生成式人工智能医学语料库：数据风险、合规义务及应对方案

王 蕾[1,2] 刘 苗[2] 王 茜[1] 赵琬清[1] 胡佳慧[1] 方 安[1]

（[1] 中国医学科学院医学信息研究所/图书馆 北京 100020 [2] 北京科技大学 北京 100083）

〔摘要〕 **目的/意义** 探讨我国生成式人工智能医学语料库的合规义务及风险应对方案，进一步推动该领域语料库合规建设。**方法/过程** 根据生成式人工智能语料库数据生命周期，按阶段梳理服务提供者的合规义务，并针对隐私泄露、训练数据偏倚、知识产权风险提出应对方案。**结果/结论** 应以合法性为基准，遵守目的限制与最小必要性原则、数据主体权利保障原则、数据安全与风险防控原则，采用自动化辅助手段，应对生成式人工智能医学语料库构建与管理面临的各类风险。

〔关键词〕 生成式人工智能；医学语料库；数据合规；合规义务；风险应对

〔中图分类号〕 R－058 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673－6036.2026.01.002

Data Risks, Compliance Obligations and Countermeasures for Medical Corpora in Generative Artificial Intelligence

WANG Lei[1,2], *LIU Miao*[2], *WANG Qian*[1], *ZHAO Wanqing*[1], *HU Jiahui*[1], *FANG An*[1]

[1] *Institute of Medical Information/Library, Chinese Academy of Medical Sciences & Peking Union Medical College, Beijing 100020, China;* [2] *University of Science and Technology Beijing, Beijing 100083, China*

〔**Abstract**〕 **Purpose/Significance** To explore the compliance obligations and risk mitigation strategies relevant to medical corpora in generative artificial intelligence (GenAI) in China, and to promote the compliance construction of corpora in this field. **Method/Process** Based on the data lifecycle of corpora in GenAI, the compliance obligations of service providers are sorted out by step. Targeted solutions are proposed to address three major risks: privacy leakage, training dataset bias, and intellectual property risks. **Result/Conclusion** It should be emphasized legality as the foundation, following key principles such as purpose limitation and data minimization, data rights protection, data security and risk prevention and control. Automated auxiliary means should be adopted to address various risks faced in the construction and management of medical corpora in GenAI.

〔**Keywords**〕 generative artificial intelligence (GenAI); medical corpora; data compliance; compliance obligations; risk mitigation

〔修回日期〕 2025－12－19

〔作者简介〕 王蕾，副研究员，发表论文 16 篇；通信作者：方安，研究馆员。

〔基金项目〕 中央级公益性科研院所基本科研业务费（项目编号：2024－ZHCH630－01）；中国医学科学院医学与健康科技创新工程项目（项目编号：2021－I2M－1－057）；中国医学科学院/北京协和医学院医学信息研究所/图书馆青年人才培养专项（项目编号：2024YT08）。

1 引言

语料库是生成式人工智能服务大语言模型训练的基础，构建高质量语料库是提高生成式人工智能服务水平、降低“幻觉”的重要途径。但是，医学语料库构建面临隐私泄露、训练数据偏倚和知识产权等方面的数据风险。对此，有研究通过向大模型提问[1]、分析风险的表征与特征[2]、对比分析不同模型在不同场景中的应用价值[3]、划界区分风险[4]等方法，开展针对医学大模型发展现状[5]、应用价值[6]、应用技术[7]、潜在风险[8]、应对策略[9]、法律责任[10]等方面的研究。然而，上述研究多聚焦模型或应用层面的风险识别与规范回应，对服务提供者应遵守的合规义务要点和数据风险应对方案仍讨论不足。因此，本研究从隐私泄露、训练数据偏倚和知识产权 3 方面分析生成式人工智能医学语料库的数据风险，基于数据生命周期梳理各阶段合规义务，并针对医学语料库的多重数据风险提出应对方案。

2 生成式人工智能医学语料库的数据风险

2.1 隐私泄露风险

医学生成式人工智能服务提供者在模型预训练、模型微调及模型服务中均面临隐私泄露风险[11-12]。隐私数据一旦泄露，不仅影响服务提供者的社会声誉，导致其受到处罚，还可能引发国家安全问题。生成式人工智能医学语料库的隐私泄露风险主要与数据类型、数据来源有关。数据类型方面，医学语料库数据包括临床数据、医学科学数据和医学科技文献等。其中，临床数据包含敏感个人信息，反映个人生理及心理状态、疾病史、遗传信息、治疗过程等。相较于非临床数据，临床数据（如罕见疾病、基因序列）去标识难度大[13]，例如罕见病数据几乎不能真正实现匿名。数据来源方面，医学语料库中既包括服务提供者自建的医学数据资源、从第三方采集的医学数据资源，也包括服务过程中使用者输入的提示词和文档等。对于采集的数据，可采取去识别化降低隐私泄露风险。但对于服务过程中使用者输入的文本、图像、文档等，与个人行为日志、浏览记录等类型数据相比，个人信息及敏感个人信息的识别和处理难度更高。

2.2 训练数据偏倚风险

训练数据偏倚影响医学生成式人工智能服务算法的公平性，导致生成结果存在种族和性别偏见、地区差异等负面情况。其成因主要是使用了缺乏多样化、对边缘化或弱势群体代表性不足的数据集来训练模型[14-15]。因此，在需要强解释、高透明的医学领域，生成式人工智能服务提供者应重视训练数据的偏倚风险，以训练可靠的生成式人工智能服务模型。

2.3 知识产权风险

知识产权风险是指相关主体侵犯知识产权引发的医学语料库数据合法性存疑、输出结果版权归属存在争议的情况[16-19]。医学语料库知识产权侵权风险主要集中在狭义的著作权和著作邻接权领域。以医学科技文献为例，一方面，期刊论文、专著、会议集等出版物作为文字作品，受狭义著作权保护，其作者署名权、保护作品完整权及复制权、改编权、汇编权[20]、信息网络传播权等人身权与财产权，均可能在未经授权的数据采集、模型训练、模型输出中被触及；另一方面，出版商与数据库平台往往享有医学科技文献的专有出版权等著作邻接权，如果未获得平台许可便抓取科技文献的元数据、全文用于语料库构建，可能构成对其邻接权的侵害。因此应同时关注作者、出版商与数据库平台 3 方的权利结构及其潜在冲突点，合理合法地获取数据，以开展语料库构建、相关模型训练及结果输出。

3 生成式人工智能医学语料库的数据合规义务

3.1 我国医学语料库数据合规义务体系

为了维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，我国已经形成并逐步完善生成式人工智能医学语料库的数据合规义

务体系。《生成式人工智能服务管理暂行办法》《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》《深圳经济特区人工智能产业促进条例》《新一代人工智能发展规划》《新一代人工智能伦理规范》《全球人工智能治理倡议》《网络安全技术 生成式人工智能预训练和优化训练数据安全规范》等法规、倡议和国家标准进一步明确了人工智能信息服务的具体合规义务。

根据合规义务的性质，我国医学语料库的数据合规义务可划分为强制性合规义务和非强制性合规义务。强制性合规义务指生成式人工智能服务提供者必须遵守的法律法规，由我国现行相关法律法规组成，如《民法典》《网络安全法》《数据安全法》《个人信息保护法》《基本医疗卫生与健康促进法》《生成式人工智能服务管理暂行办法》等。非强制性合规义务指生成式人工智能服务提供者可以参考执行的标准、指南、倡议等，如《网络安全技术 生成式人工智能预训练和优化训练数据安全规范》《信息安全技术个人信息去标识化指南》。

3.2 基于数据生命周期的数据合规义务要点

生成式人工智能医学语料库的构建及使用包括原始数据获取、训练数据加工、训练数据存储、训练数据输出 4 个主要环节。原始数据获取阶段，通过多种渠道完成数据采集和汇聚。训练数据加工阶段，对原始素材进行数据标注、质量校验、token 化等操作，确保数据符合生成式人工智能模型训练要求。训练数据存储阶段，存储原始数据及加工后数据。训练数据输出阶段，收集生成式人工智能服务使用者输入的信息，并输出结果。在上述数据生命周期视角下，每个阶段均应满足我国生成式人工智能医学语料库数据相关合规义务要点，见图 1。

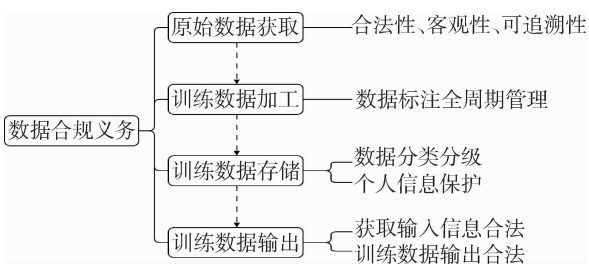

图 1 数据生命周期视角下的医学语料库数据合规义务要点

3.3 原始数据获取阶段的合规义务

用于医学生成式人工智能模型训练的原始数据应具备来源合法性、客观性和可追溯性。一是来源合法性，源数据须符合国家及收集对象对资源的各项要求。《生成式人工智能服务管理暂行办法》明确要求服务提供者使用的源数据具备合法来源，不可侵害他人依法享有的知识产权。训练语料的采集还应符合数据权益相关方的数据获取和使用范围要求。以运用科技文献构建医学语料库为例，既要严格遵守《著作权法》《反不正当竞争法》等法定规范，还要遵循科技文献出版机构、科技文献集成服务平台等被采集对象的资源获取及资源再加工许可协议，充分研究出版商、文献服务平台、期刊对元数据、全文采集的授权和限制性要求。《基本医疗卫生与健康促进法》第九十二条强调保护公民个人健康信息，禁止非法收集、使用、泄露医疗数据。因此服务提供者还要重点保障个人健康信息的来源合法性。二是客观性，原始数据能客观完整反映实际情况，即原始数据种类、来源多样，不存在偏见歧视等情况。根据《新一代人工智能伦理规范》等要求，避免可能存在的数据偏见。三是可追溯性，指原始数据的可审计、可追溯，是长期防范各种风险的重要合规义务。例如，数据采集过程应确保采集结果与实际内容一致，支持对采集结果范围、质量的定期评估。

3.4 训练数据加工阶段的合规义务

训练数据指用于训练生成式人工智能服务模型的标注或者基准数据集。训练数据加工阶段的合规义务强调提高医学语料库的数据质量，以应对训练数据偏倚风险。《生成式人工智能服务管理暂行办法》要求采取有效措施提高训练数据质量。《人工智能面向机器学习的数据标注规程》进一步提供了“前期准备－任务执行－结果输出”的语料数据标注框架流程和实施细则。因此可通过全周期管理提高数据质量，更好地满足生成式人工智能模型需求。前期准备阶段，应确定标注任务、开展标注任务评估、记录标注需求变更，还应明确标注人员范

围、开展标注人员培训、建立标注人员能力档案，营造有效的标注环境。任务执行阶段，开展标注过程控制，采用多种手段检测标注质量，进行一致性检测，建立有效的标注管理机制，进而保证数据质量。结果输出阶段，应进行内部质检，并定期维护数据。

3.5 训练数据存储阶段的合规义务

数据分类分级保护可降低个人隐私泄露风险。《数据安全法》第二十一条提出根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。《互联网信息服务深度合成管理规定》要求深度合成服务提供者和技术支持者应当加强训练数据管理，采取必要措施保障训练数据安全；训练数据包含个人信息的，应当遵守个人信息保护的有关规定。因此，标注任务开始前和用于模型训练前，应按照《数据安全法》等法律法规、参考《数据安全技术 数据分类分级规则》《卫生健康数据分类分级要求》等标准开展医学生成式人工智能训练数据的分类分级。涉及个人信息的，应遵循《个人信息保护法》《关于落实卫生健康行业网络信息与数据安全责任的通知》等要求。《个人信息保护法》第五十一条规定个人信息处理者应当根据个人信息处理的目的、方式、个人信息种类、对个人权益的影响、可能存在的安全风险等因素，采取相应的管理和技术措施，保障所处理的个人信息安全。《关于落实卫生健康行业网络信息与数据安全责任的通知》强调要落实网络信息与数据使用方的责任，确保数据可管、可控、可追溯以及数据的保密性、完整性和可用性，切实保护个人数据隐私。此外，训练数据存储还应根据《个人信息保护合规审计管理办法》定期展开合规性审计，并参照《建立术语数据库的一般原则与方法》《国家卫生信息资源分类与编码管理规范》等标准建立定期更新机制，确保数据的时效性与可追溯性。

3.6 训练数据输出阶段的合规义务

在训练数据输出阶段，生成式人工智能服务提供者收集使用者输入信息、提供大模型输出结果的过程应遵循多项相关规定，以应对隐私泄露风险、训练数据偏倚风险和知识产权风险。一是在收集生成式人工智能服务使用者输入信息的过程中要遵循《民法典》《数据安全法》《网络安全法》《个人信息保护法》《网络数据安全管理条例》等法律法规的规定，取得个人信息被收集者的同意。同时，应履行保障其收集信息安全性的义务，不得泄露、篡改、毁损其收集的个人信息，且在向他人提供个人信息前，应经过被收集者的同意。二是输出结果应遵循《生成式人工智能服务管理暂行办法》及相关法律法规要求，生成内容不得包含违反法律法规的内容。同时，基于医学生成式人工智能的服务特点，采取有效措施，不断提升服务透明度，提高生成内容的准确性和可靠性。三是在提供大模型输出结果时，应遵循《著作权法》《专利法》《反不正当竞争法》《信息网络传播权保护条例》等法律法规，充分尊重权利人依法享有的著作权、专利权及相关竞争性权益，防止未经授权内容的复制、改编或信息网络传播，同时避免生成披露他人商业秘密等侵害他人合法权益的内容。

4 医学生成式人工智语料库数据风险应对方案

4.1 基本原则

医学生成式人工智能语料库数据风险应对方案由基本原则、应对措施和技术手段 3 部分组成。在语料库建设过程中，合法性原则始终是基础性前提，也是高质量语料库建设的核心要求。合法性要求医学生成式人工智能语料库原始数据获取和训练数据标注均符合法律法规。这里所强调的“法”，不仅涵盖现行法律、行政法规、强制性标准等约束性文件，还包括行业规范、推荐性标准等引导性（指导性）文件。

目的限制与最小必要性原则是在数据获取和数据处理场景下合法性原则的具体延伸，强调对原始数据处理的边界与操作规范。目的限制原则要求数据处理者在启动数据收集与加工之前，应以合理目的为导向，优先界定语料使用的合法场景与目标。

最小必要性原则进一步要求，在满足上述明确目的的前提下，仅收集实现语料库应用场景所必需的最少量信息，避免收集冗余信息。例如，在进行语义识别或术语标准化研究时，应仅保留医学术语上下文，而不将个人信息作为语料库的构成要素。这种“最小化”的处理策略，有助于降低数据泄露与隐私侵害风险。

数据主体权利保障原则是合法性在数据获取场景下的具体延伸，是维护信息提供者和数据加工者合法权益的根本准则。医学生成式人工智能语料库的构建者应采取相关措施进行知识产权保护、个人信息保护等。对于罕见病等特殊数据，应着重防范隐私泄露风险，防止罕见病患者隐私数据泄露，且应进一步关注临床数据采集是否获得患者的知情同意。

数据安全与风险防控原则是合法性在数据存储场景下的具体延伸。《民法典》《个人信息保护法》等法律规范均强调应防范数据泄露、篡改或丢失，在发生数据安全事件时及时报告并补救。《数据安全法》第二十一条要求针对核心数据和敏感信息设定更为严格的保护机制。因此，数据存储者应建立健全全流程数据安全管理制度，并组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，以保障数据安全、保护原始数据和标注结构，从而防止语料库数据被泄露、篡改和滥用。

4.2 隐私泄露风险的合规应对措施

为应对隐私泄露风险，应在使用包含个人信息的语料时，取得对应个人的同意或者符合法律、行政法规规定的其他情形；在使用包含敏感个人信息的语料前，应取得对应个人单独同意或者符合法律、行政法规规定的其他情形。有关告知同意应进一步参考《数据安全技术 敏感个人信息处理安全要求》。例如，在收集敏感个人信息用于语料库建设前，应采用单独弹窗等方式向个人进行告知；应向个人信息主体告知语料信息处理者的基本情况，说明敏感个人信息作为语料的处理目的、处理方式和必要性，明确敏感个人信息的种类、保存期限和对个人权益的影响，以及个人信息主体行使个人信息主体权利的方式和途径；持续收集敏感个人信息的，应提供持续提示或间隔提示机制。在收集敏感个人信息前，应取得个人信息主体的单独同意；在法律法规另有明确规定时还应取得个人信息主体的书面同意；当涉及多项敏感个人信息处理时，应设置单独同意措施；当单项敏感个人信息被用于多种训练时，不应捆绑取得用户同意；个人信息处理者处理已公开的敏感个人信息，经评估对个人权益有重大影响的，还应取得个人的单独同意；基于个人同意处理敏感个人信息的，个人信息处理者应为个人信息主体提供便捷的撤回同意方式，同时向个人信息主体说明撤回同意可能对个人产生的影响。

4.3 训练数据偏见风险的合规应对措施

为应对训练数据偏见风险，根据《生成式人工智能服务安全基本要求》，数据采集者应加强语料来源管理，注重来源语料搭配，确保来源可追溯，并设置信息阻断手段。一是提高语料来源的多样性，对每一种语言的语料，如中文、英文等，以及每一种类型的语料，如文本、图片、音频、视频等，均应有多个语料来源；如使用境外语料，应合理搭配境内外来源语料。二是对采集结果应采用关键词、分类模型、人工抽检等方式，进行违法语料和偏倚内容过滤，开展语料质量预评估、语料采集校验。

数据标注影响训练数据和生成内容的质量。《生成式人工智能服务管理暂行办法》第七条及第八条要求，生成式人工智能服务提供者应采取有效措施提高训练数据质量，增强训练数据的真实性、准确性、客观性、多样性；在生成式人工智能技术研发过程中进行数据标注的，应制定清晰、具体、可操作的标注规则，开展数据标注质量评估，抽样核验标注内容的准确性，对标注人员进行必要培训，提升遵法守法意识，监督指导标注人员规范开展标注工作。因此，数据标注应优先遵循《人工智能面向机器学习的数据标注规程》《网络安全技术 生成式人工智能数据标注安全规范》《人工智能大模型 第 1 部分：通用要求》《网络安全技术 人工智能生成合成内容标识方法》，同时遵循《人工智能面向机器学习的数据标注规程》“前期准备 – 任务

执行－结果输出”的完整框架，通过全周期管理提高训练数据质量。《网络安全技术 生成式人工智能数据标注安全规范》进一步明确了数据标注核验要求，标注数据应具备全面性、代表性，至少覆盖《网络安全技术 生成式人工智能服务安全基本要求》附录 A 中所列主要安全风险场景，每种安全风险的安全性标注数据不宜少于 200 条，以应对数据输出的偏倚风险。由于医学生成式人工智能服务涉及诊疗等医疗信息服务场景，还应对《网络安全技术 生成式人工智能服务安全基本要求》涉及的医学内容不准确（严重不符合医学科学常识或医学领域主流认知）和内容不可靠（虽然不包含严重错误内容，但无法对医学生成式人工智能服务的使用者形成帮助）问题，进行标注结果输出质量检测。

4.4 知识产权风险的合规应对措施

为应对知识产权风险，生成式人工智能服务提供者应在原始数据获取阶段进一步落实数据获取事前、事中与事后三位一体的保护措施。

数据获取的事前阶段，根据语料来源不同进行知识产权相关分析。对于开源语料，收集语料对应的开源许可协议（CC BY 协议）或授权文件，明确数据资源的使用要求。对于网站信息，应根据网站的 robots 协议、服务政策等，排除已明确不可以采集的语料。使用医学生成式人工智能服务使用者输入的信息作为语料时，应取得使用者的授权，并在服务条款中明确使用者输入的信息将会作为语料训练模型。

数据获取的事中阶段，应建立有效采集记录制度。从第三方购买商业语料时，还应保存具备法律效力的交易合同、合作协议等，并对交易方或合作方的数据进行全面审核。如果数据来源、质量、安全方面的证明材料缺失，则不应使用该语料，以防第三方违规引发的知识产权风险。

数据获取的事后阶段，生成式人工智能服务提供者应采取技术和成本上可行的措施，避免再次生成相同的侵权内容。例如，对模型输出结果进行必要的合法性审查，防范直接复制或实质性相似等侵权行为的发生。采用文本、图像相似性比对，以及重点提示词过滤拒答等技术和机制[21]，预防后续可能的知识产权侵权行为。同时，如果生成内容是基于使用者输入的受知识产权保护的信息，服务提供者应在用户协议中明确约定知识产权归属及使用授权范围，避免权属争议。

4.5 数据合规的技术手段

生成式人工智能服务提供者可运用敏感数据识别、多样化训练数据自动化生成、知识产权侵权检测等技术手段，提升医学语料库数据合规风险识别及风险应对效率。例如，采用潜在个人敏感数据识别工具、隐私政策法规与现行业务实践差异分析工具、个人数据流动全生命周期建模工具、个人信息请求追踪工具等，提前发现问题并更好地应对医学语料库隐私泄露风险。采用训练数据自动化生成工具，生成符合人口统计特征的精准数据，从而提升数据集的质量和多样性，应对训练数据偏倚风险。采用文本相似度分析等技术，检测潜在抄袭、版权侵权的情况，以快速发现医学语料库存在的知识产权风险。采用自动识别数据所有者、使用者及数据流向的智能化工具，及时发现数据处理不当行为。

5 结语

当前，数据已经成为社会的关键生产要素之一，在生成式人工智能与临床诊疗、医学研究、医学教育等结合的场景中发挥着至关重要的作用。数据合规是降低法律风险、保障数据安全的重要举措。本研究着眼于医学生成式人工智能的数据安全与隐私泄露风险、训练数据风险和知识产权风险，基于我国制度和标准明确医学生成式人工智能语料库的数据合规义务，以医学生成式人工智能语料库建设场景为例，探究数据合规基本原则和应对措施。未来，语料库管理者及服务提供者仍应紧跟法律法规和标准变化，进一步探索医学生成式人工智能语料库合规建设路径，建立完善、高效的语料库构建指南，研发自动化解决方案，积极应对医学生成式人工智能语料库存在的各类数据风险，以推动语料构建与使用过程的合规可控。

作者贡献：王蕾负责研究设计、论文撰写；刘苗、王茜、赵琬清负责文献调研、论文修订；胡佳慧、方安负责提供指导、论文修订。

利益声明：所有作者均声明不存在利益冲突。

参考文献

1 肖仰华，徐一丹．大规模生成式语言模型在医疗领域的应用：机遇与挑战［J］．医学信息学杂志，2023，44（9）：1－11.

2 谢潇，罗世杰．论生成式人工智能的动态风险及适应性治理［J］．北京工业大学学报（社会科学版），2025，25（1）：112－125.

3 叶元龙，曾维，陈金龙，等．生成式人工智能在口腔医学领域应用价值的比较研究［J］．华西口腔医学杂志，2024，42（6）：810－815.

4 王硕，刘天语，汪琛，等．试论生成式人工智能的医疗应用能力与风险边界［J］．医学与哲学，2024，45（12）：1－5.

5 康砚澜，郭倩宇，张文强，等．基于知识增强的医学语言模型：现状、技术与应用［J］．医学信息学杂志，2023，44（9）：12－22.

6 李启渊，张静，徐权光，等．ChatGPT 在中医医院智慧化建设中的应用、挑战及对策［J］．卫生软科学，2024，38（4）：78－81.

7 潘高涧，叶冠志，方韶韩，等．ChatGPT 在医学临床实践应用与伦理探索［J/OL］．中国胸心血管外科临床杂志，1－6［2025－11－20］．https：//link.cnki.net/urlid/51.1492.R.20240321.1047.022.

8 颜见智，何雨鑫，骆子烨，等．生成式大语言模型在医疗领域的潜在典型应用与面临的挑战［J］．医学信息学杂志，2023，44（9）：23－31.

9 王燕萍，金钢，赵佳，等．我国医疗人工智能的应用现状、风险及对策建议［J］．卫生软科学，2024，38（10）：74－78.

10 刘维，马春晓．ChatGPT 的风险挑战及刑事应对［J］．警学研究，2023（5）：33－45.

11 WANG C，LIU S，YANG H，et al. Ethical considerations of using ChatGPT in health care［J］. Journal of medical internet research，2023，25（8）：e48009.

12 施锦诚，王国豫，王迎春．Esg 视角下人工智能大模型风险识别与治理模型［J］．中国科学院院刊，2024，39（11）：1845－1859.

13 EL EMAM K，JONKER E，ARBUCKLE L，et al. A systematic review of re－identification attacks on health data［J］. Plos one，2011，6（12）：e28071.

14 YEUNG J A，KRALJEVIC Z，LUINTEL A，et al. AI chatbots not yet ready for clinical use［EB/OL］.［2025－11－20］. https：//www.medrxiv.org/content/10.1101/2023.03.02.23286705v2.

15 BOUGUETTAYA A，STUART E M，ABOUJAOUDE E. Racial bias in AI－mediated psychiatric diagnosis and treatment：a qualitative comparison of four large language models［J］. NPJ digital medicine，2025，8（1）：332.

16 顾萍，王成荫，伍波，等．创新与著作权的平衡：Thomson Reuters v. ROSS Intelligence 案对 AI 训练数据的规制［EB/OL］.［2025－11－20］. https：//www.zhonglun.com/research/articles/54361.html?utm_source=chatgpt.com.

17 HOWARD M J，BARGER K. Kadrey v. Meta platforms，Inc.［EB/OL］.［2025－07－19］. https：//www.loeb.com/en/insights/publications/2023/12/richard－kadrey－v－meta－platforms－inc.

18 中国保护知识产权网．多名图书作者向人工智能公司 Anthropic 提起诉讼［EB/OL］.［2025－11－20］. https：//ipr.mofcom.gov.cn/article/gjxw/ajzz/bqajzz/2025057/1992565.html.

19 DIDSURY H，ZHU X A. Transformative training：an analysis of AI training data and fair use in Authors Guild v. OpenAI Inc.［J］. Publishing research，2025，4（9）：e2.

20 徐伟，韦红梅．生成式人工智能训练数据风险治理：欧盟经验及其启示［J］．现代情报，2025，45（5）：89－98.

21 朱开鑫. AIGC 服务提供者版权侵权责任研究［J］．上海师范大学学报（哲学社会科学版），2024，53（6）：39－49.

欢迎订阅 欢迎赐稿