• 专论:智能体及其医学应用 •

编者按: 智能体是一种能够感知环境、自主决策并执行动作以实现特定目标的实体,具有自主性、反应性、主动性等特点。近年来,在人工智能技术,特别是大语言模型的推动下,智能体的发展迈入全新阶段。目前基于大语言模型的智能体逐渐应用于药物研发、临床、医学模拟、医疗辅助等领域,呈现从单点任务自动化向复杂工作流整合、从后台数据分析向一线临床交互、从被动式工具向主动式伙伴演进等发展趋势,在提升医疗服务可及性、优化临床流程和推动精准医疗等方面展现出巨大潜力,能有效弥合医疗资源鸿沟,形成全新的以标准和数据驱动的医疗服务范式。本期专论着眼于智能体及其医学应用,所载论文包括智能体技术进展与医学领域应用、网络健康信息多维评估智能体研究、病历生成智能体研究等,以期为智能体在医学领域的智能化、智慧化应用提供参考。

AI 智能体技术进展与医学领域应用思考

刘湘闽 王 茜 刘 会 周 易 赵琬清 姚宽达 陈凌云 方 安

(中国医学科学院/北京协和医学院医学信息研究所/图书馆 北京 100020)

〔摘要〕 **目的/意义** 探讨人工智能(artificial intelligence, AI)智能体在医学领域的应用现状及挑战,为其智能化、智慧化应用提供参考。**方法/过程** 采用文献调研法,系统分析 AI 智能体的概念起源、核心架构,总结其在医学领域的应用现状及挑战,并提出展望。**结果/结论** AI 智能体在整合医学复杂工作流、提升诊疗效率方面潜力显著,但其在医疗领域中的应用仍处于探索阶段,有待攻克技术难题、完善规范体系。

〔关键词〕 AI 智能体;智能医学应用;大语言模型

〔中图分类号〕 R-058 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2025.11.001

Considerations on the Technological Progress of AI Agent and Its Application in the Medical Field

LIU Xiangmin, WANG Qian, LIU Hui, ZHOU Yi, ZHAO Wanqing, YAO Kuanda, CHEN Lingyun, FANG An

Institute of Medical Information/Medical Library, Chinese Academy of Medical Sciences & Peking Union Medical College, Beijing 100020, China

〔**Abstract**〕 **Purpose/Significance** To investigate the current application and challenges of artificial intelligence (AI) agent in the medical field, and to provide references for their intelligent and smart applications. **Method/Process** By using the literature research method, the conceptual origin and core architecture of AI agent are systematically analyzed. Their current application and challenges in the medical field are summarized, and prospects are proposed. **Result/Conclusion** AI agent demonstrate significant potential in integrating complex medical workflows and enhancing the efficiency of diagnosis and treatment. However, their application in the medical field remains in an exploratory stage, necessitating the resolution of technical challenges and the refinement of regulatory frameworks.

〔**Keywords**〕 artificial intelligence (AI) agent; intelligent medical application; large language model

〔修回日期〕 2025-09-12

〔作者简介〕 刘湘闽,硕士研究生;通信作者:方安,研究馆员,硕士生导师。

〔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(项目编号:2021-I2M-1-056)。

1 引言

人工智能（artificial intelligence，AI）技术正在成为推动医学革新和加速医学研究的重要力量。大语言模型（large language model，LLM，以下简称大模型）具有强大的语言理解与生成能力，其通过海量数据预训练学习领域专业知识，在医学知识问答、知识检索等方面展现出广泛应用价值[1]。然而在面对复杂医学任务时，大模型因缺乏自主决策和执行能力，难以根据环境变化动态调整策略，应用灵活性和效率受限，需要大量提示工程和任务适配，才能实现智能化自主运行[2]。与大模型相比，智能体强调在复杂环境中的自主行动能力，其能够根据实时环境作出合理决策，从而完成系列复杂任务。基于大模型的智能体也称为 AI 智能体（AI agent）。全球知名调研机构 Forrester 在《2025 年十大新兴技术》[3]中指出“AI agent 代表了自动化的下一个前沿，使系统能够独立、有目的地作出决策”。本文回顾智能体概念起源，分析 AI agent 架构与关键技术，探讨其在医学领域的应用进展和潜在挑战，以期为 AI agent 在医学领域的智能化、智慧化应用提供参考。

2 AI agent 概述

2.1 概念起源

智能体概念起源于哲学，本意是对“行动者”（agent）的探讨。马文·明斯基（Marvin Minsky）[4]将其引入人工智能领域，并定义为一种自主运行的计算或认知实体，具备感知环境、推理决策和执行任务的能力。目前学界关于智能体的定义尚未统一。Xi Z 等[5]认为智能体是以大模型为核心的“大脑”，融合感知模块与行动模块，具备自主决策、知识推理、规划学习和社会交互能力的智能系统。Russell S 等[6]认为任何通过传感器感知环境并通过执行器作用于该环境的事物都可以被视为智能体。Wiesinger J 等[7]更强调智能体的自主性与主动性，将其定义为一个应用程序，可通过观察世界并利用可用工具采取行动，以实现特定目标。综上，智能体可以定义为一种能够感知环境、自主决策并执行动作以实现特定目标的实体，具有自主性、反应性、主动性等特点。

伴随人工智能技术的发展，智能体的概念也在不断演进。早期符号主义强调规则和符号，智能体以规则和逻辑为核心，可进行简单决策并具备一定的自主性，如专家系统 MYCIN[8]。行为主义强调智能体在环境中的行为和交互，因此前期诞生的反应式智能体强调快速和实时响应，后期基于强化学习的智能体主要关注复杂不确定性环境下的交互。包容架构[9]、信念－愿望－意图架构[10]等思想的出现，为智能体分解成多个简单、独立的模块行为层提供了可行策略，使其能够面对不同复杂环境进行个性化建模。连接主义借鉴神经元连接方式，奠定了深度学习蓬勃发展的基础。在此基础上，大模型推动智能体发展进入新阶段，即 AI agent 阶段。

2.2 架构与关键技术

2.2.1 基本架构（图 1）

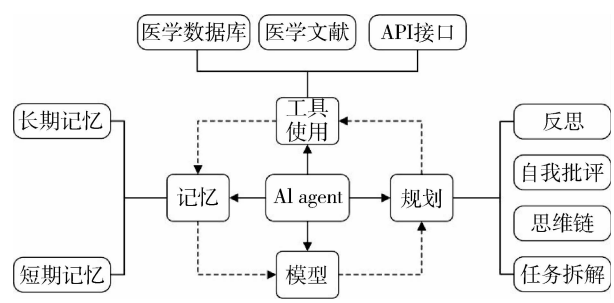

图 1 AI agent 基本架构

Weng L[11]认为 AI agent 的核心组件包含规划、记忆和工具调用。Wiesinger J 等[7]认为其运行组件包括模型、工具和作为工具上层调度模块的编排层。总体而言，AI agent 的基本架构主要包括模型、规划、记忆、工具使用 4 个模块，其中大模型是核心，规划、记忆和工具使用等作为辅助，按照“感知－思考－行动”的循环协同工作[12]。

2.2.2 模型模块 大模型是 AI agent 的核心智能引擎，能将用户的自然语言转换为结构化指令，

还可解析用户意图、理解环境信息、进行常识推理、制定计划、选择工具以及生成最终响应。在具体任务中，模型模块负责统筹和协调，驱动规划、记忆与工具使用等其他模块协同运作。当接收到任务时，模型结合当前环境信息进行自我分析，调用规划模块分解任务，根据需要指挥记忆模块检索历史经验或外部知识，驱动工具使用模块与外部世界交互，执行具体操作。模型掌控动态调度过程，其能力决定 AI agent 的智能程度[5]。

2.2.3 规划模块 规划模块能将复杂任务分解为一系列可管理、可执行的子任务或步骤，用于协助智能体进行逻辑推理、寻求解决问题的可靠方案，根据其反馈机制可分为无反馈规划和反馈规划。（1）无反馈规划。典型技术是思维链，通过引导大模型进行逐步思考，分解复杂问题，能显著提升模型在算术、常识和符号推理任务上的准确性[13]。思维树在思维链基础上，将规划过程从单一的链扩展为多条推理路径，通过回溯或广度/深度优先搜索等策略，选择最优路径，赋予了 AI agent 更强的全局规划和自我纠错能力[14]。（2）反馈规划。对于需要长期规划和适应环境变化的复杂任务，AI agent 常采用反馈规划。反馈规划可根据行动结果和环境观察进行迭代反思和计划修正。ReAct 框架边想边做，执行实时策略，形成“思考－行动－观察”循环。即大模型生成思考，基于该思考选择行动，接收并处理来自该行动的观察，将结果纳入下一次思考的输入，从而形成动态的决策过程[15]。Reflexion 框架采用“事后复盘”的长期学习机制，从已完成的任务中吸取教训，以优化未来的行为。其在 ReAct 的基础上引入更高层次的反思能力，不仅会进行简单的重试，还会对整个行动轨迹进行自我反思，生成关于失败原因的摘要存入记忆，并在未来的规划中避免同样的错误[16]。

2.2.4 记忆模块 记忆模块负责管理历史信息，包括 AI agent 的思考过程、已执行动作、环境观察结果以及用户交互记录[17]。有效的记忆机制对于 AI agent 保持对话连贯性、从经验中学习以及适应新情境至关重要。记忆可分为短期记忆与长期记忆。短期记忆通过上下文窗口实现，所有在当前会话中的交互记录、中间思考过程均被置于上下文中。AI agent 可以利用上下文学习，维持多轮对话的连贯性，但受容量限制，记忆会随会话结束而消失。长期记忆则将检索历史信息编码为自然语言文本、向量嵌入或其他结构化形式，并利用外部存储进行保存，其核心技术是检索增强生成。AI agent 先将查询任务转化为向量，然后在包含历史经验或外部文档的向量数据库中通过计算语义相似度检索出若干相关信息片段；再将其与原始提示结合，一起返回到大模型的上下文窗口中；最后结合包含原始问题、历史经验或外部知识的增强版提示进行综合推理，生成更加精准翔实且有据可依的回答[18]。

2.2.5 工具使用模块 工具使用模块赋予 AI agent 与外部世界交互、获取最新信息、执行特定计算或调用其他应用程序接口（application programming interface，API）的能力[19]。AI agent 主要通过函数调用技术实现工具使用。该技术向模型提供包含每个工具详细描述、功能和参数定义的工具清单，大模型分析用户请求意图并与已注册工具匹配，生成结构化的 JSON 对象，精确描述要调用的函数及其参数。工具使用模块接收并解析大模型生成的指令，调用外部工具[20]，外部 API 或医学数据库执行具体操作并返回数据结果或操作。

3 医学 AI agent 应用现状与趋势

目前医学 AI agent 应用涵盖药物研发、临床、医学模拟、医疗辅助等领域，呈现从单点任务自动化向复杂工作流整合、从后台数据分析向一线临床交互、从被动式工具向主动式伙伴演进等发展趋势。代表性应用案例，见表 1。

表 1 医学领域 AI agent 应用案例

名称	基础模型	应用领域	简要介绍
DrugAgent[21]	GPT－4o	药物研发	用于药物重定位决策
OpenBioMed[22]	BioMedGPT、BioMedGPT－R1	药物研发	用于生命科学与药物研发的智能体开发平台
MALADE[23]	GPT－4	临床	用于药物警戒
MMedAgent[24]	LLaVA－Med	临床	可调用工具实现多模态任务，包括图像分类、定位分割、医学报告生成等
TxAgent[25]	TxAgent－T1－Llama－3.1－8B	临床	整合 211 种工具，用于分析药物相互作用，生成治疗方案
睿兵 Agent[26]	“华西黉医”医学大模型、DeepSeek	临床	聚焦消化领域，可实现健康知识普及、疾病全程管理等功能
KG4Diagnosis[27]	—	临床	可诊断 362 种常见疾病
AgentClinic[28]	GPT－4、Llama、Mixtral－8x7B	医学模拟	能够实现 4 种不同医疗角色模拟
AIPatient[29]	GPT－4－turbo	医学模拟	能够实现患者－医生互动模拟
Agent Hospital[30]	GPT－4	医学模拟	构建虚拟医院，其中所有角色均由 AI agent 模拟
MRAgent[31]	GPT－4	医疗辅助	能够实现文献挖掘－因果推断－结果解读
Aireview Agent[32]	Qwen、DeepSeek	医疗辅助	能实现证据检索、提取、评价等全流程智能化，为中医药研究提供证据支持
KGARevion[33]	—	医疗辅助	整合大模型结构化知识，提升医疗问答准确性

3.1 药物研发

AI agent 早期应用聚焦特定任务自动化，如利用数据挖掘分析海量药物文献和实验数据，发现未知药效机制，或者对化合物进行高效筛选[34]。近年来多智能体协同打通研发全链条的新范式逐渐成为主流趋势，可系统性优化整个研发周期的各个环节。PharmAID[35]能够协同处理前期分子结合点位预测、后期毒理优化以及医学写作等复杂任务，显著缩短研发周期。OpenBioMed 平台[22]通过低代码、拖拽式的工作流搭建，极大地降低了技术门槛。Inoue Y 等[21]构建药物靶标关联预测多智能体系统，在激酶－化合物基准测试中，有效降低药物发现假阳性率，提升了研发成功率。

3.2 临床

在临床领域，AI agent 正在从处理后台历史数据的分析工具，逐步成为能够辅助医生决策并与医患直接交互的“数字伙伴”。前者如 MALADE[23]，利用检索增强生成技术分析电子病历等数据，识别潜在的药物不良事件。后者如 MMedAgent[24]，利用多种工具处理医疗报告和影像，辅助生成报告和图像分割。KG4Diagnosis[27]分层多智能体通过构建和利用知识图谱进行推理，模拟多医生会诊，显著提升诊断准确性。

3.3 医学模拟

在医学模拟领域，AI agent 正从模拟孤立静态的医疗参与者转变为仿真多元联动的复杂医疗生态系统。前者如 AgentClinic[28] 和 AIPatient[29] 等，能模拟患者与医生对话，独立收集病情信息，执行体温、血压、心电图等基础医疗检查。后者如 agent Hospital[30]虚拟医院，医生、患者、护士均由 AI agent 构成，医生智能体互相联动，通过治疗海量患者积累经验，借助群体智能实现医术的自我学习与进化。AI agent 模拟在公共卫生领域也展现出广阔的应用前景，可用于推演公共卫生策略并优化医院管理流程。

3.4 医疗辅助

在慢性病管理、健康科普等医疗辅助领域，AI agent 正从被动响应用户查询的知识库，逐渐转变为能主动干预、持续追踪的健康管家。AI agent 通过扩展连接可穿戴设备等外部工具，实时监控血糖、血压等，并主动预警[36]。结合知识图谱增强技术，AI agent 能够整合大模型的非编码知识以及知识图

谱的结构化知识，显著提高医疗信息检索的准确性和可靠性，帮助公众更轻松地获取可靠、专业的医疗知识[37]。

4 AI agent 应用于医疗领域的挑战

4.1 医学可信困境

AI agent 固有的“黑箱”特性和“幻觉”问题，以及医学语料实体中存在的长距离依赖与细粒度依存关系[38]，导致 AI agent 会输出缺乏医学证据支持的结果。提升决策执行的可信度已成为行业共识，医疗领域人工智能国际共识指南 Future – AI[39]指出未来 AI agent 必须向可信 AI 方向深入探索，构建强解释性 AI 是赢得临床信任、保障患者安全的关键。可综合利用检索增强生成、权威医学知识库进行事实校准，同时运用知识图谱对 AI agent 的推理过程加以逻辑约束，并开发置信度评估机制，以筛选和标记不确定性高的答案[40]。

4.2 医学标准生态困境

医疗 AI agent 产业进程面临技术孤岛问题，难以与医院信息系统实现数据协同与互操作。AI agent 深化应用需要完善的技术生态和开放兼容的生态接口。以函数调用规范为代表的统一技术标准是 AI agent 从孤立功能个体走向互联互通产业生态的基石。例如，针对剂量计算等核心医疗任务，应达成统一共识，确保不同 AI agent 在执行同一关键任务时，采用经验证的统一逻辑，输出稳定一致且可靠的结果。生态接口方面，应定义清晰的 API 与数据交换格式，向上兼容各类医院信息系统，向下为算法开发者提供便捷的接入框架，吸引更多参与者共建医疗 AI agent 生态。

4.3 医学伦理约束

现阶段 AI agent 缺乏共情能力与医学道德，不具备在复杂伦理情境下进行决策的能力。医疗服务始终应以患者为中心，医疗的人性化本质不在于是否使用某种技术，而在于技术应用中是否始终体现对人的尊重与关怀。因此应建立 AI agent “医疗伦理规则引擎”，将《希波克拉底誓言》核心条款转化为可计算的伦理约束条件，确保算法决策符合有利原则、不伤害原则等传统道德规范。

4.4 医学隐私泄漏

医疗数据包含基因信息、病史、生物特征等个人敏感信息，具有强隐私属性，泄漏后果严重，监管要求严苛。美国《健康保险流通与责任法案》[41]要求医疗数据中必须删除姓名、地址、医疗记录编号等 18 类直接标识符，并确保剩余数据无法通过间接标识组合识别个体。欧盟《人工智能法案》[42]将医疗 AI 列为高风险类别，要求数据全链路可控可追溯。技术方面尽管联邦学习等技术在跨机构数据协作方面被寄予厚望，但其“本地训练 – 参数聚合”模式仍存在信息泄漏风险。实验[43]表明通过对抗性攻击可从联邦学习的模型参数中还原部分患者的血糖波动曲线，足以推断患者的用药习惯与生活方式。因此 AI agent 相关隐私保护技术仍有待不断完善。

5 AI agent 在生物医学领域的应用前景展望

研究[44]认为通用人工智能按照能力由弱到强可分为无 AI、新兴、胜任、专家、大师、超人 6 个层次。作为类比，当前 AI agent 在医疗领域的应用仍处于新兴阶段，距离胜任乃至更高层次尚有差距。未来 AI agent 将围绕多模态融合与具身智能加速突破。

目前 AI agent 大多是单模态输入，存在认知局限。突破认知局限的关键在于深度融合多源异构医学数据，实现全域数据表征能力进化。一方面可以通过整合电子病历、病理影像、基因测序乃至语音信息，构建统一数据空间，进而为患者构建精准的个体“数字孪生”模型，真正实现个性化医疗。另一方面要推动虚拟医院与实体医院协作循环：实体医院为 AI agent 提供海量、无偏的真实世界数据；以 AI agent 为核心的虚拟医院则通过群体智能持续进化，输出高质量诊疗方案，赋能实体医疗。

具身智能（机器人）能够通过实体对物理世界进行感知，并与之实时交互。与具身智能技术的融

合将拓展 AI agent 与物理世界的交互能力。例如，为手术机器人配备 AI agent，可提前规划手术路径，根据实时传感压力及患者实时生理体征实现手术自动化。综上，将 AI agent 的强大能力延伸到现实世界，能有效弥合医疗资源鸿沟，形成一种全新的、以标准和数据驱动的医疗服务范式。

6 结语

本文系统阐述了 AI agent 的核心概念与关键架构，总结其在药物研发、临床辅助、医学模拟及医疗辅助等领域的应用现状。AI agent 凭借其强大的自主规划与工具调用能力，在整合复杂工作流、提升诊疗效率方面展现出巨大的应用潜力。但是，仍须正视并克服 AI agent 固有的技术局限与多重应用挑战。在技术层面，须建立更为严格的统一技术标准，以解决原生模型“幻觉”问题，深化临床应用的同时确保决策可信。在应用层面，医学伦理与隐私保护是其落地应用的前提和不可逾越的红线，亟待构建完善的隐私规范与伦理监管框架。未来 AI agent 将通过融合海量生物医学数据构建个体健康模型，实现模型端从多模态数据到全息数字生命的跨越，也可以赋能具身智能实现自动化诊疗与手术，实现应用端从数字世界到物理世界的跨越。

作者贡献：刘湘闽负责文献调研、论文撰写；王茜、刘会负责论文修订；周易、赵琬清、姚宽达、陈凌云负责资料收集；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 ZHAO W X, ZHOU K, LI J, et al. A survey of large language models [EB/OL]. [2025-05-09]. http://arxiv.org/abs/2303.18223.
2 BURTSEV M, JOB A. The working limitations of large language models [J]. MIT sloan management review, 2023, 65 (1): 1-5.
3 Forrester. Forrester unveils top 10 emerging technologies for 2025 [EB/OL]. [2025-05-09]. https://www.forrester.com/press-newsroom/forrester-top-10-emerging-technologies-2025/.
4 马文·明斯基. 心智社会 [M]. 任楠, 译. 北京: 机械工业出版社, 2016.
5 XI Z, CHEN W, GUO X, et al. The rise and potential of large language model based agents: a survey [J]. Science China information sciences, 2025, 68 (2): 121101.
6 RUSSELL S, NORVIG P. 人工智能现代方法（第 4 版）[M]. 张博雅, 陈坤, 田超, 等, 译. 北京: 人民邮电出版社, 2022.
7 WIESINGER J, MARLOW P, VUSKOVIC V. Agents [EB/OL]. [2025-05-03]. https://www.kaggle.com/whitepaper-agents.
8 SHORTLIFFE E H, DAVIS R, AXLINE S G, et al. Computer-based consultations in clinical therapeutics: explanation and rule acquisition capabilities of the MYCIN system [J]. Computers and biomedical research, 1975, 8 (4): 303-320.
9 BROOKS R. A robust layered control system for a mobile robot [J]. IEEE journal on robotics and automation, 2003, 2 (1): 14-23.
10 RAO A S, GEORGEFF M P. BDI agents: from theory to practice [C]. San Francisco: The First International Conference on Multi-Agent Systems, 1995.
11 WENG L. LLM powered autonomous agents [EB/OL]. [2025-05-02]. https://lilianweng.github.io/posts/2023-06-23-agent/.
12 凌峰. AI agent 开发与应用：基于大模型的智能体构建 [M]. 北京: 清华大学出版社, 2025.
13 WEI J, WANG X, SCHUURMANS D, et al. Chain-of-thought prompting elicits reasoning in large language models [EB/OL]. [2025-05-02]. https://arxiv.org/abs/2201.11903.
14 YAO S, YU D, ZHAO J, et al. Tree of thoughts: deliberate problem solving with large language models [EB/OL]. [2025-05-02]. https://arxiv.org/abs/2305.10601.
15 YAO S, ZHAO J. ReAct: synergizing reasoning and acting in language models [EB/OL]. [2025-05-02]. https://arxiv.org/abs/2210.03629.
16 SHINN N, CASSANO F, GOPINATH A, et al. Reflexion: language agents with verbal reinforcement learning [EB/OL]. [2025-05-02]. https://arxiv.org/abs/2303.11366.
17 WANG L, MA C, FENG X, et al. A survey on large language model based autonomous agents [J]. Frontiers of computer science, 2024, 18 (6): 186345.
18 LEWIS P, PEREZ E, PIKTUS A, et al. Retrieval-augmented generation for knowledge-intensive NLP tasks [EB/OL]. [2025-05-02]. https://arxiv.org/abs/2005.11401.
19 SCHICK T, DWIVEDI-YU J, DESSI R, et al. Toolformer:

language models can teach themselves to use tools [EB/OL]. [2025-05-02]. https://arxiv.org/abs/2302.04761.

20 LIU W, HUANG X, ZENG X, et al. ToolACE: winning the points of LLM function calling [EB/OL]. [2025-05-30]. http://arxiv.org/abs/2409.00920.

21 INOUE Y, SONG T, WANG X, et al. DrugAgent: multi-agent large language model-based reasoning for drug-target interaction prediction [EB/OL]. [2025-04-23]. http://arxiv.org/abs/2408.13378.

22 OPENBIOMED. OpenBioMed [EB/OL]. [2025-05-10]. https://openbiomed.pharmolix.com/login?utm_source=ai-bot.cn.

23 CHOI J, PALUMBO N, CHALASANI P, et al. MALADE: orchestration of LLM-powered agents with retrieval augmented generation for pharmacovigilance [EB/OL]. [2025-05-30]. http://arxiv.org/abs/2408.01869.

24 LI B, YAN T, PAN Y, et al. MMedAgent: learning to use medical tools with multi-modal agent [EB/OL]. [2025-04-23]. http://arxiv.org/abs/2407.02483.

25 GAO S, ZHU R, KONG Z, et al. TxAgent: an AI agent for therapeutic reasoning across a universe of tools [EB/OL]. [2025-05-30]. https://arxiv.org/abs/2503.10970.

26 冯若冰. “睿兵 Agent”来了 [N]. 大众健康报, 2025-03-04 (3).

27 ZUO K, JIANG Y, MO F, et al. KG4Diagnosis: a hierarchical multi-agent LLM framework with knowledge graph enhancement for medical diagnosis [EB/OL]. [2025-05-30]. http://arxiv.org/abs/2412.16833.

28 SCHMIDGALL S, ZIAEI R, HARRIS C, et al. AgentClinic: a multimodal agent benchmark to evaluate AI in simulated clinical environments [EB/OL]. [2025-05-30]. http://arxiv.org/abs/2405.07960.

29 YU H, ZHOU J, LI L, et al. Simulated patient systems are intelligent when powered by large language model-based AI agents [EB/OL]. [2025-05-30]. http://arxiv.org/abs/2409.18924.

30 LI J, LAI Y, REN J, et al. Agent hospital: a simulacrum of hospital with evolvable medical agents [EB/OL]. [2025-04-23]. http://arxiv.org/abs/2405.02957.

31 XU W, LUO G, MENG W, et al. MRAgent: an LLM-based automated agent for causal knowledge discovery in disease via mendelian randomization [EB/OL]. [2025-05-30]. https://pubmed.ncbi.nlm.nih.gov/40194554/.

32 全球首个“中医药循证评价智能体 (Aireview Agent)”发布 [J]. 天津中医药大学学报, 2025, 44 (4): 298.

33 SU X, WANG Y, GAO S, et al. KGARevion: an AI agent for knowledge-intensive biomedical QA [EB/OL]. [2025-05-30]. http://arxiv.org/abs/2410.04660.

34 GALKIN F, REN F, ZHAVORONKOV A. LLMs and AI life models for traditional Chinese medicine-derived geroprotector formulation [EB/OL]. [2025-05-30]. https://www.aginganddisease.org/EN/10.14336/AD.2024.1697.

35 复星医药. 复星医药深度拥抱 AI, 自研 PharmAID 决策智能体平台助力高效创新 [EB/OL]. [2025-06-05]. https://www.fosunpharma.com/content/details37_13643.html.

36 DE LAURETIS L, PERSIA F, COSTANTINI S, et al. How to leverage intelligent agents and complex event processing to improve patient monitoring [J]. Journal of logic and computation, 2023, 33 (4): 900-935.

37 LECU A, GROZA A, HAWIZY L. Knowledge graph-driven retrieval-augmented generation: integrating deepseek-R1 with weaviate for advanced chatbot applications [EB/OL]. [2025-05-30]. https://arxiv.org/abs/2502.11108.

38 李建清, 刘雷. 医学大数据与人工智能 [M]. 北京: 人民卫生出版社, 2023.

39 LEKADIR K, FRANGI A F, PORRAS A R, et al. FUTURE-AI: international consensus guideline for trustworthy and deployable artificial intelligence in healthcare [EB/OL]. [2025-05-30]. https://doi.org/10.1136/bmj-2024-081554.

40 WU J, ZHU J, QI Y, et al. Medical graph RAG: towards safe medical large language model via graph retrieval-augmented generation [EB/OL]. [2025-05-30]. http://arxiv.org/abs/2408.04187.

41 U.S. Department of Health and Human Services. Health insurance portability and accountability act of 1996 (HIPAA) [EB/OL]. [2025-05-30]. https://www.hhs.gov/hipaa/index.html.

42 European Parliament, Council of the European Union. Regulation (EU) 2024/1689 of the European parliament and of the council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act) [EB/OL]. [2025-05-30]. https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

43 DU J, HU J, WANG Z, et al. SoK: on gradient leakage in federated learning [EB/OL]. [2025-05-30]. http://arxiv.org/abs/2404.05403.

44 MORRIS M R, SOHL-DICKSTEIN J, FIEDEL N, et al. Levels of AGI for operationalizing progress on the path to AGI [EB/OL]. [2025-05-30]. http://arxiv.org/abs/2311.02462.