

医疗场景中生成式人工智能的法律规制研究

徐钟翔 罗艺雅

西南医科大学 法律硕士，四川泸州，646699；

摘要：大数据时代，人工智能的应用范围越来越广泛。人工智能深入医疗领域已经是必然的趋势，但是对于人工智能领域的法律则需要进一步完善。本文从行政许可的角度限制生成式人工智能在医疗场景中的准入机制，严格把控人工智能应用于医疗领域的合理性以及科学性。

关键词：生成式人工智能；行政许可；医疗领域

DOI: 10. 69979/3029-2808. 25. 07. 026

1 问题的缘起

进入大数据时代，随着人工智能的快速发展其应用范围越来越广泛，尤其是生成式人工智能基于各种病历库的学习能力对于医疗领域的发展，推动中国人民的健康水平持续提升有着重要作用。人工智能技术辅助医疗将会降低医院医生资源短缺不足，患者于医疗资源严重失衡的问题。3月29日至31日在重庆召开的2024中国医学装备大会展览现场出现“AI医生”进行问诊分诊，医学影像设备智能出具检查报告，医生操作手术机器人进行微创手术等，人工智能进入医疗领域已经是不可逆的趋势，“当前，我们正处于科技大爆炸的全新时代，AI大模型、元宇宙、‘数智’医疗等技术日趋成熟。”中国医学装备协会第六届理事会理事长赵自林说，新技术和高端医疗装备融合交叉，将在医疗健康领域催生出一系列颠覆性新产品、新模式、新动能。《“十四五”医疗装备产业发展规划》特别提出加快智能医疗装备发展，《关于进一步完善医疗卫生服务体系的意见》明确加快推进互联网、人工智能等在医疗卫生领域中的应用占比将会更大，我国也不断加强顶层设计，推进“人工智能+医疗”的发展。

在医疗领域已经开始使用生成式人工智能技术，辅助医院医生在医疗诊断的同时也带来的相应的法律风险挑战。2024年1月，美年健康与华为云、润达医疗达成战略合作，三方宣布共同打造国内首款健康管理AI机器人——“健康小美”数智健管师，利用先进的生成式AI技术和精准的数据驱动服务，“健康小美”能够为用户提供个性化的健康管理建议、计划及服务，并结合最新的医疗研究成果，为用户量身定制健康管理计划，及时调整和优化建议，以适应用户健康状态的变化。人工智能在医疗领域的面向医务人员群体，医疗人工智能发挥着辅助疾病诊疗、提供治疗方案并预测病情发展等作用，常以“最高效率提炼最权威依据后作出最优解”的机器运行程式，把控基本医疗经验的内在规律。但是

如何解决人工智能存在的训练数据偏见，数据标注偏见，开发者偏见以及数据的透明度等却是人工智能研究的短板。生成式人工智能技术可以运用大数据对已有的患者的疾病病历进行量化分析，建立病历与病历之间相似性，实现相似病症配对与推送。但是由于患者自身体质存在的个体差异通过类比推送就缺乏医生在针对个体差异所进行的差别对待。这就会导致药不对症等医疗损害的发生。

基于此，如何更好地利用人工智能技术实现同类病症精准治疗降低医疗损害，实现医学发展规律同人工智能技术的结合。本文坚持从行政许可角度使人工智能在医疗领域中的使用更有针对性，目的性，对人工智能技术进行科室区分，缩小工作范围，加强专业深度。

2 人工智能所引发的问题

2.1 人工智能医疗纠纷的法律使用问题

生成式人工智能在医疗领域造成患者损害后，责任的承担目前法律适用存在不明的问题。在美国，也有学者进一步将人工智能（AI）技术作出的决策类比于代理人决策，并据此认为人工智能决策产生的责任类似于雇主责任（respondeat superior）。这类说法将人工智能比作雇佣工人在医疗领域人工智能造成患者损害由医院承担侵权责任。那么对于人工智能提供者对于侵权损害承担何种责任。法律层面上，现今通说认为人工智能并不属于自然人不具备承担法律责任的能力，即不属于承担责任的主体。但是现阶段人工智能已经越来越多地具备自然人的某些特征，同时又具有“物”的属性，未来将会给界定医疗损害责任主体带来挑战。例如 gap t4 等人工智能，通过自然语言处理、生成对抗网络等技术发展已具有高仿真、拟人化的特征，能够模拟甚至复制人类的思考方式、创作过程和表达逻辑已经具备一定的类人性。

医疗过程中人工智能单独或者与医生联合进行医疗活动时造成损害，这时就会涉及多方疑是责任主体即

医疗机构、医生、人工智能的开发者、销售者。在此很难确定由谁承担责任以及如何确定分配比例。英国在2015年2月进行该国首例机器人心脏瓣修复手术，机器人在操作过程中把病人的心脏“放错位置”，还戳穿大动脉；机器臂“乱动”打到医生的手，机器人在运行过程产生的嘈杂声使得医生之间的交流也很滞后，最终导致损害结果的发生。该事故的造成有医生对机器人的操作不熟练，医疗机构也没有事先经过周密的演练排除可预见的风险，同时机器人本身算法也存在瑕疵等多方原因。根据我国《民法典》现行规定医疗行为致人损害归责原则是过错，责任主体是医疗机构。医疗产品致人损害则适用的是无过错责任，责任主体是销售者和生产者。在人工智能缺乏明确定义下，适用法律也仍然比较模糊，所以归咎责任时在缺乏法律的明确规定的情况下导致患者很难得到快速有效合理的救济。

如前所述，医疗行为与人工智能的联合已是必然发展方向，未来由此产生医疗损害将会越来越多，如果无法解决人工智能的主体问题，确定人工智能的开发者、销售者，医疗机构、医生之间的责任划分以及医疗损害的构成要件一系列法律问题那么对于受害者的损害救济将会成为立法、司法的新挑战、新威胁、患者对人工智能也会产生信任危机。

2.2 人工智能的技术问题

在“强人工智能”技术迭代加速的背景下，生成式人工智能在医疗领域的应用场景不断拓展，其基于深度学习的算法模型已能辅助完成疾病诊断、治疗方案生成等复杂任务。然而，技术落地过程中仍面临显著的通用性与个性化矛盾，集中表现为算法逻辑与医学实践特性的深层冲突。

当前医疗AI的算法设计普遍依赖标准化数据训练，其决策模型基于群体病历的统计规律构建，本质上遵循“共性优先”的技术逻辑。这种模式在处理常规病症时具备高效性，但面对罕见病、疑难杂症或患者个体差异显著的病例时，算法的局限性便会凸显。

2.3 人工智能的伦理问题

随着人工智能的不断发展其涉及的伦理问题也越发尖锐，在2021年联合国教科文组织通过的《人工智能伦理问题建议书》中提到现今人工智能系统引发了许多新型伦理问题，包括但不限于其对决策、就业和劳动、社交、卫生健康、教育、媒体、信息获取、数字鸿沟、个人数据和消费者保护、环境、民主、法治、安全和治安、双重用途、人权和基本自由（包括表达自由、隐私和非歧视）的影响。尤其是在医疗领域中人工智能信息获取来源，对患者隐私保护，开发者所收集数据的歧视性，男女性别差异等因素现阶段都是无法得到有效解决。

2.3.1 患者个人隐私的保护

生成式人工智能的应用是以已有的数据为算法基础因此所需大量的有关健康医疗领域的大数据。然而健康医疗领域的大数据不仅包括结构化数据，如患者病历、检查结果等，还包括非结构化数据，如医学影像、患者反馈等。这些数据为医疗科研提供了丰富的素材，有助于推动医疗技术的进步。《个人信息保护法》规定将敏感个人信息定义为一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，同时列举了敏感个人信息的种类，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。由此可见前述所说患者病历、检查结果等就属于敏感个人信息。这就导致医疗人工智能在收集数据时会涉及到大量敏感信息。因此医疗人工智能所处理信息的敏感性以及各国争相开展的医疗信息共享项目与精准医疗计划，目的限制与告知同意等传统数据保护原则在医疗人工智能领域的适用困难重重，个人健康数据保护问题在医疗人工智能领域面临着更加复杂的局面。

2.3.2 医疗领域中人工智能信息获取来源

人工智能开发者的偏好直接决定人工智能数据的获取的倾向，在这过程中就可能产生性别歧视、种族歧视等伦理问题。如不同种族群体的弗明汉卒中量表与发生心脑血管疾病之间的联系明显不同，测量自发眨眼率的分析算法在亚裔群体内准确率不高，甚至在某些存在着宗教信仰、尖锐的种族歧视、性别歧视的国家的开发者在对人工智能的数据获取来源本身就存在歧视只片面的选择自己信仰的宗教群体的数据或者摒弃歧视的种族数据导致其所制造出来的人工智能本身存在偏见最终在不断的迭代发展过程中形成不可填补的巨大鸿沟。

人工智能训练数据信息的获取直接决定着人工智能的可靠性，在医疗领域中的一系列个人数据，医院数据，群体资料等都需要相应授权的，那么数据来源的监管力度必然与获取数据数量产生矛盾冲突。人工智能要想获取足够的大量高质量的训练数据就应当取得更多的当事人、医院、行政机关的授权，但是开发者不乏存在利用网络漏洞避开合法授权直接获取所需数据，导致数据来源不正当其所开发出的人工智能也将对信息所有者、储存者权益造成损害，存在着数据输入不合规的风险。

3 人工智能的法律规制的完善

目前解决人工智能所面临的问题所能依据得法律较少，目前，人工智能治理手段主要集中在制定伦理准则和技术标准等方面，在全球层面尚无一部成文法律，

主要国家和地区 也尚未制定专门的人工智能法律法规,或者现有法律法规对于人工智能的科技与新疆域监管还不够完善,导致人工智能的发展和应⽤缺乏法律依据,这也增加了人工智能治理的难度。中国现行法律中有关人工智能管理方面的实施有效的法律规范是 2023 年 7 月由国家互联网信息办公室所发布的《生成式人工智能服务管理暂行办法》,其中虽然明确了人工智能的使用部分法律问题、伦理问题,更多却是有关人工智能在使用过程的原则性、倡导性规定。对于人工智能在医疗领域产生的具体纠纷、显而易见的问题的解决办法,以及如何规制人工智能在医疗领域的野蛮⽣长仍存在较为模糊的状态缺乏实施细则,例如人工智能是否能成为责任主体享有法律上的部分权利或者义务等急需解决的法律问题并未在《生成式人工智能服务管理暂行办法》进行准确说明,因此现有的法律制度并不能为人工智能在医疗领域的蓬勃发展保驾护航。随着生成式人工智能的快速发展进一步完善该领域的法律对于医院如何使用人工智能促进医疗事业的发展,保障患者的健康有着不可避免的作用。许多专家学者也对人工智能的立法进行大量研究,

对于人工智能在医疗领域的应⽤管理是分阶段性的,不同的阶段所采取的治理手段也是有所区别所涉及的主体也不尽相同,笔者认为未来存在的医疗人工智能从开发到使用可以划分为开发阶段、临床试验阶段、和投入使用阶段四个发展过程阶段,不同的阶段进程需要的治理机制体制,也是不尽相同的,所涉及的治理对象也是有所区别例如开发阶段主要治理重点更多是涉及开发者或者开发公司责任倾向也应当更多向其倾斜,临床实验阶段更多是检验公司责任,使用阶段更多是使用者即院方承担更多的责任,可以通过制定不同的行政许可机制进行相应的治理,相应的责任匹配。

严格限制人工智能多科室服务,通过行政许可限制人工智能服务科室,通过这种方式可以降低人工智能监管难度,责任鉴定。增加人工智能的可操作性使得开发者在研发过程中的重心更加明显,对于人工智能在医疗行业的发展也通过这种方式进行区分。

人工智能由于其以大量数据为算法基础构建出的,所以意味着它有能力涉及的许多不同的医疗区域而相比于医生群体他们更加全面,它可以参与诊疗也可以参与手术无论难度高低都可以。但是这对于我们进行管理也就存在困难,通过行政许可的方式进一步限制人工智能的用途,仅限于某一个区域例如手术。那么该人工智能只能获取到有关手术方面的数据、算法也仅围绕其其尽⼤限度发挥作用,这既加强人工智能本身的实用性也

可以通过大量实践及时发现人工智能本身存在的不足甚至缺陷,同时一旦出现医疗纠纷这样在归责过程中对于开发者的责任的鉴定难度就会降低。确定人工智能考核期限,严格测试收集人工智能工作数据以达到高准确率低事故率设立考核标准,是人工智能进入长期服务的考核标准。

4 结语

生成式人工智能与医疗领域的深度融合,既是科技革命赋予医疗行业的“新基建”,也是对法律治理能力的“大考”。当前,技术的飞速迭代与制度的相对滞后形成鲜明对比,医疗 AI 在提升诊疗效率的同时,已暴露出责任认定模糊、数据隐私泄露、算法伦理失范等深层矛盾。这些问题不仅关乎个案中患者的损害救济,更涉及医疗公平性、技术可控性乃至公众对医疗科技的信任根基。

从长远看,破解困局需跳出“头痛医头”的碎片化治理思维,在立法层面确立“分类分级、全周期管控”的原则:对开发阶段严格数据合规与算法审查,对临床应用阶段明确“人机协同”的权责边界,对风险场景设置强制性伦理评估。同时,需建立跨学科的治理联盟,推动法学、医学、计算机科学的深度对话,避免法律规制陷入“技术黑箱”的认知盲区。

值得关注的是,医疗 AI 的终极价值并非替代医生,而是通过技术赋能让医疗决策更具温度——这要求法律规制在防范风险的同时,为“以患者为中心”的创新保留空间。唯有在安全与发展之间找到动态平衡点,才能让人工智能真正成为守护人类健康的“智慧伙伴”,而非游离于法律之外的“风险黑箱”。未来的医疗法治实践,应当在技术理性与人文关怀的交织中,勾勒出更具包容性的治理图景。

参考文献

- [1] 参见仝媛媛,郑婉婷:《健康公平:医疗人工智能中的偏见与治理》,《医学与哲学》,2024 年 4 月,第 45 卷第 7 期,第 36 页到 39 页。
- [2] 参见王素芳,孙爱青:《人工智能在临床应用中的侵权责任探析*》,《现代医学与法律》,2021 年第 13 卷第 5 期,第 70 页。
- [3] 参见韩成芳:《医疗人工智能领域个人健康数据保护的困境及其破解》,《科技与法律(中英文)》,2024 年第 1 期,第 54 页。
- [4] 参见赵申洪:《全球人工智能治理的困境与出路》,《现代国际关系》,2024 年第 4 期,第 118 页。