

AI 新药研发出海法律实务

第二篇：数据合规篇——《AIDD 场景下个人信息保护与数据安全》

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

第二篇: AIDD 场景下个人信息保护与数据安全

在生物医药与人工智能深度融合的今天，数据已成为核心生产要素。中国对人类遗传资源(HGR)及敏感个人信息的监管已进入“精细化治理”时代。对于中国 AI 药企而言，如何在严守“数据安全”红线的前提下，实现算法模型的全球化迭代？本文将深入拆解“人遗办”审批、数据出境安全评估以及隐私计算技术在跨境研发中的合规应用。

一. 特殊类型数据监管

(一) 人类遗传资源

中国人类遗传资源管理办公室(简称“人遗办”)最早成立于 1998 年，由科技部与原卫生部联合设立，设在科技部。起初，其监管依据是《人类遗传资源管理暂行办法》，旨在应对当时国际科研合作中出现的中国遗传资源流失风险。2019 年，国务院正式施行《中华人民共和国人类遗传资源管理条例》，标志着监管进入法治化轨道。2023 年机构改革后，相关职能由科技部划转至国家卫生健康委员会，进一步强化了人遗资源在生物安全与公共卫生维度的战略地位。

针对药物研发中的人类遗传资源的跨境行为，中国确立了严密的审批与备案制度：(1)外国组织、个人及其实际控制的机构(外方单位)在中国境内采集、保藏或利用人遗资源，必须与中方单位进

行国际合作开发; (2)若合作是以上市为目的临床试验、不涉及材料类人遗资源出境且不产生知识产权分享, 通常履行备案手续即可; (3)若合作涉及信息类人遗资源的出境或向境外机构开放使用, 应进行事先报告并提交信息备份; (4)若涉及大规模采集、保藏或将人遗资源材料出境, 则必须经过严格的行政审批。

中国 AI 药企在开展 AI 训练中涉及的基因序列、基因组、转录组、表观组及 ctDNA 等核酸类生物标志物等数据信息属于受监管的人类遗传资源信息。如中国药企在训练模型使用了第三方数据库或医院合作数据中的人遗资源信息, 需核查原始采集是否(需)经过人遗办审批; 如向外方单位提供、开放使用或转让人遗信息(如处理后的基因序列、突变位点等)的, 须向卫生健康行政部门提交报告并将信息备份; 若提供的信息达到特定规模(如涉及 500 人以上的全基因组测序等), 或可能影响国家安全、社会公共利益, 必须通过专门的安全审查。

实践中, 中国药企可能忽略“隐形”风险。例如, 在 AI 研发中使用境外公有云(如 AWS、Azure)处理中国人遗数据, 或外方单位通过 API 接口调用中方服务器上的人遗信息进行模型调优, 即便数据不实际发生跨境, 也可能构成“对外提供使用”, 需履行报备手续。再如, 虽然人遗办尚未明确 AI 训练模型使用的参数本身是否属于人遗信息, 但若模型中包含可还原的敏感基因特征, 可能被视同为人遗信息出境, 因而需履行事先报告及安全审查。

(二) 个人信息

在靶点发现和临床研究等阶段, 除基因信息外, AI 模型处理的数据广泛涉及多组学数据(如蛋白质组学、代谢组学、转录组学)、临床记录(病史、诊断记录、用药史、生化检测结果)、医学影像资料(CT/MRI); 以及人口统计学信息(年龄、性别、种族、地理位置, 其中地理位置常作为群体遗传学的特征变量)。

中国药企必须识别上述数据中的个人信息, 特别是生物识别数据等敏感个人信息。针对敏感个人信息, 中国药企必须更新知情同意书(ICF), 明确告知受试者其数据不仅用于临床研究, 还将在经过技术处理后用于“全球 AI 模型的联合训练”; 不仅要告知受试者数据的采集范围, 还要以显著方式告知 AI 算法可能对数据进行的自动化处理逻辑及其对个人后续的所有 AI 模型训练.....。

实践中, 中国药企往往通过加密、伪掩码等手段, 使数据在不借助额外信息的情况下无法识别特定自然人, 即实现个人信息的去标识化。尽管如此, 去标识化后的数据仍属于受法律监管的个人信息, 作为处理者的企业仍需履行个人信息全生命周期合规义务。更进一步, 有企业采取匿名化手段, 使得数据无法被还原且无法关联至特定个人, 依法完成匿名化的数据不再属于个人信息, 可免于适用个人信息保护相关义务。需要提醒的是, 信息类人类遗传资源(如基因数据)作为特殊类型的敏感个人信息, 由于其具有唯一性和不可逆识别性, 即使是匿名化后, 其仍可能构成个人信息; 并且, 基因信息涉及国家安全与公共利益, 处理者还需依法履行前文所述的审批、备案等手续, 不会因匿名化为由豁免。

中国药企应理解，个人信息合规不是企业“不得已而为”，而是构建合法、稳固的算法模型资产的法律基础。如果个人信息处理不合规(例如“非法收集”)，可能影响整个项目下的算法模型的知识产权在合法性上产生瑕疵，进而影响其确权和商业化利用。作为个人信息合规的抓手，企业自开展模型训练或向第三方授权使用数据前，**必须**开展并留存个人信息保护影响评估记录，重点评估处理敏感个人信息的必要性、对个人权益的影响及风险、数据接收方(被许可方，如大药厂)的数据安全保障能力。

二. 算法出境、可解释性

中国药企开展 AIDD 并开展跨境授权(Out-licensing)的业务场景中，涉及算法披露与数据流转的合规性主要受《互联网信息服务算法推荐管理规定》《数据出境安全评估办法》以及《出口管制法》等多重法律框架约束。因此，中国药企应从业务属性、数据敏感度及技术管制目录三个维度综合研判算法备案、安全评估问题。

在算法备案方面，目前的合规要求具有较强的针对性。根据《互联网信息服务算法推荐管理规定》，只有具备“舆论属性”或“社会动员能力”的算法推荐服务才强制要求在官方系统进行备案。医药研发领域的靶点筛选算法或临床分析模型，本质上属于辅助科学研究的工具，若仅用于内部研发或特定 B2B 商业合作，通常不属于强制备案的范畴。然而，如果该 AI 平台具有生成式 AI 功能(如自动生成医疗建议)或向不特定公众提供服务，则可能触发生成式人工智能算法备案的要求。

相较于算法备案，数据出境安全评估则是此类交易中不可回避的核心环节。由于药物研发涉及大量的临床试验数据，这些数据往往包含特定量级受试者的个人健康信息，极易触及“敏感个人信息”或“重要数据”的法律底线。根据国家网信办的相关规定，若中国药企处理的个人信息达到法定阈值(如累计向境外提供超过 100 万人的个人信息或 10 万人的敏感个人信息)，或者所提供的算法模型参数与训练数据被认定为影响国家安全的重要数据，则必须向国家网信部门申报数据出境安全评估。

除了前述的国家层面的监管要求，中国近年来在自贸区开展的制度创新，特别是上海自贸区临港新片区实施的“数据跨境分类分级管理”制度，为医药企业的国际化协作提供了更为高效的替代选择。对于注册在临港新片区(或自贸区)内的生物医药企业而言，如果其数据出境行为落入区域性的“一般数据清单”(即“白名单”)范畴，则有望在很大程度上简化乃至豁免前述繁琐的国家级安全评估程序。

临港新片区针对生物医药领域发布的《场景化一般数据清单》，将药物研发、临床试验、药物警戒及商业合作伙伴管理等核心场景下的特定数据字段定性为“一般数据”。在该框架下，中国药企在与大药厂进行在研药物商业化权益许可(Out-licensing)时，所涉及的试验方案、研究者信息、安全性报告以及非敏感的合规管理数据，只要在清单界定的范围内，企业仅需向临港新片区管委会履行简单的登记备案手续，即可自由开展跨境传输。这一制度显著降低了初创型 AI 制药企业进入国际市场的合规门槛，避免了长达数月的国家级安全评估周期。

然而，企业在享受自贸区政策红利时，仍需划清“一般数据”与“红线数据”的边界。尽管自贸区简化了流程，但若算法模型涉及人类遗传资源(如基因组数据)的深度处理，或临床数据规模达到“重要数据”

的界定标准，则依然必须回归到《人类遗传资源管理条例》及国家网信办的严苛审批程序中。此外，即便在自贸区内，算法作为核心知识产权的“技术转移”属性并未改变。如果相关 AI 算法被列入《中国禁止出口限制出口技术目录》，公司仍须严格履行商务主管部门的技术出口许可手续，确保技术资产的披露符合国家出口管制政策。

简言之，中国药企在谋求海外商业化合作时，应采取“国家级合规为底线、地方性政策为支撑”的双轨策略。若企业具备入驻临港等特定自贸区的条件，优先利用“一般数据清单”完成临床数据的跨境合规，同时针对核心算法进行专项的技术出口合规审查，将是目前最为高效且稳妥的商业路径。

此外，考虑到算法本身可能构成国家出口管制目录下的“禁止/限制出口技术”，公司在披露核心源代码或关键逻辑前，还需核查《中国禁止出口限制出口技术目录》，并在必要时申领《技术出口许可证》。

三. 技术合规

数据不仅事关个人信息主体权益，更涉及国家安全与公共利益。在跨国 AIDD 业务模式中，中国药企常因不同国家之间的数据主权博弈而陷入两难合规困境。例如，在许可合同中，中国药企经常遭遇审计权的“双向夹击”：一方面，大药厂根据《生物安全法案》(BIOSECURE Act)的要求，主张对中国药企实验室进行穿透式审计，包括调取原始服务器日志、查看研究员身份信息及算力资源分配记录；另一方面，中国《数据安全法》及《人类遗传资源管理条例》严禁在未获批准的情况下，向外国司法或执法机构提供境内存储的数据，且审计活动不得涉及国家秘密或重要数据。这要求中国药企在合同谈判中审慎设计审计条款，在满足境外合规审查需求与坚守境内数据安全底线之间寻求平衡。

徒法不足以自行，技术手段日益成为法律合规的重要延伸。以个人信息出境安全评估/标准合同备案为例，中国药企可考虑采用联邦学习技术，通过“数据不动模型动”的架构而实现境内外联合研发。在此情形下，即便原始数据未离开中国服务器，传输的“梯度(Gradients)”(即经过差分隐私加密后的参数)不构成个人信息，但企业需要在《算法风险评估报告》中进行充分论证。在多中心研究中，中国企业可利用隐私求交计算技术(PSI) 对比中美受试者的入组特征，可在不泄露各自原始名单的前提下完成相关性分析，这可有效规避跨国数据共享合规风险。

结语

AIDD 业务模式中，中国药企应充分认识数据合规的重要性：数据合规不仅是保护私益需要，并且是国家数据主权框架下的法定监管底线。中国药企应将数据全生命周期保护融入新药研发的“底层设计”，实现合规与研发的一体化融合。

具体而言，在事前审批方面，宁可推迟研发进度，也绝不触碰人遗出境的底线；从技术兜底角度，优先采用联邦学习等去中心化技术，从源头上减少原始数据的跨境流转需求；在交易合同中：应在跨境合作协议中明确数据主权属于中国，合作方(大药厂)仅享有模型输出结果的使用权，而不对底层原始数据主张任何权利。

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