与运维成本。这种协同架构已成为物联网在煤矿安全监测领域的重要技术方向。

5 煤矿安全监测系统的优化策略

5.1 实时监测与动态预警模型的构建

煤矿作业环境复杂多变，安全风险往往表现为突发性和不可预见性，这要求监测系统具备高效的实时性和动态化响应能力。通过在井下关键区域布设高精度传感器，能够对瓦斯浓度、温湿度、风速、气压以及设备运行状态进行多维度同步采集，从而实现对环境参数和设备工况的全面感知。在此基础上，动态预警模型的引入显得尤为重要。该模型结合数据挖掘与模式识别技术，能够对历史数据进行分析，识别出潜在的危险趋势，并根据实时数据变化情况进行动态修正。通过设定多级阈值和概率判别标准，预警模型不仅可以提前发现风险隐患，还能自动调整预警等级，实现分级响应。预警信息在井下端和调度端同时发布，为操作人员和管理层提供及时的参考依据。该模式还可结合应急预案联动机制，在风险达到临界状态时快速启动处置流程，缩短应对时间。实时监测与动态预警的结合，不仅提升了风险发现的灵敏度和可靠性，也为实现煤矿安全生产的本质保障提供了坚实支撑。

5.2 数据融合与智能化风险识别方法

煤矿监测过程中采集的数据来源广泛，包含气体浓度、通风参数、设备运行信息以及人员定位等多维度数据。若仅依赖单一数据指标进行判断，往往会出现误报或漏报现象，难以形成科学的风险评估。因此，数据融合成为优化系统性能的重要手段。通过多源数据的交叉验证，可以有效消除噪声和冗余，提高整体信息的准确度。采用机器学习与模式识别方法，对大量监测数据进行特征提取与分类建模，能够识别出与事故相关的隐含规律，实现对复杂风险的智能化判定。例如，通过对瓦斯浓度波动与通风系统运行状态的联合分析，可以更加精准地判断瓦斯积聚的危险程度。数据融合不仅提升了系统对异常情况的识别能力，还能实现趋势预测，对潜在风险进行提前预警。智能化方法还可根据事故发生概率自动分配资源，实现风险管理的精细化和动态化。将数据融合与智能识别相结合，能够推动监测系统由传统的被动监控转变为主动预防与预测，为煤矿安全管理注入新的技术动力[4]。

5.3 系统冗余设计与可靠性提升路径

煤矿监测系统在运行过程中，可靠性是保障其有效性的核心指标。井下环境中湿度高、粉尘浓度大、电磁干扰强，极易导致设备故障或信号传输中断，因此必须建立完善的冗余设计机制。通过在关键节点部署备用传感器和多通道通信线路，可以有效避免因单点失效造成的监测盲区。冗余设计不仅体现在硬件层面，还包括软件层面的容错与恢复机制。当数据传输发生中断时，系统应能够自动切换至备用通道，并在信号恢复后进行数据补偿与修正，以确保监测信息的完整性和连续性。在系统可靠性提升方面，还需注重设备选型与结构防护的优化，采用防爆、防水、防尘等级更高的传感器与通信模块，提升设备在恶劣环境下的稳定运行能力。同时，建立周期性维护与健康诊断机制，实时监控设备状态，预测可能出现的故障并进行预防性检修。通过硬件冗余、软件容错与维护管理的多重保障，可以大幅度提升煤矿监测系统的整体可靠性与抗风险能力，为矿井安全运行提供坚固的技术屏障。

6 结语

基于物联网的煤矿安全监测系统优化设计，不仅是对传统监测模式的改进，更是实现矿井本质安全的重要路径。通过多参数传感器的合理配置、无线传输协议的优化选择以及边缘计算与云端协同机制的应用，系统在实时性、可靠性和智能化方面得到了全面提升。动态预警模型与数据融合方法的引入，使风险识别更为精准，冗余设计与容错机制的加强，则为系统的长期稳定运行提供了有力保障。实践表明，这种优化模式能够有效降低事故发生概率，提升矿井安全管理水平。未来，随着信息技术的持续进步，该系统将进一步拓展功能，实现与生产调度、应急指挥等平台的深度融合，推动煤矿行业在数字化和智能化方向的高质量发展。

参考文献

[1] 刘志恒,孙建国.基于物联网的煤矿安全监测系统研究[J].煤炭工程,2023,55(8):112-118.

[2] 周景涛,魏鸿宇.煤矿安全生产智能化监测关键技术探讨[J].安全与环境学报,2022,22(5):45-52.

[3] 高彦磊,赵成浩.物联网技术在矿井安全监控中的应用与优化[J].工矿自动化,2024,50(3):77-83.

[4] 郑怀德,陈立鹏.矿山智能感知与预警系统设计方法研究[J].中国安全科学学报,2021,31(12):96-103.

 DOI: https://doi.org/10.12345/bdai.v6i6.34034

Legal compliance risks and countermeasures of artificial intelligence in the big health industry

Xinyue Zhang Taichu Wang

Beijing Sequoia Smith Partners, Beijing, 100004, China

Abstract

The rapid advancement of artificial intelligence (AI) is profoundly transforming operational models in China's healthcare sector. Cutting-edge technologies including deep learning, big data analytics, and natural language processing are now playing pivotal roles in disease diagnosis, pharmaceutical development, personalized health management, and public health initiatives. However, the widespread adoption of these innovations has inevitably raised legal compliance concerns, particularly regarding data security, privacy protection, and liability attribution. As China's legal framework continues to evolve, effectively mitigating AI-related compliance risks in healthcare applications has become a critical priority. This study examines legal compliance challenges and strategic solutions for AI implementation in the healthcare industry through theoretical analysis and practical case studies, providing actionable insights for policymakers and practitioners.

Keywords

Artificial Intelligence; Big Data; Healthcare Industry; Legal Compliance; Risks; Strategies

人工智能在大健康产业中的法律合规风险与对策

张馨月 王太初

北京市司凯律师事务所，中国·北京 100004

摘 要

快速发展的人工智能日益深入地影响着我国大健康行业的运行模式，现阶段以深度学习、大数据挖掘、自然语言处理为代表的一系列人工智能技术在诸如疾病诊治、药品研制、个人健康管理和公共卫生等方面发挥出重要作用。但与此同时，创新技术的应用不可否认带来了数据安全、隐私保护、责任承担主体认定等多方面法律合规风险。在法律规则体系不断完善进程下，如何有效规避人工智能在大健康产业中应用的法律合规风险就显得尤为关键。基于此，本文结合研究与实践就人工智能在大健康产业中的法律合规风险与对策展开探讨，以供参考。

关键词

人工智能；大数据；大健康产业；法律合规；风险；对策

1 引言

人工智能（AI）技术的蓬勃发展为大健康产业的深度融合带来新的契机。其强大的数据处理能力与智能决策支持系统，不仅能够精准匹配医疗服务供需，还能助力构建覆盖预防、诊疗、康复的全链条健康服务体系。但从实践情况来看，人工智能在大健康产业中应用法律合规风险较为突出，为此如何有效应对成为了一项重要内容。

2 人工智能与大数据在大健康产业的主要应用

2.1 医疗影像与智能测绘诊断

在大健康产业当中，人工智能在医疗影像方面应用较为广泛，其主要利用深度卷积神经网络（CNN）自动识别分割医学影像可以精准定位出疾病区域，比如目前部分国内医疗机构已经把人工智能技术应用到 CT 和 MRI 影像分析的过程中开展肺结节、脑部肿瘤和乳腺等级别智能化检测，并通过与院内 PACS 系统相连接让医生实时获取到病灶定量化诊断建议，大大提高影像阅片的速度以及准确性[1]。此外，基于深度强化学习的影像辅助诊断系统还可以为某些手术提供规划和导航服务，如骨科或者神经外科的手术可以利用三维重建和虚拟测绘提供更为精确的手术路径设计，从而实现更为安全、高效的操作。

2.2 药物研发与基因分析

人工智能应用于药物研发与基因分析上不仅能够大幅缩短新药研制时间，同时借助于通过大数据深度挖掘海量生物医学数据可以对药物作用靶点予以精准识别，从而给药物分子设计提供重要依据。药物研发以往主要通过实验筛选、结构推导，而应用人工智能技术经由分子动力学模拟、大数

【作者简介】张馨月（1989–），女，中国黑龙江牡丹江人，博士，从事生命大健康、法律合规、数据安全研究。

据回归来预测药物—靶点间作用力。国内部分制药企业目前利用机器学习算法开展化合物筛选、ADMET 特性预测，并基于高通量基因组学数据进行靶点识别模型开发，从而实现新药候选分子的自动生成，大幅缩短药物研制时间。此外，大数据在基因编辑、精准医学方面也有诸多应用，其通过对 WGS 数据的深度分析能够发现致病位点，辅助进行风险分层，比如肿瘤治疗上大数据通过利用多组学数据深度挖掘与分析可输出个性化治疗方案。

2.3 个性化健康管理与预测分析

人工智能和大数据相结合，在健康管理方面已经形成动态化、个性化的服务。从可穿戴设备获取的生理指标（包括心率、血糖、睡眠模式等）信息作为输入，人工智能算法利用时间序列分析和行为模式识别对用户的健康状况予以评估，并预测未来的疾病风险点。现阶段，部分互联网医疗平台打造的人工智能驱动的健康管理生态就是基于这个逻辑，在累积大量的用户端健康数据后通过人工智能与大数据建立起针对性用户的健康画像，从而为他们提供健康早期预警与干预决策。同时将用户的历史健康数据、体检报告等信息及生活方式结合起来进行深入关联分析之后，由人工智能健康管理系统提供生活干预和康复建议 [2]。另外，利用自然语言处理技术建立的智能问诊系统则为解决优质医疗资源分布不均的问题提供了一项重要的解决措施。

2.4 公共卫生与疫情预警融合

新时期下公共卫生治理领域，人工智能与大数据的应用日益发挥出重要价值。

人工智能算法通过整合多源数据（医院就诊记录、药店销售数据、交通流量、社交媒体舆情信息等），随后再借助于大数据深度挖掘传染病流行病学特征并预警其传播趋势、风险等级以及防控疫情发展。利用人工智能还可开展疫苗研发和公共卫生政策模拟，在世界范围内比对所有病原体的基因序列并根据病原体突变趋势为新疫苗设计提供技术支持，而通过机器学习模型开展智能流行病监测并用聚类技术追溯病例来源，在提高疾控机构紧急情况应急反应速率同时也为公共卫生决策制定提供依据。

3 人工智能在大健康产业的法律合规风险分析

3.1 数据隐私与个人信息保护风险

对大健康产业而言，人工智能应用的核心资源是数据，而医疗数据作为高度敏感的数据，我国相关法律法规明确对其采集、存储和跨境传输等方面都做了严格的规定。但从实际情况来看，现阶段人工智能在大健康产业中应用存在着数据匿名化与去标识化处理没有统一标准规范现象，这导致算法可逆重识别的风险。同时，有些医疗机构在开展数据共享和模型训练时没有履行好知情同意、最小必要原则造成患者隐私泄露或被滥用风险大增。另外，部分第三方算法服务商在参与大健康产业建模的过程当中对于权限的认定并不是特别明确，这样也会增加数据合规性管理风险。

3.2 算法歧视与决策透明性不足

结合实践来看，人工智能算法存在“黑箱性”有时会导致医疗决策出现不透明、不公正的情况，简单而言如果训练数据本身存在偏见，则算法也会在其模型构建过程中不可避免地产生隐形的歧视，例如性别、年龄上的不公正诊疗结果。现阶段我国法律上对于算法歧视缺乏系统的规制措施，同时在实际中医疗机构也往往只看算法准确率指标，对于公平性和解释性的要求往往选择忽略。另外，对于使用者来说，如果没有可供追溯算法决策逻辑的途径，医疗机构难以满足患者的知情权和解释权。

3.3 医疗责任认定与产品安全风险

人工智能应用于大健康产业的医疗场景中还会给传统医疗过错责任认定带来挑战，即当人工智能辅助系统被用于协助完成诊断和治疗决策后，一旦出现了误诊或损害的情形会出现责任主体难以认定。若该系统是由医疗机构自身研发，则可能因为其本身的算法具有过错而导致医疗机构承担过错责任；若该系统是由第三方提供的则涉及产品质量责任 [3]。因此人工智能以何种身份、什么类型的责任主体的适用，其主体资格需要进一步论证与完善。与此同时，民法典、医疗器械监督管理条例等规范性文件中对人工智能医疗产品的安全性仍然处在原则性的规定层面，未设置针对性人工智能自主学习特点的动态监管制度，这导致其存在较大的产品安全风险。

4 法律合规对策与建议

4.1 强化数据合规与隐私保护机制

基于人工智能引领下大健康产业发展中必须要强化数据合规与隐私保护，从而杜绝法律与伦理风险，具体为：首先，需要实施精细化的数据分级分类管理机制，将医疗数据按敏感度划分成一般性、敏感性以及高度敏感性三个等级，根据其敏感度设置不同级别的数据访问权限与最小化授权方案，并引入基于属性的访问控制（ABAC）模型，使数据能够根据个人的属性动态分配访问权限并及时进行校验，从而确保医疗数据不会被非法越权访问调用。其次，建立标准化的数据脱敏去标识化技术体系，采用 k —匿名、差分隐私、同态加密等多种保护措施，形成“算法不可逆识别”的技术壁垒，对于算法提供者、数据管理方和使用者分别予以责任归因，防范隐式身份重识别的风险出现在模型训练、推理阶段。此外，医疗数据共享和流通的过程中要建立“可信计算环境 + 区块链审计”的一体化管控体系，一方面在硬件上使用可信执行环境（TEE）完成安全计算隔离，另一方面在软件层面使用区块链分布式账本来记录数据调用、加解密以及访问的过程信息，如此一来保证流程的安全可追溯以及不能篡改。最后，医疗机构内部还应设立单独的数据合规管理制度，组建跨部门的人工智能数据合规评审制度，对医疗数