

AI 新药研发出海法律实务

第三篇：算法与伦理监管篇——AIDD 算法伦理与参与方责任

作者：潘永建 | 邓梓珊

人工智能(AI)通过降本增效、提高成功率和拓展创新空间，正在从根本上重塑生物新药研发。例如，传统研发一款新药通常需要 10 年时间 和 10 亿美元以上 的投入，其中仅早起研发就需要 4-5 年, AI 的介入能将这一时间缩短至 18 个月左右。

近年来，中国药企形成了“AI 赋能研发+国际多中心临床(MRCT)验证+跨境授权(License-out)”的创新出海新范式。通过 AI 大幅缩短靶点发现与分子优化周期，结合符合国际标准的 MRCT 数据，中国原创药在安全性与有效性上获得了全球监管及跨国药企的高度认可。

在实践规模上，这一模式已进入爆发期。2025 年，中国药企对外授权交易总额突破 1,300 亿美元，占据全球相关交易额的近 50%，授权管线数量超过 150 项。以科伦博泰、百利天恒、英矽智能等为代表的领军企业，通过与默沙东、BMS、阿斯利康等巨头达成数十亿乃至百亿美元级的合作，成功实现了从底层算法创新到全球商业价值兑现的闭环。

与此同时，在当前地缘政治博弈与数字化研发转型的双重背景下，中国生物医药企业借助 AI 开展跨国新药研发及多中心临床研究，正面临着前所未有的复合型法律合规挑战。

- 第一， 境内监管。中国对于人类遗传资源出境、个人信息跨境流转、以及《生物医学新技术临床研究和临床转化应用管理条例》下算法伦理审查与临床研究备案均设有严苛的监管程序；
- 第二， 境外审查。美国《生物安全法案》(BIOSECURE Act)高压下，对中国背景实体施加了供应链“去风险化”(De-risking)与物理隔离的要求；与此同时，美国食品药品监督管理局(FDA)对 AI 辅助决策的算法可解释性与潜在偏见提出了更高的审查标准；

.....
如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com

第三，在 AI 药物研发(AI-Driven Drug Development, AIDD)中，法律通常滞后于技术的突破，然而各类新兴风险——包括算法偏见、AI 幻觉、伦理问责等——却常常在既有法律规则形成之前便已实质性存在。

第四，跨境交易。跨国合作中，围绕算法逻辑等知识产权所有权、数据主权归属问题，已成为双边博弈的焦点，进一步加剧了交易结构的法律复杂性。

从以下四个维度，本系列文章旨在赋予中国生物医药企业一双“慧眼”，识别 AI 新药研发商业化的市场蓝海中的法律合规风险“暗礁”。

1. 地缘政治与准入篇：重点分析《生物安全法案》对 AIDD 许可合同条款的改变，以及“清洁子公司”下的实质性运营合规等问题。
2. 数据合规篇：重点解析个人信息保护与数据安全视角下人遗办(HGRAC)审批备案、网信办(CAC)安全评估，以及联邦学习、隐私求教计算等技术解决方案。
3. 算法监管与伦理篇：深度解读《生物安全法》《生物医学新技术临床研究和临床转化应用管理条例》《科技伦理审查办法(试行)》等对 AI 算法风险评估报告的具体要求及临床责任划分。
4. 核心资产博弈篇：探讨许可与商业权益合同中 AI 模型所有权与数据权等实务操作。

如您希望与作者对本主题相关问题进行进一步深度讨论，或索要具体落地文件(例如《AIDD 合规尽调清单》)，请与本文作者联系。

AI 新药出海法律实务

第三篇: AIDD 算法伦理与参与方责任

随着 AI 的应用场景从“研发辅助”延伸至临床“辅助决策”，对 AIDD 的监管重点已从数据合规上升至算法安全与医疗伦理。本文旨在分析中国法下 AI 算法的可解释性合规要求、知情同意的重构，以及当 AI 决策导致临床不良事件时，药企、AI 服务商与医疗机构之间的法律责任划分。

一. 伦理规制

(一) 框架制度

《数据安全法》《生物安全法》《生物医学新技术临床研究和临床转化应用管理条例》以及《科技伦理审查办法》四部法规从数据源头、技术属性、临床转化到价值导向，对 AI 算法模型实施了全维度的伦理规制。

《数据安全法》与《生物安全法》构筑了算法伦理的底层安全基石。前者强调算法在处理大规模生物数据时必须遵循“合法、正当”的原则，严禁利用算法漏洞从事危害国家安全或公共利益的数据处理活动；后者则将算法伦理提升至国家生物安全高度，特别是在处理人类遗传资源(HGR)信息时，算法被要求具备高度的可控性与溯源性。换言之，任何涉及中国人群基因特征的算法模型，在进行跨境披露或授权时，其伦理评估必须重点关注是否会损害中国国家生物主权，

算法的逻辑输出是否危害生物物种安全或公众健康。对于 AI 生物医药公司而言，如果其算法模型是基于大规模中国人群的基因组或临床数据训练而成的，那么该模型的权重、参数等核心逻辑极可能被界定为“利用人类遗传资源产生的数据信息”。将此类算法逻辑披露给境外药厂，已不再属于单纯的商业行为，而构成受监管的数据出境行为。此类行为不仅需要通过国家网信办的数据出境安全评估，还可能根据技术的敏感程度，触发《出口管制法》下的技术出口许可。为合规之目的，企业必须遵循“审批早于披露”的原则，确保再技术交付期已对算法的生物安全影响完成评估并取得相应许可。

《生物学新技术临床研究和临床转化应用管理条例》明确规定，AI 辅助的生物学技术在进入临床转化阶段前，必须接受严格的风险评估。对于涉及基因编辑、细胞治疗等高风险领域的算法应用，监管要求其必须具备极高的透明度与可解释性，以防止因算法预测偏差引发不可逆的临床损害。在此情形下，算法伦理的核心原则可概括为“医学获益大于风险”，这要求中国药企在与境外药厂合作时，必须证明其算法建议的科学性与安全性已通过国家级行政许可及专家论证，而非仅仅依赖机器预测结果作为临床决策依据。

《科技伦理审查办法》正式将算法纳入科技伦理审查范畴，要求从事相关研发活动的企业必须设立科技伦理委员会，对算法进行前置审查。在跨境授权场景下，该办法要求企业对算法可能产生的偏见、歧视以及对人类尊严的影响进行专项评估，特别是针对生物医药领域可能存在的样本偏差问题。根据该办法的要求，药企在披露算法时，不仅要交付代码本身，还须提交一份涵盖算法逻辑、数据来源及社会影响评估的《科技伦理审查报告》，以确保技术出境符合“尊重生命、公平公正、风险控制”的公认的伦理规则。

(二) 风险分级

《生物学新技术临床研究和临床转化应用管理条例》最终未采纳其征求意见稿中“风险分级”规定，但这并不意味着监管部门对算法伦理的规制有所放宽。相反，这一变化标志着中国对前沿技术的监管逻辑已从“静态的条文罗列”转向了“动态的清单管理”。究其原因，AI 与生物医药技术的迭代速度远超立法周期，难以在行政法规层面预先设定固定的风险等级。因此，相关监管机制应通过跨部门的统筹机制，将风险分级管理的实质要求嵌入到更为具体的专项规章之中。

《科技伦理审查办法》已体现这一监管思路。该办法的规制体系采取了以“特征判定”取代“条文目录”的策略：凡是涉及对人类生命健康、生物安全具有潜在重大影响，或处理大规模敏感个人信息的 AI 算法活动，因其技术特征而被自动纳入“科技伦理高风险清单”，接受严苛监管。在此框架下，AI 制药公司必须从被动等待官方定级转向主动的合规治理，建立完善的内部科技伦理委员会，并根据算法的应用场景、数据敏感度及决策影响力，自主建立一套科学的伦理风险自我评价体系。

AI 辅助药物设计，尤其是在涉及基因编辑、合成生物学等前沿领域时，往往被列入“科技伦理高风险清单”。这要求中国药企必须建立内部科技伦理委员会，开展严谨的模型风险评估。评估重

点包括算法的透明度、数据偏见、以及训练数据来源的合法性。在与国际药企合作时，提供一份《科技伦理审查报告》已与提供专利证明具有同等重要性，它证明了 AI 生成的先导化合物在研发阶段未违背生命伦理基本原则，从而降低了境外合作伙伴在国际市场面临的监管合规风险。

二. 临床研究责任的划分

(一) AIDD 下临床研究责任

临床研究事故的责任分配通常遵循“申办方最终负责、临床专家把关、技术方过错追偿”的原则。根据中国《药物临床试验质量管理规范》(GCP)，中国药企作为申办方，是对受试者安全与试验质量承担第一责任的法定主体。即便事故是由 AI 算法的“幻觉”或错误用药建议引发，申办方也必须首先完成对受试者的赔偿。与此同时，医院作为研究机构负有“临床最终决策”层面的注意义务。由于医生拥有对用药指令的终审权，如果 AI 给出的建议明显违背医学常识(如剂量严重超标)而医生未能纠正并予以实施，医院需承担相应的医疗过错责任。相比之下，AI 模型供应商的责任通常界定为过错责任：若其已通过科技伦理审查并履行了合理的风险提示义务，算法偶发的随机“幻觉”在现有技术条件下往往被视为研发过程的固有风险，而非必然导致技术方的侵权责任。

在跨境许可场景下，作为许可方的中国药企与作为被许可方的境外药厂之间的责任划分更加复杂。通常，AI 公司负责算法研发阶段的“技术真实性”与“伦理合规性”，而临床试验的最终法律责任则随着权益转让转移至医疗机构和全球合作伙伴。然而，若算法存在“隐性缺陷”并引发非预期的临床毒性，可能导致巨额的违约责任或侵权指控。因此，授权协议中必须嵌入细化的赔偿条款：中国药企通常承担境内的合规义务(如人类遗传资源备案、国内伦理审批)，而境外合作伙伴则承担在海外临床应用这些 AI 工具的“操作性风险”。

(二) 合同约定与救济

对于中国药企而言，临床事故引发的研究停滞或数据失效，往往会导致对境外药厂(被许可方)的里程碑交付出现延误。在跨境授权协议(Out-licensing)中，此类延迟原则上不能作为免责事由。研发过程中的技术故障、AI 错误或临床意外，在法律上通常被归类为“商业风险”而非“不可抗力”。除非事故触发了政府监管部门(如国家药监局)下令整体关停研发项目的行政指令，且该指令超出了药企的合理预见与控制范围，否则药企很难主张“监管不可抗力”以豁免对境外合作方的违约责任。因此，在合同谈判中，中国药企应积极争取设置“补救期”条款，或在风险披露中预先列明 AI 技术的不确定性，以减轻交付延迟带来的赔偿压力。

当中国药企对外承担赔偿责任后，其向内部合作伙伴追偿的能力在很大程度上取决于合同具体约定。在向 AI 供应商追偿时，药企常面临供应商设置的“责任限额条款”(如赔偿额上限为服务费总额)的阻碍。要突破此类限制，药企必须证明供应商存在重大过失，例如模型未按约定进行算法备案、存在已知未披露的缺陷，或违反了《科技伦理审查办法》中的合规义务。而针对医院的

追偿，关键在于证明研究者违反了试验方案或未尽到专业核查义务。为了降低求偿难度，药企在签署三方协议时，应明确将“算法验证”设为医生的强制性操作节点，并引入专门的临床试验保险来覆盖因“算法错误”引发的第三方损害赔偿。

三. 应对要点

(一) AI 算法合规

中国药企在临床试验启动前，必须完成专项风险评估报告。该报告必须证明算法已通过多样化族裔测试。对于中美多中心研究，这意味着必须证明 AI 在亚洲人群和欧美人群中能表现出一致的预测效能，从而防止产生“人口统计学偏见”。此外，报告还必须明确定义“人工覆盖协议”，界定 AI 在何种情况下必须停止自主运行，并移交医生进行最终确认或否决。

细节往往决定成败。AIDD 下部分传统的合规做法已难以满足监管要求，中国药企应充分注意这些细节。例如，传统药物研发的知情同意(ICF)应提升至受试者“决策同意”高度，即受试者必须被明确告知 AI 参与了其治疗方案的选择，并拥有要求研究者提供“人类可理解的解释”的权利；根据《个人信息保护法》和《生物医学新技术临床研究和临床转化应用管理条例》，受试者应有权选择退出 AI 筛选，并要求临床团队进行人工手动复核，且不应因此受到任何歧视性对待。

(二) 合同条款设计

中国药企宜在专业律师的支持下，通过合同条款将 AI 算法应用于临床研究所产生的不确定责任在相关方之间进行最大限度的合理分配；否则，相关责任将依法由药企独自承担。为此，我们建议中国药企在合同中考考虑纳入如下保护机制条款：

1. 明确 AI 的“辅助工具”定位与技术免责

在合同的“技术描述”或“陈述与保证”章节中，明确写明“该 AI 算法系基于概率学和统计学模型构建，双方承认其在运行过程中存在发生‘算法幻觉’及固有偏差的科学可能性”。这一条款旨在防止境外药厂在后期以“交付的技术存在欺诈或根本缺陷”为由，要求退还已收取的首付款。

2. 设置“勤勉尽责”标准，而非“结果保证”

针对带有 AI 辅助的临床里程碑，中国药企应坚持适用“商业上的合理努力(Commercially Reasonable Efforts)”标准，而非绝对的“结果保证”。根据这一条款，只要中国药企能证明其在算法训练、数据清洗、日常维护中已尽到了行业公认的审慎义务，即使最终因算法偏差导致数据未达预期或出现轻微延误，也不构成根本性违约。

3. 里程碑日期的“弹性延展期”

为每个 AI 参与的临床里程碑设置 60 天以上的补救期(Cure Period)或宽限期(Grace Period)。一旦 AI 出现偏差导致数据需要重新跑批、清洗或小规模追加临床病例, 中国药企应享有合法的缓冲时间去修正算法, 而不直接触发违约赔偿或合同终止。

4. 责任上限与间接损失免责

对因 AI 错误所导致的损失赔偿总额予以严格限制, 其上限不超过中国药企在该阶段已收取的累计款项(或双方约定的一定比例)。同时, 必须明确排除“间接损失、预期利润损失以及因丧失后续商业机会”所产生的损失赔偿责任。

5. 数据污染与输入责任切分

如果 AI 模型的训练或运行需要依赖境外药厂提供的患者数据、靶点参数或历史临床指标, 应设定数据污染免责条款, 以避免境外药厂在提供低质量数据(即“垃圾输入, 垃圾输出” Garbage in, Garbage out)后, 向中国药企索赔。

如您希望就相关问题进一步交流，请联系：



潘永建
+86 21 3135 8701
david.pan@llinkslaw.com



邓梓珊
+86 21 6043 3793
susan.deng@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市朝阳区光华东里 8 号
中海广场中楼 30 层
T: +86 10 5081 3888
F: +86 10 5081 3866

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: Llinkslaw

本土化资源 国际化视野

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2026