程的验证应考虑到过程的复杂性和可以预见到的所有可能性，包括校验求和、案例计数、数据的质量控制等。

数据迁移前，应进行风险分析，识别最可能出现的风险并制定恰当的风险预案。应使用测试数据对制定的风险预案措施进行验证，用验证结果来评估风险和应对措施。迁移完成后，应对迁移到新系统的关键数据进行核验。应对迁移过程每一步骤都详细记录，确保所有的数据操作和数据转换过程中的变更均可追溯。

应保留从旧系统到新系统的映射信息。不应分割整体临床试验中的数据、上下文信息和稽查轨迹。如果将数据迁移到新系统导致数据丢失，应采取适当的补救措施，采用可靠稳定的方法，整合数据和稽查轨迹，为所有数据使用者提供完整的数据信息。如果无法实现这一整合，应提供详细的解释。应提供数据和元数据之间的关联信息。

（六）数据签署

研究者是录入 eCRF 和其它电子采集工具中数据的责任方。申办者应在预定的项目节点请研究者或其授权人员对数据进行签署，确认其提交给申办者的数据符合 ALCOA++原则。被授权的数据签署人应具备审阅数据应有的资质并符合

国家法律法规的相关要求。

申办者应在风险评估的基础上规定每一特定临床试验数据签署的可接受时点和频率。风险评估应考虑到所采集数据的类型和重要性、试验总时长、申办者根据试验数据所做决定和做决定的时间点等方面的因素。

在期中分析和最终分析前必须进行数据签署确认，同时应及时签署重要数据，比如上报的 SAE、要裁定的重要事件和主要终点数据、数据监查委员会审阅的数据等。不应仅在数据库锁定前进行一次数据签署，而应及时对直接录入 eCRF 的数据进行阶段性审阅和签署。试验中的数据采集工具应设计具备支持阶段性数据签署的功能。

在给监管机构递交上市申请前，所有准备递交的数据都需要先由研究者或其符合资质的授权人员完成数据签署，然后再提取用于分析的数据。

（七）分析前数据库的最终确认

应根据临床试验方案的要求，由医学、统计、数据管理、药物警戒、项目运营等团队共同讨论，界定用于期中和最终分析的详细数据范围。应制定明确的数据清理完成节点及数据质量要求，按照已制定的规程完成所有数据采集、审核、医学编码及外部数据的一致性核查，及时更正错误，汇编方案偏离等不依从问题并判断对分析的影响，按照已制定的规程完成数据清理，达到预定的数据库锁库前数据质量要求，

完成数据库锁定。

在数据库锁定后发现数据错误，应按照已制定规程对需要更正的数据进行讨论，对需要解锁更正的数据完成数据库解锁、数据更正和再锁定过程。

按照预先制定的规程提取清理后的数据库，依照统计分析计划进行数据分析。应清晰记录上述所有工作内容，完成归档。

（八）数据复制

1.定义与适用范围

复制数据是指将原始记录或电子数据从一个介质或系统复制到另一个介质或系统的过程，目的是备份、归档、共享或用于分析。复制的数据可以包括源数据、元数据（包括稽查轨迹）、电子签名等内容。复制数据的行为必须确保数据可靠性，复制过程不得改变原始数据的内容或结构；确保数据可追溯性，复制行为应记录在稽查轨迹中，包括复制时间、执行人、复制目的等；有明确的版本控制状态，复制的数据应标明版本信息，确保与源数据的一致性；确保数据的安全性，复制过程应在受控环境下进行，防止数据泄露或篡改。

2.技术要求

复制数据的系统和工具应符合以下技术要求：支持数据校验以验证复制的准确性；支持稽查轨迹记录复制行为；支

持加密传输与存储；支持权限控制，确保只有授权人员可执行复制操作。

3.合规性要求

复制数据的行为应符合包括但不限于如下要求：保留复制记录；确保复制数据与原始数据具有同等法律效力；在临床试验过程中，复制的数据不得替代原始记录，除非已被认证为“核证副本”。

（九）核证副本

核证副本是指用于永久替代原始记录的复制件，必须经过验证，确保其内容与原始记录一致，并具备法律效力。核证副本应与原始记录内容完全一致，包含认证标识（如签名、时间戳、认证声明），可供检查人员、监查人员和稽查人员查阅，并被视为原始记录的合法替代品。

核证副本的生成应遵循以下流程：使用受控系统复制原始数据，通过技术手段验证副本与原始记录一致，由授权人员签署认证声明，注明副本生成时间、目的、责任人等，并将核证副本归档，并在系统中标识为”核证副本”。此外，核证副本必须具备与原始记录同等的可靠性；所有核证副本应纳入试验主文件或研究者文件夹中，并保留至法规要求的保存期限结束。

（十）数据控制

临床试验中在研究中心生成的试验参与者数据应在临

床试验进行过程中和结束后始终向研究者开放，以便研究者做出与试验参与者是否符合入排条件、如何治疗和护理等相关的决定，并确保研究者能够在法定的数据保留期限内履行职责保留数据的独立副本，包括中心实验室数据、独立影像数据和电子化临床结局评估数据等外部数据。如有例外情况应在方案中加以说明，例如与研究者共享信息会危及试验的盲态保持。

申办者不应在任何时间点对计算机化系统内的数据拥有唯一控制权。为了满足要求，研究者应能够自行下载同期的数据核证副本。

由研究者输入数据采集工具的数据应在当地法律规定的整个期限内可供研究者使用，这可以通过在研究中心同步保存数据核证副本或使用服务提供商等方式来实现。

任何有关托管的合同都应确保研究者对数据的控制。如果申办者通过服务供应商代表研究者安排托管，则合同应确保研究者对数据的控制范围。如果研究者将数据托管给服务供应商，应确保对数据使用符合当地法律法规要求和研究中心内部规定。

### （十一）云解决方案

#### 1.定义与适用范围

云解决方案是指通过互联网提供的远程数据存储、处理和访问服务，通常由第三方云服务提供商运营。在临床试验

中使用云服务必须确保数据的可靠性、安全性和合规性。

2.云解决方案的合规性要求

合规性要求包括数据主权与访问控制，必须明确数据存储位置，确保符合适用的数据保护法规。申办者和监管机构应拥有对数据的完全访问权。云服务提供商必须经过资格评估，并接受稽查或检查。与云服务供应商应签署的合同中应明确数据所有权、服务水平协议、安全措施、数据迁移与销毁条款。云平台必须经过验证，确保其功能、安全性和稽查能力符合 GCP 要求。

3.技术要求

云解决方案的技术要求应包括但不限于：支持加密传输与存储，提供完整的稽查轨迹，支持多因素身份验证，可配置权限管理，以及支持灾备与数据恢复机制。

（十二）数据备份

1.数据备份的原则与目的

数据备份是为了防止临床试验数据因意外丢失或损坏而采取的保护措施。通过定期复制并安全保存数据，确保数据的可靠性和可恢复性，是保障试验数据可靠性的关键环节。

2.备份策略的基本要求

应根据数据的重要性和更新频率设定备份周期，如每日、每周或实时备份。备份数据需存储在与主数据不同的物理或逻辑位置，并采用加密技术及访问权限控制以确保安全性。

同时，应定期进行恢复测试以验证备份的有效性，并将所有备份活动记录在稽查轨迹中，包括时间、内容及责任人等信息。

3.特殊备份要求

备份数据必须与原始数据保持一致。在系统退役或迁移前，需确保备份数据完整且可恢复。此外，所有备份数据应保留至符合相关法规规定的保存期限结束。

（十三）应急计划

1.定义与目的

应急计划是为应对系统故障、数据丢失、自然灾害或其他突发事件而制定的预案，旨在保障临床试验数据的可靠性和业务的持续运行。作为质量管理体系的重要组成部分，应急计划有助于在危机情况下迅速响应并恢复关键功能。

2.应急计划的核心内容

应急计划应包括全面的风险评估，识别可能影响试验的数据和流程的风险点；建立明确的响应机制，涵盖事件通知、隔离、修复和恢复规程；制定数据恢复策略，明确恢复时间目标和恢复数据点目标；准备替代方案，如备用系统或手工记录流程；确保相关人员接受应急培训，并定期进行演练以验证计划的有效性。

3.合规性与稽查

应急计划必须纳入质量管理体系并获得申办者批准。所

有应急响应活动应完整记录，确保可供稽查。随着试验阶段和技术环境的变化，应急计划也应动态更新，以保持其适用性和有效性。

（十四）归档

研究者和申办者应了解临床试验数据、元数据和重要文件的保存期限。保存期限应遵循数据保护原则的存储限制。应在被允许的保存期限内维护好所有重要数据和文件的清单，并明确与数据对应的每项临床试验活动，记录清楚文档存放地点及谁拥有访问或编辑文档的权限。

应制定实施有效的安全控制措施以确保数据的保密性和可靠性。应确保文件在整个保存期内保持可访问状态。数据迁移相关的内容也同样适用。

应建立适当的归档系统来保障数据的可靠性。归档时间要符合临床试验数据递交国家的监管要求。有授权人员应始终能够随时访问源文件和数据，完成监管要求的各项任务。

应保证数据保存的方式安全且仅可按照经过验证的流程在不同的地理位置之间传输。试验数据和相关元数据应以可检索和只读的方式归档，并应在整个保存期间防止未经授权的访问和更改。

（十五）数据库下线

试验结束后可以进行数据库下线。如果会近期进行上市递交申请，建议在递交完成后归档时再进行数据库下线。

下线前应保留数据库的核证副本，完成数据归档并确保数据可以随时被访问。申办者应确保数据库下线后归档的格式能够恢复数据库。如果归档由供应商完成，此要求应在合同中写明。这里包括恢复动态功能和所有相关元数据如稽查轨迹、事件日志、已实施的线上核查、质疑、用户日志等。如果无法重新恢复数据库，申办者应确保所有包含元数据（如稽查轨迹）在内的数据文件都存在归档的动态数据文件中。

申办者应审查计算机化系统，确定系统中有稽查轨迹和日志，并可以作为动态文件保留。如果计算机化系统由供应商提供服务，应在合同中说明。不应用静态格式归档动态数据。

（十六）销毁

临床试验数据（包括元数据）的销毁必须在确保数据可靠性、合规性和可追溯性的前提下进行。

有效的数据销毁应遵循以下基本原则：销毁行为必须符合适用的监管要求，包括数据保存期限、稽查轨迹、伦理审查和申办者或监管机构的批准（如适用）；销毁过程必须记录在案，包括销毁的时间、方式、责任人及批准记录；销毁过程应确保数据无法恢复，防止数据泄露或滥用；应采用适当的技术手段（如加密擦除、物理销毁）和组织流程（如双人核查）确保销毁的有效性和安全性。

数据销毁应在以下条件满足后进行：数据保存期限届满，应满足根据国家法规、申办者或监管机构的要求保存期限；所有相关的监管检查已完成，且无进一步保留数据的要求；销毁计划应获得申办者、伦理委员会或监管机构的批准（如适用）；应制定正式的销毁计划，包括销毁范围、方法、责任人、时间表和记录模板。

销毁方法与记录要求包括：对电子数据，应使用符合行业标准的数据擦除工具；对物理介质（如硬盘、光盘、纸质记录），应采用粉碎、焚烧或其他不可恢复的方式；销毁记录应包括数据类型、销毁日期、执行人、监督人、销毁方法、批准文件等；销毁记录应作为稽查轨迹的一部分保存，并可供监管机构查阅。

## 五、参考文献

[1] ICH. E6(R3): Guideline For Good Clinical Practice. Jan.2025. https://database.ich.org/sites/default/files/ICH_E6%28R3%29_Step4_FinalGuideline_2025_0106.pdf

[2] 药物临床试验质量管理规范（修订稿征求意见稿）. 2025 年 10 月. https://www.nmpa.gov.cn/xxgk/zhqyj/zhqyjyp/20251028164306197.html?type=pc&m=

[3] EMEA: Guideline On Computerised Systems And Electronic Data In Clinical Trials. Mar. 2023. https://health.ec.europa.eu/document/download/5170c32d-757e-4bdc-9f09-d66

93e76c668_en?filename=mp_ctr-guideline-computerised_en.pdf

[4] FDA: Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations Questions and Answers. Oct. 2024. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/electronic-systems-electronic-records-and-electronic-signatures-clinical-investigations-questions

[5] FDA. Part 11, Electronic Records; Electronic Signatures — Scope and Application. Sept. 2003. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application

740 # 附录：中英文对照表

| 中文 | 英文 |
| --- | --- |
| 标准操作规程 | Standard Operation Procedure，SOP |
| 病例报告表 | Case Report Form，CRF |
| 电子病例报告表 | Electronic Case Report Form，eCRF |
| 电子化患者报告结局 | Electronic Patient-Reported Outcome，ePRO |
| 电子数据收集系统 | Electronic Data Capture System，EDC |
| 核证副本 | Certified Copy |
| 恢复时间目标 | Recovery Time Objective |
| 恢复数据点目标 | Recovery Point Objective |
| 销毁计划 | Destruction Plan |
| 协调世界时 | Coordinated Universal Time，UTC |
| 源数据 | Source Data |
| 元数据 | Metadata |

741