药物临床试验 信息安全 •广东共识（2023 年版）

（广东省药学会 2023 年 3 月 23 日发布）

为更好地构建药物临床试验信息安全环境，尊重并切实保障受试者个人信息保护权益，依据《中华人民共和国个人信息保护法》以及国内外相关法规、指南和参考文献，编写本共识。

本共识主要围绕数据安全和个人信息保护两方面进行编写，数据安全主要包含药物临床试验受试者的数据采集、传输、存储、使用、共享以及最终销毁的全生命周期数据安全要求，个人信息保护主要根据个人信息保护措施以及个人信息权益响应两方面进行展开。

本共识在征求意见期间，收到业内同行的积极反馈，经共识撰写小组共同讨论，在吸纳同行对此探讨交流与反馈意见的基础上，形成本共识，期待得到各位业内同行的支持和认可，成为药物临床试验各方在处理药物临床试验数据安全和受试者个人信息保护方面的参考。

一、药物临床试验信息安全共识适用场景

1.存储受试者数据、重要试验数据的系统安全规范以及药物临床试验机构的受试者数据处理准则。

2.药物临床试验机构针对招募受试者个人信息的采集、存储、使用等环节的个人信息保护要求。

3.涉及受试者数据的系统以及可采集个人信息的医疗设备供应商，针对个人信息保护以及数据安全性设计。

4.监管机构及行业监管对于医疗行业数据安全与隐私保护监督的评估参考。

二、药物临床试验信息安全相关术语和定义

1.个人信息

在药物临床试验过程中涉及以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

药物临床试验个人信息举例可以参考附录A。

2.敏感个人信息

敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

药物临床试验敏感个人信息举例可以参考附录A。

3.知情同意

知情同意指向受试者告知一项试验的各方面情况后，受试者自愿确认其同意参加该项临床试验的过程，须以签名和注明日期的知情同意书作为文件证明。

4.知情同意书

知情同意书是每位受试者表示自愿参加某一试验的文件证明。研究者需向受试者说明试验性质、试验目的、可能的受益和风险、可供选用的其他治疗方法以及符合《赫尔辛基宣言》规定的受试者的权利和义务等，使受试者充分了解后表达其同意。

5.明示同意

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。注：肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

6. 去标识化

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

三、药物临床试验数据安全基本要求

（一）药物临床试验数据采集安全

1. 在药物临床试验方案编制过程中，应明确试验全生命周期各步骤中所应当采集的最小且必要的个人信息范围，并经过伦理委员会审核同意。受试者的数据采集也应遵循最小且必要原则，常见药物临床试验场景采集个人信息的最小化范围可以参考附录B。

2. 知情同意书中应加入受试者个人信息采集的类型、目的、个人信息的处理方式及保存期限，并获得有效的受试者知情同意。

3. 在采集十四周岁（含）以下未成年人或其他无自主明示同意能力人员个人信息时（例如植物人、精神病患者等），应提前获得其监护人的明示同意。可参考《药物临床试验 无障碍知情同意•广东共识》。

4. 知情同意书应由伦理委员会审核同意，确保格式及其内容包含数据采集的类型和目的，确保个人信息的采集在药物临床试验项目规定的合理范围内，且数据安全与个人信息保护满足相关法规和本共识要求。

5. 经穿戴设备采集受试者健康信息，如心率、脉搏、体温等，均应在批准的知情同意书所规定的范围内。不得采集与药物临床试验无关的数据信息，并应充分考虑穿戴设备本身缓存数据的安全性，以及共享数据的第三方的情况。

6. 直接将医疗机构患者的诊疗卡个人信息和诊疗信息作为药物临床试验数据的，应事先获得患者本人的明示同意。

7.药物临床试验数据分类分级

①应在受试者数据采集和存储阶段进行分类、分级管理。针对受试者个人身份信息、健康信息、联系方式等分类维度以及数据敏感等级进行标签化管理，对于不同敏感等级数据，应配备相应的安全保护能力。

②行业主管部门或其他监管机构规定规定属于国家重要数据的，应在分类、分级时，给予其最高安全等级的保护。

（二）药物临床试验数据传输安全

1.当使用电子邮件和通讯工具以及物理存储介质等方式传输数据时，应对数据进行加密处理，加密后的密码应通过其他安全方式传递给数据接收方。

2.针对样本数据的使用，应详细记录接触样本的人员以及样本传输的数据流，留存记录时间至少应在药物临床试验项目结束后5年以上。

3.系统数据传输应对传输通道进行加密，并进行双方身份鉴别及认证。根据传输数据敏感级别，应同步提升相应的安全传输保障手段。

（三）药物临床试验数据存储安全

1.应对受试者个人信息进行加密存储，加密算法应选用安全的加密算法，应当遵循密码管理相关国家标准 。

2.个人生物识别信息与个人身份信息建议分开存储，生物识别信息包括人脸、指纹、声纹、步态、虹膜等。非必要的，不应存储原始生物识别信息，只存储摘要信息。

3.用于申请药品注册的药物临床试验，必备文件应当至少保存至试验药物被批准上市后5年；未用于申请药品注册的药物临床试验，必备文件应当至少保存至药物临床试验终止后5年。

4.机构伦理审查委员会应当保留伦理审查的全部记录，包括伦理审查的书面记录、委员信息、递交的文件、会议记录和相关往来记录等。所有

记录应当至少保存至药物临床试验结束后5年。

5.数据应做好可靠备份和恢复演练计划。

6.系统供应商应针对系统制定完整的应急预案，以确保系统在发生故障时，能最短时间内恢复正常运行。

7.原则上，受试者个人信息应存储在机构内网环境中，外部宜使用VPN或专线进行访问。

（四）药物临床试验数据使用安全

1.应采用去标识化和匿名化等技术，严格控制可见试验用药组别信息的范围，包括在试验机构数据集成平台所使用的去标识化和匿名化技术。

2.应严格按照与受试者签署的知情同意书范围处理受试者个人信息，如超出处理范围，应再次征得受试者的有效的知情同意。

3.采用受试者画像进行药物临床试验项目推荐或其他药品、广告推荐的，应向受试者明确必要的个性化退出机制，包括短信退订机制、线上系统的关闭按钮等。

4.个人信息使用应遵循最小且必要原则。应由伦理委员会定期审核受试者个人信息使用情况，确保当前使用符合批准的范围。

5.当涉及受试者信息需要传输至药物临床试验机构外的情形时，应对其进行加密或对其进行脱敏处理，完全去除其可识别个人的信息内容，且在不借助药物临床试验机构的能力下不可溯及受试者个人。

6.EDC、远程监查等系统在可显示受试者个人信息页面或涉及药物临床试验重要数据的内容展示时，应采用明文水印或其他安全技术，保障不被截屏、拍照，以防止数据泄漏，或泄漏之后可以进行有效的追查。

7.一旦EDC系统保存输入的数据后，应对所有数据的删改保留稽查轨迹，并且稽查轨迹不得从系统中被删除或修改。

8.系统操作日志、网络设备日志以及安全设备日志应保存至少6个月

以上。

9.系统权限设置应遵循最小化原则，如因其他特殊情形需要使用个人信息时，应有明确的审批流程，记录具体使用个人信息的类型、数量以及使用目的。

10.揭盲相关数据信息应妥善保管，存储时进行加密，严格控制其信息的访问及使用权限。

（五）药物临床试验数据共享安全

1.在多中心协作药物临床试验项目中，原则上不应共享包含受试者身份信息的原始数据。若确需共享的，应提前对数据进行匿名化处理，或使用其他可信任方式，如多方可信计算或联邦学习等。

2.如确需共享非匿名化受试者个人信息数据，应提前获得受试者的、有效的知情同意。

3.数据共享应与被共享方签署数据安全保密协议，明确数据使用目的、范围和数量等，约束双方责任以及数据保护义务。

（六）药物临床试验数据转移、委托处理、公开披露安全

1.原则上，受试者个人信息不应公开披露。受试者个人信息的公开披露应该符合相关的法律、法规和规章的规定，并应向受试者告知公开披露其个人信息的目的和个人信息类型，签署知情同意书。

2.当申办方、合同研究组织倒闭重组或其他情况转让受试者个人信息时，应事先告知受试者接收相关方的详细信息，并告知其数据接收方保护数据的能力，接收方的数据安全保护能力宜不低于当前申办方或合同研究组织，并重新获取受试者知情同意。

3.当药物临床试验机构无处理受试者个人信息的能力，需要委托其他相关方进行处理时，应提前告知受试者被委托处理其数据的第三方信息，被委托方的数据安全保护能力不应低于委托的机构，并重新获取受试者知

情同意。

四、药物临床试验数据出境

药物临床试验数据出境应遵循人类遗传资源管理办公室、国家网信部门等监管机构的要求。

五、药物临床试验个人信息权益保护要求

（一）在知情同意书中，应明示受试者的个人信息权益，包括查询、更正、撤回同意其个人信息，获取其个人信息或健康信息副本的权益。

1.药物临床试验机构宜向受试者提供查询其个人信息及其类型、来源、所用于的目的或途径。

2.受试者发现药物临床试验机构所持有的其个人信息有错误或者不完整的，药物临床试验机构应为受试者提供更正或者补充信息的方法。

3.药物临床试验机构应该向受试者提供撤回收集、使用其个人信息的授权同意的方法，撤回个人信息同意之后不影响之前个人信息所处理的结果。

4.药物临床试验机构应该向受试者提供获取本人的基本资料、身份信息、健康生理信息、教育工作信息等个人信息副本的方法，或在技术可行的前提下直接将其个人信息副本传输给受试者指定的第三方。

（二）药物临床试验机构应建立并公开受试者个人信息权益响应机制，并能在15日内响应受试者需求。如决定不响应受试者的请求，应向受试者告知该决定的理由，并向受试者提供投诉的途径。

（三）药物临床试验机构应建立并公开投诉管理机制和投诉跟踪流程，并在15日内对投诉进行响应。

（四）药物临床试验机构对于个人信息安全事件应制定应急预案并组织应急培训和演练。当发生受试者信息泄漏事件时，应能及时通知被泄漏信息受试者其泄漏的信息内容、产生影响，以及最后的解决措施。对于影

响较大、波及人员较多的个人信息安全事件，应同时上报地方监管部门。

六、信息安全管理要求

（一）组织及从业人员安全管理

1.药物临床试验机构应指定一名具有相应资质的人员，作为试验过程个人信息保护责任人，负责制定、实施、维护和监督试验过程中的个人信息管理过程，以确保机构药物临床试验遵守个人信息保护相关的适用的法律、法规和规章。

2.涉及处理受试者个人信息的项目人员应签署保密协议，明确保护责任。

3.药物临床试验过程中，涉及处理受试者个人信息的项目人员应每年参加不少于 1 个工作日的数据安全及个人信息保护的培训。

4.药物临床试验机构应制定规范化的个人信息保护制度，以确保药物临床试验合法、合规和有效。

（二）物理环境及资产安全

1.应确保重要区域（如机房、药房、检验样本贮藏室、纸质病历/简历存放室等）物理环境安全，设置门禁管理，明确门禁权限持有人员清单并定期进行权限审计清理。针对非授权访客进出做好记录，记录内容应包含：进/出物理区域具体时间、访问人员姓名（签字）、访问人员所在单位名称、访问事由、随访陪同人员姓名（签字）等信息。在必要时，重要区域访问还应经过审批授权后方可进入。

2.试验过程打印文件应及时取走，废弃文件应使用合规的碎纸机销毁。

（三）访问控制安全

1.在药物临床试验过程中，使用系统的所有用户必须拥有唯一的用户名和密码组合。密码在系统内部必须以加密方式存储。也可以用动态口令卡、USB-KEY 数字证书、生物学标记（如指纹）等更高级别的安全措施来替

代密码，或使用双因素验证机制，其中一种验证方式应为密码形式。

2.不应共享涉及受试者个人信息的系统帐号密码。

3.密码复杂度宜设置8-16位，至少包含大小写字母，数字、特殊字符四项中的三项。密码宜至少每90天更换一次。

4.在药物临床试验系统中，应特别注意涉及个人信息查阅、编辑、导出等操作权限的用户，并且对用户权限应定期进行复查与清理。

5.当药物临床试验涉及系统中任一项目成员退出药物临床试验项目，或药物临床试验项目中止时，应及时收回或停用系统中相应项目成员帐号权限。

（四）系统安全

1.药物临床试验系统产品验证流程应遵循GAMP5的方法。

2.在药物临床试验系统中，针对涉及个人信息处理的系统，应在设计阶段引入安全合规理念，做好个人信息处理合规性评估，并针对个人信息制定相应保护措施设计（例如，加密存储、脱敏展示、用户知情同意模块设计等）。

3.药物临床试验系统每年应至少能进行一次渗透测试与漏洞扫描，发现其内部存在的漏洞并及时修复。

4.药物临床试验系统应建立系统故障/中断事件应急预案，并每年组织进行演练，评审并优化预案内容。

（五）供应商安全管理

1.应对试验过程选用供应商进行信息安全背景调查，满足一定信息安全防护水平后方可采购相应服务/产品。

2.在试验过程中，如需引入涉及个人信息处理的供应商，应当与供应商在合同中约定委托处理个人信息的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对供应商的个人信息处理活

动进行监督。

3.应当与供应商明确，未经药物临床试验机构同意，受托人不得转委托其他组织或个人处理个人信息。

4.应每年对供应商进行服务评审，包括供应商履行信息安全保护合约情况及其他信息安全评价标准。

七、附录

附录A：药物临床试验数据个人信息与敏感个人信息举例

个人信息	个人身份信息	身份证、工作证、社保卡、居住证等
	个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
	个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
敏感个人信息	个人健康生理信息	外部仪器检测数据（如血生化、心电图、血流仪、生命体征监测、影像学检查等）、基因序列、特殊族系信息、个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等
	个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等

附录 B：药物临床试验常见场景中最小必要个人信息参考

个人信息收集主体	收集场景	最小必要个人信息参考	备注
受试者	招募	● 患者成年并具有自主意识及行为能力： 姓名、身份证、用药史、病史、个人电话号码、电子邮件地址、年龄、检验检测报告、疾病诊断、性别、签字信息 ● 患者未成年/不具有自主意识或行为能力： ● 患者:姓名、身份证、用药史、病史、年龄、检验检测报告、疾病诊断、性别 ● 监护人：姓名、个人电话号码、电子邮箱地址、签字信息	如非必要，不应采集如籍贯、性别、学历程度、性取向、职业信息等其他可能会危害人身和财产安全、损害个人名誉和身心健康、导致差别性待遇的个人信息。
PI	筛选	姓名、工作单位、职级职称、工作地址、个人电话号码、电子邮箱地址、过往药物临床试验研究经验、学历信息、工作经历	如非必要，不应采集如籍贯、性别、性取向、经济情况信息等其他可能会危害人身和财产安全、损害个人名誉和身心健康、导致差别性待遇的个人信息。
	患者知情同意书披露	姓名、工作单位、职级职称、工作地址、个人电话号码、电子邮箱地址	
	药物研究对外披露	姓名、工作单位、职级职称、工作地址、个人电话号码、电子邮箱地址、过往研究经验	
CRC	筛选	姓名、工作单位、工作地址、个人电话号码、电子邮箱地址、过往药物临床试验项目经验、学历信息、工作经历	如非必要，不应采集如籍贯、性别、性取向、经济情况信息等其他可能会危害人身和财产安全、损害个人名誉和身心健康、导致差别性待遇的个人信息。
CRA	筛选	姓名、工作单位、工作地址、个人电话号码、电子邮箱地址、过往药物临床试验项目经验、学历信息、工作经历	

参考文献

[1]全国人民代表大会常务委员会.中华人民共和国个人信息保护法[S/OL](2021.8.20)[2022.12.9]
http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
[2]全国人民代表大会常务委员会.中华人民共和国数据安全法[S/OL](2021.6.10)[2022.12.9]
http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml
[3]中华人民共和国国务院.中华人民共和国人类遗传资源管理条例[S/OL](国令第717号)(2019.6.10)[2022.12.9]
http://www.gov.cn/zhengce/content/2019-06/10/content_5398829.htm?t=1635546920963
[4] 国家药品监督管理局.药物临床试验质量管理规范[S/OL](2020年局令第57号)(2020.4.26)[2022.12.9]
https://www.nmpa.gov.cn/yaopin/ypggtg/20200426162401243.html
[5]全国信息安全标准化技术委员会.国家标准化管理委员会.信息安全技术 个人信息安全规范(2020.3.6)[2022.12.9]
https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=4568F276E0F8346EB0FBA097AA0CE05E
[6]全国信息安全标准化技术委员会,国家标准化管理委员会.信息安全技术 健康医疗数据安全指南(2020.12.14)[2022.12.9]
https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=239351905E7B62A7DF537856738247CE
[7]广东省药学会.药物临床试验受试者隐私保护·广东共识(2020年版)[Z].(2020.8.1)[2022.12.9]
http://www.sinopharmacy.com.cn/download/104.html

起草专家组

顾问：

洪明晃	中山大学肿瘤防治中心	临床研究部
杨忠奇	广州中医药大学第一附属医院	药物临床试验机构
邹燕琴	中山大学孙逸仙纪念医院	药物临床试验机构办公室

执笔：

张勋	广东省中医院	药物临床试验机构办公室
华贤扬	浙江太美医疗科技股份有限公司	质量安全部
吴佳荣	广东省中医院	信息管理办公室

成员：(按姓氏拼音排序)

曹烨	中山大学肿瘤防治中心	临床研究部
陈琳	暨南大学附属第一医院	药物临床试验机构办公室
杜彦萍	广州中医药大学第一附属医院	药物临床试验机构办公室
傅昊阳	广东省中医院	信息管理办公室
韩珂	广州医科大学附属第二医院	药物临床试验机构办公室
蒋发烨	广东省人民医院	药物临床试验机构办公室
梁伟雄	广东省中医院	药物临床试验机构
柳超	浙江太美医疗科技股份有限公司	质量安全部
吕丽虹	中山大学孙逸仙纪念医院	药物临床试验机构办公室
倪穗琴	广州市第一人民医院	药物临床试验机构办公室
潘芸芸	南方医科大学南方医院	I 期临床研究室
石磊	中国人民解放军南部战区总医院	药物临床试验机构
司徒冰	广州医科大学附属第三医院	药物临床试验机构办公室
孙健	中山大学附属第三医院	临床研究中心
万帮喜	浙江太美医疗科技股份有限公司	质量安全部
吴建龙	深圳市第二人民医院	药物临床试验机构
许重远	南方医科大学南方医院	药物临床试验机构
叶丽卡	广州医科大学附属第二医院	I 期临床研究室
曾晓晖	广州市花都区人民医院	药物临床试验机构办公室