医学科学报 Medical Science News

主管单位：中国科学院
主办单位：中国科学报社
学术顾问单位：
中国人体健康科技促进会
国内统一连续出版物号：CN11-0289

地址：
北京市海淀区中关村南一条乙3号
邮编：100190
编辑部电话：010-62580821
发行电话：010-62580707
邮箱：ykb@stimes.cn

广告经营许可证：
京海工商广登字20170236号
印刷：廊坊市佳艺印务有限公司
地址：
河北省廊坊市安次区仇庄乡南辛庄村
定价：2.50元
本报法律顾问：
郝建平 北京灏礼默律师事务所

院士之声

吴世忠：注重医疗领域的数据安全问题

◉本报记者 刁雯蕙

近日，在香港中文大学（深圳）举办的2024新质生产力、医工融合创新大会上，中国工程院院士吴世忠以《人工智能视角下的医疗数据安全与患者隐私保护》为题进行主题报告。

他提到，随着人工智能（AI）技术的不断发展和迭代，人类社会已进入大算力、大模型、大数据、大应用时代。医疗领域早已引入人工智能，在流行病监测、药物研发、医疗影像识别、心理健康等方面发挥重要作用。与此同时，与之相随的数据安全隐患也日益凸显。

当前，医疗领域网络化、数字化、智能化进程面临的安全风险主要包括：数据泄露与隐私泄露、网络攻击与黑客入侵、数据篡改与伪造、不当访问与授权管理、医疗数据共享风险、数据存储的第三方服务风险、内部人员的泄密、数据冗余与保存不当、法律合规风险等。

首先是网络安全问题。随着人工智能技术的应用，网络安全风险出现了新变化，传统的网络安全问题受人工智能影响变得更加复杂，数据劫持、网络钓鱼、勒索攻击更加猖獗。

医疗领域的网络犯罪十分突出，医疗数据遭受攻击和破坏的案例不断增加。例如，2023年，印度新德里的全印度医学科学研究所医疗设备遭遇勒索病毒攻击；今年9月，美国人工智能医疗公司Confidant Health的服务器配置错误，泄露了5.3TB的敏感心理健康记录。根据IBM《2024年数据泄露成本报告》显示，医疗行业数据泄露平均成本达977万美元，连续14年成为数据泄露成本最高行业。

吴世忠

其次是模型安全问题。人工智能模型的安全性直接影响应用效果，尤其是在医疗领域，近年来已经暴露出一些问题，包括个人隐私泄露、算法或模型攻击、模型偏差以及系统脆弱性和网络安全。这些问题的主要原因是模型本身在可靠性和可解释性方面存在不足。例如，人工智能模型受到简单的扰动可能就会产生错误的输出，或者数据本身存在问题导致人工智能模型结果不准确。

再者，伦理问题也是人工智能在医疗领域应用中不可忽视的一个方面。全球多国发布了关于人工智能伦理文件，提出了包括合作、透明度、公平、非恶意责任、隐私等基本要求。医疗领域也提出了如何保护个人自主权、个人健康和安全以及公众利益等具体要求。然而，随着实际应用的推广，与人工智能相关的偏见、歧视、技术滥用、事故责任认定等伦理挑战越来越突出。

针对人工智能在医疗领域应用方面的风险问题，吴世忠从数据、安全和管理等角度进行分析。

在数据方面，要提高安全防护水平，确保数据安全和隐私保护，促进人工智能技术在现代医疗领域的转型和升级。数据是现代医疗的重要生产要素，具有很高价值。虽然当前医疗数据数量越来越大，但数据质量并没有随之提高，“数据孤岛”问题依然存在，数据协同合作动能和效能不足，跨境数据流动面临较多待破解难题等，亟须全方位突破。

在安全工作方面，要统筹安全与发展，强化安全保障体系。具体而言，要把软件作为网络安全服务的重点，确保医疗智能化系统的稳定性和可靠性。同时，需要加强医疗数据的保护，防范患者隐私数据丢失，但要确保促进正常的科研合作和数据流动。此外，还需要提高安全意识，通过定期培训与教育、营造安全文化氛围、模拟演练与应急响应、建立安全意识提示机制等举措，提升医疗行业从业人员整体的网络安全意识。

在管理方面，要坚持依法依规。做好“技管并重”。可以充分利用数字医疗技术、安全保障技术等手段确保人工智能技术在医疗领域的发展和安全。同时，还要高度重视对新技术安全风险方案的研究，严格遵守法规政策，遵循技术标准和行业规范，以确保人工智能应用的安全性。

免疫衰老领域首个多组学数据库设立

本报讯 记者近日从中国科学院北京基因组研究所（国家生物信息中心）了解到，该所研究员张维绮、鲍一明团队与中国科学院动物研究所研究员刘光慧、曲静研究组合作，建立了免疫衰老领域首个多组学数据库Immunosenescence Inventory，旨在为整合、分析与免疫衰老相关数据提供一体化平台。

随着全球人口老龄化趋势的加剧，老年人口的健康问题日益受到关注。免疫衰老作为影响老年人健康的关键因素之一，与感染性疾病的易感性增加和年龄相关慢性疾病的发病风险上升密切相关。免疫衰老通常被称为“炎症老化”，是指随着年龄增长、免疫系统功能逐渐减退的现象，包括新免疫细胞生成减少、现有免疫细胞功能改变以及慢性低度炎症状态持续存在。

该数据库由知识图谱、多组学数据集和工具三大核心模块组成。知识图谱模块构建了一个数字知识图谱，详细记录了免疫细胞类型、分子标志物、与免疫相关的基因注释、免疫细胞随年龄动态变化的特征、与衰老相关的细胞因子变化以及免疫衰老的生物标志物和干预策略。多组学数据集模块展示了不同物种免疫衰老的多维组学变化。其中，单细胞转录组学模块收集了来自4个物种、13种组织中59种免疫细胞的基因表达变化。工具模块则提供了在线工具，以辅助开展免疫细胞识别和免疫时钟计算。（冯丽妃）