药物临床试验 受试者隐私保护·广东共识（2020 年版）

广东省药学会 2020 年 8 月 1 日发布

起草说明

纵观《赫尔辛基宣言》及《药物临床试验质量管理规范》等相关原则规范，对临床试验受试者的权益保护高于科学及社会效益；受试者权益保护贯穿于药物临床试验的全程，其中受试者隐私保护是容易忽视的环节。药物临床试验过程中对受试者的个人信息进行规范使用和必要保护是试验各方应当遵守的基本准则，是研究者和机构的法定义务，也是公众愿意参与临床试验的前提保证。

2020 年 5 月 28 日第十三届全国人民代表大会第三次会议通过《中华人民共和国民法典》以及近年来发布的各项法律法规中，都将保护公民隐私权和个人信息提到了前所未有的高度，特别是网络时代和电子化数据时代的到来，对公民隐私保护带来新的挑战。为了切实提高药物临床试验参与各方对受试者隐私保护的意识，保护受试者个人信息安全，防范受试者隐私泄露所致的伤害和风险，广东省药学会药物临床试验专业委员会组织国内从事药物临床试验的专家、数据科学工作者以及法务工作者，起草《药物临床试验 受试者隐私保护·广东共识》，以期引导各方对受试者隐私给予特殊关注，为更好地保护受试者隐私提供参考。

本共识经撰写成员多次讨论反复推敲，虽数易其稿，但鉴于共识涉及跨专业领域及知识，撰写成员认识与经验有限，共识尚待完善和优化，期待业内同行能多提宝贵意见和建议。

共识起草小组

2020 年 7 月 8 日

目　录

受试者的隐私保护包含在受试者保护的范畴中，在临床试验中优先于科学探索。从知情同意、入组、到试验结束之后的随访，受试者的个人信息将会贯穿整个临床试验的过程。对受试者的个人信息进行规范使用和必要保护是试验各方应当遵守的基本准则，也是公众愿意参与临床试验的前提保证。

1 受试者的个人信息和隐私

受试者作为自然人，其个人信息受到法律保护；享有隐私权，任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害其隐私权。

1.1 定义

根据《中华人民共和国民法典》第一千零三十四条，自然人的个人信息是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而识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。

根据《中华人民共和国民法典》第一千零三十二条，隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。在医疗场景中，患者隐私保护还应包含：在医疗活动中对患者身体的隐私部位、病史、身体缺陷、特殊经历、遭遇等隐私进行保护，以确保不受任何形式的外来侵犯的权利。这种隐私的内容，除了患者的病情之外还包括患者在就诊过程中只向医生公开的、不愿意让他人知道的个人信息、私人活动以及其他缺陷或者隐情。在临床试验场景中，受试者隐私还应包含：个人参加临床试验的意

愿和事实、知情同意过程、临床试验过程中从受试者处采集并用于临床试验的含有受试者隐私的各类数据。

1.2 范畴

临床试验过程中通常会收集的受试者个人信息主要包括:

（1）受试者的身份信息。常见的这类信息包括受试者的姓名、性别、年龄或出生日期、职业、学历、婚姻状况、家庭住址、电话号码、证件（身份证号、护照号、社会保障卡号、医疗卡号）、住院号、门诊号、银行账户信息、签名等。

（2）受试者的健康信息。通常体现为受试者的疾病诊断与治疗用药、血型、家族疾病和遗传性疾病史等个人的医疗记录。

上述信息如果泄露，均有可能给受试者造成不同程度的损害或负面影响。医学研究中记录、管理和使用受试者个人信息，常常会涉及受试者隐私的资料，如果未征得受试者同意使用涉及个人身体状况或行为等的资料就是侵犯隐私，研究过程中没有妥善保护受试者提供的信息即违反了资料的保密义务。

2 受试者隐私保护的主要环节

在临床试验项目中，隐私保护问题不仅涉及受试者的个人法律权利，而且也是一个医学伦理问题。根据《药物临床试验质量管理规范》，包含受试者隐私信息的记录和文件应当被妥善处理和保存，直接查阅的任何一方应当按照相关法律法规，采取合理的措施保护受试者隐私以及避免泄露申办者的权属信息和其他需要保密的信息。受试者的姓名等身份识别信息应当用“受试者鉴认代码”进行代替。根据临床试验不同环节中可能存在的受试者隐私保护问题，现归纳相应的主要保护措施如下:

2.1 伦理委员会审查

一项临床试验开展前，需经过伦理委员会的审查。伦理委员会应严格审查试验中的有关受试者隐私及保密的措施，并做出是否同意开展的决定。临床试验项目在进展过程中，也应全程接受专业的伦理审查监督。一旦发现受试者隐私存在泄漏风险，或者受试者个人信息有被滥用、泄露或盗用等风险的，应立即责成相关方予以纠正、排除风险。对侵犯受试者隐私或个人信息的，应当要求责任方给予赔偿或依法承担相应法律责任。

2.2 受试者招募

申办方和研究机构应建立渠道，如发布经伦理委员会审批通过的招募信息、张贴招募广告等，使有潜在入组可能的患者可直接联系到研究者，避免信息通过第三方公司或组织转介。个别特殊领域的研究项目，比如罕见病等，由于招募困难等原因通过第三方公司招募受试者的，在收集潜在受试者的个人信息时，应严格遵守相关法律法规，采取必要措施或提供可保障该信息安全的手段或承诺。从事此类服务的第三方招募公司必须专业、有完善的合规体系且有良好的从业记录。

2.3 知情同意和知情同意书

将隐私保护写入知情同意书，对受试者进行充分告知，取得受试者的同意，以使受试者知道其个人信息和隐私受到法律保护且研究团队将按法律规定和知情同意书等文件的要求合理使用，但还应告知受试者隐私保护的局限性。一旦发现受试者的个人信息或隐私受到侵犯，受试者可提起质疑甚至诉诸法律手段，而这些行为不应影响其正常的临床诊疗。

知情同意书中，关于受试者隐私保护的表述建议包含但不限于以下内容：为什么要收集我的个人信息？由谁收集？谁会接触我的个人信息？如何保护

我的个人信息？将收集我的哪些个人信息？将会如何使用我的个人信息？我对我的个人信息具有哪些权利？如果我想撤销使用我的个人信息的同意怎么办？

2.4 营造隐私保护的随访环境

倡导“一医一患一诊间”，随访诊疗在私密性较好的诊室或专用房间，如“临床试验接待室”中进行，尽量采用个体谈话，避免集体谈话。

2.5 匿名化或编码

采取保密措施确保研究项目资料的保密性。通常的做法包括但不限于，使用代码来记录受试者的身份确认信息。受试者纳入研究时，将其姓名转换为“受试者鉴认代码”，确保身份信息、疾病信息、生物样本信息等数据经过编码“脱敏”处理后提供给申办方以及有必要获得相应部分信息的其他试验参与方；病例报告表（CRF）上使用受试者鉴认代码。

2.6 控制接触鉴认代码表人员

受试者姓名、住址等身份信息和与之对应的代码登记在“鉴认代码表”中，无论是项目进行阶段还是结题归档，主要研究者应严格控制接触鉴认代码表的人员，由授权人员填写并保管。非授权人员查看鉴认代码表应做好查阅记录。

2.7 存储设备和设施管理

研究资料由专人管理，储存在有标识的带锁文件柜。尤其应注意含有受试者姓名的研究病历、知情同意书、检查检验报告、鉴认代码表等资料不应随手放置于公共桌面。

2.8 试验文件管理

规定凡是离开研究基地保存设施的临床试验资料，均不应含有受试者的个人信息。任何研究资料离开研究机构保存设施之前应进行严格检查。

2.9 查阅权限

在临床试验的信息和受试者信息处理过程中应当注意避免信息的非法或者未授权的查阅、公开、散播、修改、损毁、丢失。只有研究者和研究组成员可按照工作授权在必要范围内查询代码对应的受试者信息。仅在不违反保密原则和相关法规且工作必须的前提下，监查员、稽查员、伦理委员会和药品监督管理部门检查人员可以查阅受试者的原始医学记录，以核实临床试验的过程和数据。任何人被获准查询前，管理员均应核对其有效身份，以确保试验资料的保密性。

2.10 样本管理

涉及医学判断的样本检测实验室，应当符合相关规定并具备相应资质。临床试验中采集标本的管理、检测、运输和储存应当保证保密性。禁止实施与伦理委员会同意的试验方案无关的生物样本检测。临床试验结束后，剩余标本的继续保存或者将来可能被使用等情况，应当由受试者签署知情同意书，并说明保存的时间和数据的保密性问题，以及在何种情况下，数据和样本可以和其他研究者共享等。

2.11 信息公布

研究项目对外发布信息应有严格的流程管理。即使发布临床试验结果时，受试者的身份信息仍应保密。

2.12 参研人员的管理和培训

研究者、外聘 CRC 等参研人员需接受保密教育、参加保密培训、签署保密协议，尊重受试者隐私，增强各参研人员的隐私保护意识。

3 隐私保护的特殊考量

3.1 特殊受试者

基于特殊受试者隐私泄露更易导致心理危害或社会危害，如因艾滋病史、认知障碍及家族遗传病史的泄露而遭到社会排挤或偏见，应在知情同意及伦理审查方面给予该类受试者特殊的考虑。

3.1.1 知情同意

特殊受试者维护自身意愿或权利的能力可能存在不足或者丧失，因此执行知情同意时更应注意知情方式和语言，完善知情同意的程序，如艾滋病受试者；对知情告知及随访的场所与时间应有更高的要求，如注意在场人员的权限和保密性，防止因隐私泄露造成对受试者的伤害。

3.1.2 伦理审查

涉及特殊受试者的研究，伦理审查时应聘请相关专业背景的委员或吸纳倡导特殊受试者权益保护的人士，评估受试者隐私保护和敏感信息保密的措施；有条件的伦理委员会可组织实地访查，审查知情同意过程的规范性。

3.2 生物样本及相关数据

3.2.1 基本原则

研究者须告知受试者研究所采取的安全保密措施及可能的局限性，隐私泄露的潜在不良后果；获取的生物样本及其相关数据应匿名化或以编码等形式处理，限制第三方对生物样本及相关数据的访问和使用权限，储存及使用的过程中不得出现与知情同意相矛盾或相违背的情况；妥善保管生物样本的身份鉴认代码；以聚合形式披露数据，个体数据的发布应隐去可识别到个人的信息。

3.2.2 特殊考量

3.2.2.1 基因数据

当生物样本研究涉及基因数据背景，相关身份识别变量的删除或聚合数据发布的传统模式对隐私保护的有效性待考究。此类研究的隐私风险评估，不能仅孤立的局限于数据披露层面，亟需将整体数据环境纳入考虑，以降低间接识别受试者身份的风险。

3.2.2.2 生物样本的转移

在符合人类遗传资源法律规定和管理程序的前提下，签署协议方可转移生物样本库，以确保生物样本的可追溯性。转移协议应根据知情同意内容规定生物样本库的使用范围和保密性，以及使用完毕后的状况及去向，并明确协议所涉各项工作内容的相关责任方。

3.3 健康相关研究产生的数据

3.3.1 基本原则

健康相关研究产生的数据，其范围大于受试者的个人信息，但隐私保护的基本原则与“生物样本及相关数据”一致。

3.3.2 特殊考量

3.3.2.1 数据的二次使用

拟对已存储数据进行二次使用，其预期用途、风险管控及数据的可识别性特征须符合原知情同意的范围，由伦理委员会审查研究目的、保密条件和知悉范围，并判断是否需要再次知情同意。

3.3.2.2 数据挖掘

对于非有意收集健康相关数据的研究，但其所收集的数据可经挖掘，进一步用于健康相关研究的价值时，应建立相应的管理架构和机制对已收集储

存的数据进行妥善的保管和监督，确保数据挖掘过程中无法识别个人数据主体。

3.3.2.3 数据共享

隐私保护并非信息孤岛，而是数据共享的适当条件，应搭建数据共享保障体系，以创建负责任的数据共享文化。建议在不损害共享数据的科学有用性的基础上，通过对共享数据的对象及共享条件的控制来降低共享数据所带来的受试者个人信息泄漏的风险；共享数据的组织应签署数据使用协议，规范脱敏和数据安全的措施。

3.4 电子化收集和网络传输的数据

3.4.1 基本原则

使用网络环境和数字化工具收集数据时，须明确保护隐私的措施，以防止直接暴露个人信息，或防止当数据出版、共享、整合或链接时，受试者个人信息被推测出来。评估研究的潜在隐私风险，尽可能降低这些风险，并对剩余风险做出说明，在研究的全程中预测、控制、监查和审查数据的使用和交互影响。

在数据的静态存储和动态传输方面，须对其进行物理安全和网络安全的保护控制，建议采用保守的方式如光盘等进行网络传输，采取相应的加密存储、脱敏处理等安全措施，以实现数据安全隔离与受试者隐私保护。此外，针对数据访问，需根据访问数据的类型、涉及敏感信息的级别以及使用者的目的，建立基于风险的不同级别的身份认证和授权。

3.4.2 特殊考量

3.4.2.1 数据库关联

鉴于隐私风险并非仅是单个数据库的具体领域、属性或关键词里某一功能的呈现或缺乏，因此随着电子化收集数据的普及化，数据库信息的叠加性，提高了受试者身份锁定的可能。应选择和实施恰当的措施以降低隐私风险，并对数据相关的预期用途和隐私风险采取安全控制的措施，如制订数据访问的精准度、数据使用的限制条件、数据泄露的应急计划。

3.4.2.2 通过公共网站收集已存在的数据

研究者通过公共网站收集已存在的个人和群体的数据时，仍须承担尊重隐私和降低风险的义务，若无法与数据主体直接沟通，至少应获得网站所有者的许可，告知研究意图，并确保符合网站公布的使用条款。

3.4.2.3 中心化监查

制订中心化数据监查相关的监查规范和标准操作规程，如监查的原始文件副本的管理和处置。中心化监查的监查范围应当与监查计划或规定的范围一致，建议侧重于受试者的安全和数据一致性。与研究中心商榷远程访问受试者电子原始记录的程度，传输前对受试者身份信息进行脱敏。

4 隐私泄露的风险评估

面对隐私泄漏的风险，常用的机制是通过数据匿名化为临床试验提供一种处理保护受试者隐私和数据效用最大化之间紧张关系的方式。但是由于数据并非完全随机的，所以匿名化也并非绝对的，因此，我们在谈及隐私泄漏的风险时面临的主要挑战是了解“可接受的风险水平”。并需要在评估风险水平时，考虑任何可能违反保密规定的后续影响，这种影响可能很难定义。不仅依赖于数据本身，更依赖于数据产生后的上下游以及使用数据和数据与数据环境交互所产生的数据情况。

4.1 数据环境

数据环境本身通常是动态的和复杂的，这取决于数据共享和发布的约束条件。虽然难以描述，但一般来说，数据环境可以通过以下四个方向来进行描述:

- 数据代理（可以是临床试验参与人员，也可以是相关电子系统）;
- 数据范围;
- 数据治理（包括决定谁可以访问数据，以及对用户的使用有哪些限制）;
- 安全性的基础设施。

从数据环境出发，受试者隐私数据的安全性取决于数据与特定数据环境之间的关系：相同的数据在不同的情况下会有不同的风险。也就是说仅孤立的考虑数据本身来确定风险是不全面的，从以下三个关键领域出发结合对数据环境的考虑也许可以给到我们更多的风险评估思路:

- 数据情况的审计（系统地描述数据及其环境，数据资源使用方法，数据资源涉及的法律及道德范畴）;
- 风险分析及控制（根据数据情况评估披露的风险及如何管理风险）;
- 影响管理（在共享或发布数据之前采取的降低重新识别风险的可能，以及意外情况下需要重新识别风险或出现安全漏洞的情况采取的措施）。

4.2 风险评估的定量和定性方法

考虑数据环境后，可以从定量和定性两个不同的方式进行隐私泄露的风险评估。

4.2.1 定量方法

隐私泄漏风险的定量评估方法是应用实际发生的概率并使用统计分析的方式来进行估计鉴定。需考虑受试者医疗数据本身的重要性，数据的使用频

次等，对不同的变量进行分析。在该方法中会预先设立一个确定的风险阈值，通过比较实际结果和预设阈值来确认隐私保护的程度。选择定量方法进行风险评估，需要详细的描述所使用的算法和使用参考。

4.2.2 定性方法

在隐私泄漏的风险评估中应用定性方法不需要评估概率，而是使用低/中/高风险的限定词。通常需确定风险级别中事件发生的严重性，主观评价对受试者潜在的社会和经济损害，并鉴定风险的相关的细节信息，以及容易出现某些潜在的隐患。

定量风险评估的速度较慢，原因之一可能是不确定所划定的范围是否足够保护受试者隐私。通常，基于“适应症罕见性”、“患者数量”、“研究地点数量”等特定条件，可以推导出一个风险水平。一般来说，规模小的研究或分中心少的临床试验中，隐私泄漏的风险会增加，在风险评估时对于个人信息的匿名化水平不同，需要特别注意。在确定匿名化方法时，申办方应该仔细考虑这些因素。

4.3 不同监管辖区数据共享的风险

在隐私泄漏的风险评估时，清楚的分析了数据环境，选择了合适的定量和定性的评估方法后，对不同监管管辖的地域实际情况，以及全球多中心的临床试验中不同国家对不同数据的法规要求也是需要考虑的，这些同样影响着隐私泄漏的风险评估和具体合规措施的制订。

4.4 特殊受试者群体对风险评估的影响

从数据环境这个基础出发，在方法论上找到切合的定量或定性的评估方式，加上结合不同监管管辖的地域实际情况对于数据风险的影响管控之外，

由于特殊的临床试验受试者群体的不同特征，隐私泄漏的风险评估工作也需要做到具体情况具体分析。以下述两点为例：

4.4.1 罕见疾病

在罕见疾病中，患者、数据和生物样本尤其稀缺，因此，在这些疾病相关的临床试验中，协作和数据共享的需求是至关重要的。然而，罕见病对数据共享提出了特别的挑战，因为很难在不显著降低数据效用的情况下，从小型试验、小患者群体或具有特定基因突变的人群中进行数据匿名化。隐私泄漏的风险评估中也要考虑到受试者的个人或地理上的接近性的影响。例如，如果邻居或同事意识到受试者患上了罕见的疾病，同时又在网络上发布个人消息等，这些使得隐私泄漏的风险更遥远或更抽象。从患有罕见疾病的受试者角度出发，共享数据的重要条件包括：在批准临床试验之前考虑需要收集的数据；数据收集者将结果置于受控访问环境或公共域共享之前，具备资质的第三方应向数据收集者解释其目标和结果；并在情况发生变化和适当的时候再次征求受试者的同意。

4.4.2 未成年人

由于知识和医疗状况的不同，未成年人在参与临床试验过程中对数据的理解和观点，将会随着年龄的变化而变化。因此，同意数据共享的能力取决于未成年人的成熟程度，以及他们对隐私权的充分了解；另外，考虑到未成年人使用社交媒体的频率与方式，他们作为受试者的隐私泄漏风险可能是增加的。

5 隐私泄露的补救措施

5.1 撤销对个人信息使用的同意

受试者本人或监护人及经授权的家属可提出撤销对受试者个人信息的继续使用。在此情况下，研究申办方或研究者应遵从受试者意愿，尽可能将其数据从总数据集中删除。若数据集已经发表或因各种原因无法删除，应向受试者做出书面说明，并提交伦理委员会备案。

5.2 对泄露信息责任人的处罚

对泄露个人信息或隐私的责任人采取处罚措施，要求其立即停止，赔礼道歉，消除影响，赔偿损失。

5.3 对造成严重后果的侵权赔偿主张

受试者如因个人信息或隐私泄露而导致个人生活受到影响，名誉受到损失，精神受到损害，可依据相关法律法规提起诉讼，主张赔偿。

6 研究各方的职责

6.1 研究者职责

研究者对于受试者隐私保护的认识和态度直接影响受试者隐私保护的实施及效果。妥善保护受试者隐私，既是临床研究的伦理要求，也是研究者与受试者建立信任，确保研究顺利且可持续开展的保证。研究者应主动树立受试者隐私保护的意识，并对受试者隐私保护负重要责任。

研究者对受试者隐私保护的职责贯穿临床研究全程，以下分别介绍在研究的不同阶段需要关注的具体事项。

6.1.1 研究准备阶段

在研究准备阶段，研究者应着重关注研究方案中受试者隐私保护的措施，制定细致可行的隐私保护方法及细则，具体包括哪些人员可以接触到受试者

个人信息及研究数据，其个人信息以何种方式编码及加密，哪些信息需要采取加密方式处理等。

6.1.2 研究进行阶段

在研究进行阶段，研究者应督促其他研究人员（包括研究护士、研究协调员、研究监查及稽查人员等）对受试者隐私进行保护，除保护书面形式的受试者隐私以外，还需要注意避免在公开场合（如办公室）谈论受试者病情及个人情况，避免泄露受试者携带传染病或居住地址、婚育信息等易被忽视的隐私信息；避免委托非研究团队人员随访受试者；尽量避免研究人员频繁更换，以减少必须接触受试者隐私的人员等。

6.1.3 研究完成阶段

在研究完成阶段，研究者应再次核对，确保用于统计分析的数据中涉及受试者个人信息或隐私的信息已经过妥善加密处理，且不包含可直接或间接识别患者身份的其他敏感信息。此外，所有的伦理递交文件以及提交给申办方的文件，包括分中心小结、研究总结等均不会出现受试者的身份信息。记录受试者真实姓名及住院号、身份证号等身份识别信息与受试者编号对应关系的文件由研究者另行妥善保存。为配合研究结果发表而公开研究数据时（如在公共数据库、研究注册网站等），同样需要事先对涉及受试者隐私的信息予以脱敏和加密。

6.2 申办方和数据管理公司责任

6.2.1 构建专业的数据保护框架

构建一个专业的数据保护框架是申办方和数据管理公司必须面对的重要问题，特别是考虑到临床试验技术日益依赖于电子系统以及利用数字化来简化研究操作。“大数据”的使用正变得越来越重要，申办方和数据管理公司正

朝着无纸化和基于风险的监测战略迈进。所有这些因素都对临床试验中的数据隐私保护提出了新的挑战，需要更加仔细和前瞻地规划来确保未来的临床试验遵从性。

6.2.2 全面的评估

由于临床试验涉及对敏感个人数据的处理，因此申办方和数据管理公司需要对受试者隐私数据的影响进行评估。这项评估必须包括:

- 对于受试者隐私数据进行操作和操作目的的描述
- 对受试者隐私数据处理的必要性和比例的评估
- 对受试者的权利和自由的风险评估
- 应对这些风险的措施

6.2.3 专人负责

申办方和数据管理公司有责任和需要任命一名数据保护专员，该专员将负责就保护受试者隐私数据提供建议，监控遵守情况，并充当监管机构的联系人。该专员也需要对所有临床试验相关的文件按照法规要求梳理与保管。

6.2.4 数据操作标准化

由于申办方和数据管理公司在数据操作过程中责任需要明确。参与试验数据流处理的任何一方都需要负有一定程度的义务。其中包括以下义务:

- 对隐私的保护，包括重点数据的脱敏计划
- 执行阶段中数据处理，数据脱敏，隐私泄漏后应对策略等标准 SOP 制定。
- 建立安全可靠数据库/数据共享站点
- 定期的第三方审查小组/指导委员会的审查
- 邀请外部专家审核数据流的安全性

- 尽职调查评估（包括覆盖查找数据过程，标准数据格式，标准数据集评估等。）
- 法规遵循和审计工作（注册和发布）
- 为知情同意书、临床研究报告等创建模板，以便在共享数据时更好地保护受试者的隐私数据

6.2.5 申办方和数据管理公司的重点义务部分

按照《中国人民共和国民法典》第一千零三十五条的要求，处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理，并符合下列条件:

（一）征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外;

（二）公开处理信息的规则;

（三）明示处理信息的目的、方式和范围;

（四）不违反法律、行政法规的规定和双方的约定。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。

因此，在临床试验过程中处理相关数据应尤其注意:

- 合法、公平和透明地处理——当收集数据时，应清楚为什么要收集数据以及数据的用途。必要时，申办方和数据管理公司应提供有关数据处理的详细信息。例如，如果一个受试者询问申办方和数据管理公司的数据保护人员信息，或者申办方和数据管理公司持有受试者的数据范围，那么申办方和数据管理公司应积极解答。

- 目的的限制——申办方和数据管理公司需要有一个合法的方式和目的来处理受试者隐私数据。申办方和数据管理公司不应该收集任何没有特定用途的隐私数据，更不可以违反法规收集特定用途的隐私数据。
- 数据最小化——申办方和数据管理公司所管理的数据必须是足够的、相关的和有限的。根据这一原则，申办方和数据管理公司必须确保它们只存储用于试验项目所需的最低数量的数据。
- 数据处理的准确性——数据保管人员必须确保信息保持准确、有效、适合试验项目的目的。申办方和数据管理公司必须有适当的流程和策略来处理如何维护、处理和存储的数据。
- 存储的限制——为了确保遵从性，申办方和数据管理公司必须控制数据的存储和移动。这包括实行强制的数据保留政策，以及不允许将数据存储在多个位置。在多个位置拥有相同受试者隐私数据的多个非法副本是遵从性的隐患。
- 机密性和安全性——必须通过确保数据的安全性(扩展到电子系统、纸质记录和物理安全性)来保护数据的完整性和隐私。作为受试者隐私数据的收集者及处理者，申办方和数据管理公司应确保采取与受试者权利保护及风险情况相称的保安措施。
- 责任和溯源——申办方和数据管理公司需要有一个适当的流程来管理问责的请求，以及一个完整的审计跟踪流程，以证明采取了适当的操作。

7 受试者隐私保护常见问题

7.1 缺乏隐私保护意识

部分研究者漠视受试者隐私权的同时，受试者本人也缺乏隐私保护意识。这体现在研究者知情告知范围不全面及研究者在言谈中无意识地泄露隐私。而受试者对医患关系的依赖又可能影响到受试者的自主选择。建议普及与宣传隐私泄露所造成的危害，研究各方应树立相应的意识，将受试者隐私保护的理念在研究的全过程中予以贯彻。

7.2 缺乏有效审查监督

伦理审查是保护受试者权益的第一道防线。随着生物医学的发展，项目涉及的专业面及未知领域愈加广泛，受试者权益则愈加受到挑战。目前，伦理委员会一般未纳入信息保密方面的专业人员，且各医疗机构对患者信息的使用普遍缺乏完善的数据安全与监督机制，伦理委员会难以对受试者的医疗数据管理实现干预，对基于项目风险审查受试者隐私保护并保证数据保密性的能力有限。

7.3 存在隐私保护薄弱环节

受试者隐私保护是一项全链条的工作，任何一个节点的隐私泄露都会使其他环节的保护失去意义。目前，对受试者隐私保护的关注集中在数据采集、传输、存储、使用、披露等环节，实际上受试者保险理赔、不良事件处理及受试者补贴发放等环节均可能成为隐私安全的薄弱点，威胁受试者的隐私。

7.4 松散的电子病历及数据库权限管理

随着电子化病案及临床研究资料电子化的日益广泛应用，医疗机构及研究者对受试者隐私的保护越来越受到挑战，医务人员及其他非研究授权人员可通过医院信息终端轻易调出并查阅受试者的医疗病历，其中就包含受试者姓名、地址、家庭成员、传染病携带情况等隐私信息。如何对电子化病历调用及查阅的权限进行更为精细的限制，在临床工作的便利性与患者隐私保护

之间取得平衡，是数字时代下受试者隐私保护面临的最大问题。该问题的解决非朝夕之功，需要医院行政管理部门、信息管理部门及临床研究管理机构、伦理委员会等多方商讨，并不断在“松”、“紧”之间进行调试，改进及革新电子病历管理路径，寻求最佳处理方案。

撰写者及分工情况

章节	起草人
受试者的个人信息和隐私	曹烨
受试者隐私保护的主要环节	廖敏
隐私保护的特殊考量	韩珂
隐私泄露的风险评估	梅昀 谢非
隐私泄露的补救措施	廖敏
研究各方的职责	徐立 曹烨 谢非
受试者隐私保护常见问题	徐立 曹烨 韩珂 梅昀
指导：胡汝为　　统稿：曹烨	

参考文献:

[1] 汪秀琴, 熊宁宁, 刘沈林.临床试验机构伦理委员会操作规程[M].北京:科学出版社, 2006: 22-24.

[2] 科技民生报告丛书——大数据时代的隐私保护第五章大数据时代下如何保护隐私? 第六节隐私泄露后的补救措施[A].2019.

[3] 汶柯, 王瑾, 白楠. 药物临床试验中受试者风险最小化管理探讨[J]. 中国新药杂志, 2015, 24(16): 1862-1866.

[4] 林昕, 周欣. 论如何在药物临床试验中保护弱势群体[J]. 中国医学伦理学, 2017, 30(5): 572-575.

[5] 郭春彦, 王晓玲, 王天有, 等. 涉及儿童的药物临床试验伦理审查要素[J]. 中国临床药理学杂志, 2016, 32(2): 186-189.

[6] 国际医学科学组织理事会, 世界卫生组织.涉及人的健康相关研究国际伦理准则[M].上海: 上海交通大学出版社, 2016.

[7]曾令烽, 刘军, 潘建科, 等. 生物样本研究数据环境与受试者隐私保护伦理问题[J]. 世界科学技术—中医药现代化, 2015, 17(7): 1567-1576.

[8] 美国卫生及公共服务部.《健康保险便利与责任法案》隐私规则[Z].2009.

[9] 张海洪. 健康数据二次使用研究的伦理审查探讨[J]. 医学科研伦理, 2019, 40(3): 26-28.

[10] 管理和共享联邦资助研究所产生的数据存储库所需特征草案[Z].

[11] The World Health Organization. Handbook for Good Clinical Research Practice (GCP): Guidance for Implementation[Z].2007.