·医学信息研究·

“人工智能 + 医疗”环境下健康档案隐私安全研究

王晓君 周翔宇

（邯郸市中心医院 邯郸 056008）

〔摘要〕 阐述“人工智能 + 医疗”发展必然性，分析“人工智能 + 医疗”健康档案数据在深度学习阶段数据利用、健康管理环节数据采集、诊断治疗环节数据分析等方面存在的安全隐患，提出相应隐私安全策略，包括加强顶层设计和数据保护、制定专项法律法规、强化技术保障及宣教等。

〔关键词〕 “人工智能 + 医疗”；健康档案；隐私安全

〔中图分类号〕R - 056 〔文献标识码〕A 〔DOI〕10. 3969/j. issn. 1673 - 6036. 2021. 02. 004

Study on Privacy Security of Health Records under the "Artificial Intelligence + Medical" Environment

WANG Xiaojun, ZHOU Xiangyu, Handan Central Hospital, Handan 056008, China

〔**Abstract**〕 The paper expounds the inevitability of "Artificial Intelligence (AI) + medical" development, analyzes the potential safety hazards of "AI + medical" health record data such as data utilization in the deep learning stage, data collection in the health management, data analysis in the diagnosis and treatment, puts forward corresponding privacy security strategies, including strengthening top - level design and data protection, formulating special laws and regulations, strengthening technical guarantee and education, etc.

〔**Keywords**〕 "Artificial Intelligence (AI) + medical"; health records; privacy security

1 引言

1956 年人工智能（Artificial Intelligence，AI）概念在达特茅斯会议上正式提出，被定义为如何表示知识、获得知识并使用知识的学科[1]，是以计算机、控制论、信息论、神经心理学、语言学、哲学等多学科为基础的综合性交叉学科[2]。随着社会发展和科技进步，其迈入前沿学科序列，成为新观念新思想不断碰撞、新理论新技术迅速交融的新型学科。“人工智能 + 医疗”是以互联网为载体、以智能化为目标，以云计算、大数据等信息技术为手段，与传统医疗健康服务深度融合的新型医疗健康服务业态的总称[3]，其在提高医院医疗服务智能化水平，实现预防医学、健康管理和辅助诊断等方面具有独特的优势。“人工智能 + 医疗”依托互联网大数据、强大运算能力和深度学习模式 3 要素，不仅推动医疗体制改革和医学技术发展，也一定程度迎合了患者对医疗服务的需求。

2 “人工智能 + 医疗”发展必然性

〔收稿日期〕 2020 - 03 - 04

〔作者简介〕 王晓君，硕士，馆员，发表论文 8 篇；通讯作者：周翔宇，工程师。

2.1 时代发展需求

当前欧美、日本等发达国家和地区纷纷加大对“人工智能 + 医疗”的科研投入，制定系列发展方案以抢占新一轮科技变革先机。紧随发展潮流我国加大对“人工智能 + 医疗”的重视和投入力度并使之上升为国家发展战略。在多方利好因素合力作用下，人工智能对智慧医疗和健康档案的拉动作用显著，已渗透到健康管理、辅助诊断、医疗机器人等领域，极大推动智慧医疗向高效率、高层次发展。

2.2 医疗改革要求

在全球“人工智能 + 医疗”浪潮推动下，我国对医疗健康领域提出人工智能发展要求。其中包括政策支持，健康信息化、医疗大数据、智能健康管理等具体应用，以及明确的人工智能发展方向。陆续出台《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》《新一代人工智能发展规划》等政策，助推人工智能新模式、新手段服务于智慧医疗及健康档案。

2.3 民众就医诉求

随着人工智能技术发展，大多数医院通过选择成熟的人工智能应用产品提高医疗服务水平。如就诊阶段可通过机器人实行导诊服务；付费阶段多样化支付方式有效分流人群；健康管理阶段治未病防患于未然；诊疗阶段辅助诊断让结果更加快速精准；远程诊疗使患者免受奔波之苦；数据完善阶段足不出户就可在网上完善健康档案。

3 健康档案隐私安全隐患

3.1 概述

健康档案是“人工智能 + 医疗”的重要应用领域，其隐私安全管理涵盖数据收集、分析及挖掘等环节，流程安全建设与维护也是全生命周期的。流转节点多、时间跨度长、维护难度大是健康档案安全管理的主要难点，因此在“人工智能 + 医疗”环境下健康档案各环节隐私安全建设亟须重视。

3.2 深度学习阶段的数据利用

“人工智能 + 医疗”系统发展有赖于对健康数据的深度学习，即让机器从海量的数据中学习总结经验，进而对数据的不确定性进行建模并预测未来。因此健康数据训练是提升人工智能准确性的必要因素。现有健康档案作为机器学习的训练数据具有成本低、真实性高、易于获取等优势。但是不做限制地使用健康档案则可能引起一系列信息安全问题。如果过于注重患者的隐私保护则会制约“人工智能 + 医疗”长远发展。如何平衡健康数据利用和患者隐私保护之间的关系仍需深入研究探讨[1]。

3.3 健康管理环节的数据采集

健康管理旨在防未病、降低大病或大规模疾病暴发概率，以期提高民众整体健康水平。在人工智能浪潮不断推进下，健康管理工作已实现信息化、移动化、网络化，即可通过“智能 + 预防”手段实现“治未病”。以某健康管理部门为例，其主要关注个人健康管理和生活习惯提升，即通过健康管理优化平台进行习惯干预和预防性健康管理。用户需在网站上传自己的基因、代谢和性状数据，平台依据数据提供饮食起居等方面生活建议，帮助用户规避患病风险[4]。其中在数据采集过程中信息意外泄露事件时有发生，智能健康管理档案安全问题成为关注焦点。

3.4 诊断治疗环节的数据分析

目前部分医疗机构将人工智能应用到诊疗环节，在缓解优质医疗资源短缺带来影响的同时，也为医、护、患 3 方带来更多智能和便利体验。如人工智能可以帮助医护收集患者健康信息，协助医生解读医疗影像，智能机器人可对患者进行导引，达芬奇手术机器人开展外科手术，应用人工智能在手术室辅助进行术前评估、方法选择等麻醉管理。但随着人工智能产品落地及广泛使用，患者隐私、伦理等方面问题需要进一步考虑。如相关人员业务能力不强、防范意识不够，或遭外部恶意网络攻击、黑客利用非法技术对健康数据进行窃取，患者就诊

时对信息安全不够重视等因素造成信息泄露，一旦用于非法识别患者身份等违法违规活动[5-6]将造成严重社会影响。

3.5 二次利用环节的数据挖掘

健康信息二次利用是指将个人健康数据用于疾病研究分析，如公共卫生领域研究、卫生服务质量测评、卫生政策研究等[7-8]，当前健康数据安全中最受争议的是数据挖掘环节。数据权属拥有者和持有者是分离的，且尚缺乏对数据权属和持有者公认可行的界定和管理方法[1]。如健康数据一般在就医过程中产生，其权属拥有者应是患者。但事实上数据持有者和使用者通常是医疗和科研机构，因医用和研发目的对医疗大数据进行分析和挖掘，通常在数据脱敏后公开使用，但与其他数据关联后可能造成个人隐私泄露，如果含有基因数据则隐私安全威胁将更加凸显[9]。

4 隐私安全策略

4.1 顶层建设

人工智能在医疗领域实施进程中亟待加强顶层设计和数据保护，以保障健康档案信息安全。首先制定一系列完备制度、流程和风险应对机制以有效应对数据泄露等突发事件；其次完善收集、流转、分析、存储以及数据中心访问等关键节点、关卡安全防护，提高医务工作者、医疗科研机构从业者的防护意识；最后从整体思维出发，在组织架构、法律保障、技术队伍、加强宣教等方面入手，做出详尽周密的要求规定，建立分级授权、分类应用和权责一致的管理制度，构建层级防护体系，切实保护民众隐私和健康档案安全。

4.2 法律先行

针对“人工智能+医疗”健康数据在采集、挖掘和进一步使用过程中出现黑客攻击或数据泄露等现象，亟须法律法规予以规范。如针对“人工智能+医疗”数据保护制定专项法律法规，借助法律明确数据应用、信息安全和隐私保护之间边界，积极推进法律适用和落实执行等配套机制，明确要求各医疗机构及相关人员必须采取适当措施保护患者信息安全[10]。与此同时加大对侵犯、窃取、贩卖健康数据和档案等犯罪行为打击力度，提升犯罪成本，发挥法律引导功能。

4.3 技术保障

加大技术投入，做好主动防控。人工智能产品应用前进行严格把控和安全评估，对其安全性、可控性和操作人员可信性进行持续监管。针对所有健康数据制定明确严格的访问控制程序，通过严谨周密安排确保数据安全性。为切实保护患者隐私和健康档案安全，防止人为从后台查询患者敏感数据，需对数据进行分级管理。如涉及患者身份的信息要进行去标识化、基因信息要进行替换、姓名信息要脱敏处理，以及实施数据封装、分离等措施[11]。进行数据分析时要进行强加密处理，确保即使数据泄露也无法解密盗取。

4.4 加强宣教

管理学认为人是最大的风险来源，也是可变性最大的风险因素。针对“人工智能+医疗”中健康档案安全性问题，需反思医疗人工智能制造者和使用者应该具备和遵循哪些道德素养和标准[10]。因此加强宣教、对医疗及相关机构从业人员开展针对性教育培训，是当前完善“人工智能+医疗”安全防范的有效途径。培训内容应包括信息安全知识、隐私保护和法制教育。特别要对风险防控规定进行宣传，明确机构、岗位人员在健康数据系统风险管控中应尽的责任和义务，确保相关人员在思想上提升风险防控意识并在行动上落实。

5 结语

未来人工智能发展与诊疗模式创新将在一定程度上促进医疗健康运营模式转型。在这场变革中医疗机构及医务人员需要在医疗技术服务上做出积极改变，从共情角度出发设身处地为患者着想，切实维护患者

（下转第28页）

模式、业务场景和就医流程。需要充分考虑基层医疗机构特点，在人工智能产品设计、医疗场景搭建和业务模式构建上选择适合在基层医疗机构开展的临床业务。如利用人工智能提升基层在常见病、多发病方面的诊断能力，开展与基层医疗机构设施设备配置相匹配的人工智能诊疗服务，利用人工智能降低诊疗服务对基层人才专业技能水平的要求等。

5.3.2 提升患者信心[11] 疾病诊断是复杂的综合过程，目前人工智能技术发展水平远未达到完全取代医生诊断的程度，主要起辅助诊断作用。因此人工智能技术在辅助基层诊疗服务初期首先要取得基层患者信任，需要高水平医疗机构参与和质量把控，逐渐建立患者对基层就诊的信心，才能真正落地、推进。

6 结语

随着人工智能技术快速发展，产品不断成熟并与互联网、云计算等信息技术深度融合，会推出越来越多医疗人工智能产品和临床业务系统。相信未来会有更多“西湖模式”落地服务于分级诊疗建设，为实现优质医疗资源下沉、解决基层看病困难问题提供思路和技术方案。在人工智能技术支持下基层医疗机构服务能力将不断增强，从而有力推动国家分级诊疗体系建立。

参考文献

1 王海星，田雪晴，游茂，等. 人工智能在医疗领域应用现状、问题及建议［J］. 卫生软科学，2018，32（5）：3－5.

2 谢宇，于亚敏，佘瑞芳，等. 我国分级诊疗发展历程及政策演变研究［J］. 中国医院管理，2017，37（3）：24－27.

3 周晓梅，杨春松，林芸. 国内分级诊疗现状的系统评价［J］. 中国药房，2017，28（34）：4763－4766.

4 王烨. 基层医疗人才现状及需求分析［J］. 时代金融，2015（5）：164.

5 孙佳丽，尹梅. 我国分级诊疗面临的困境及对策建议［J］. 中国医学伦理学，2018，31（2）：236－240.

6 张莎莎，李雯，张岩. 我国分级诊疗的现状分析及人工智能对策浅探［J］. 中国妇幼健康研究，2017，28（3）：165－166.

7 洪建，颜雨春，周典，等. “互联网＋”时代下分级诊疗模式建设思考［J］. 中国数字医学，2018，13（1）：19－26.

8 萧毅，刘士远. 人工智能将改变影像医学的未来［J］. 科技与金融，2018（10）：11－15.

9 赵嘉莹，高鹏，朱勇俊，等. 人工智能的应用将改进中国基层医疗卫生服务效能［J］. 中国全科医学，2017，20（34）：4219－4223.

10 萧毅，刘士远. 医学影像人工智能进入深水区后的思考［J］. 中华放射学杂志，2019，53（1）：2－5.

11 李显文. 对我国分级诊疗模式相关问题的思考［J］. 卫生经济研究，2015（3）：18－20.

（上接第 24 页）

健康信息和隐私安全，使人工智能技术更好地助力医疗、服务患者，进而推进健康中国建设。

参考文献

1 张学高，周恭伟. 人工智能＋医疗健康：应用现状及未来发展概论［M］. 北京：电子工业出版社，2019.

2 苗芳芳，刘骏峰. 论人工智能的发展及其在医学领域的应用前景［J］. 卫生软科学，2009，23（2）：222－224.

3 庞涛. 国家卫计委首次定义“互联网＋医疗健康”［J］. 中国信息界：e 医疗，2015，8（8）：9.

4 王晨阳，潘习龙，吴曼琪，等. 人工智能在医学领域应用浅析［J］. 中华医院管理杂志，2020，36（1）：50－52.

5 马诗诗，于广军，崔文彬. 互联网医疗的隐私保护与信息安全［J］. 上海医药，2017，48（9）：14－16.

6 舒婷. “互联网＋”时代的患者隐私保护［J］. 中国数字医学，2016，11（5）：41－43.

7 Safran C，Bloomrosen M. Toward a National Framework for the Secondary Use of Health Data：an American medical informatics association white paper［J］. Am Med Inform Assoc，2007（14）：1－9.

8 K Holzer，W Gall. Utilizing IHE－based Electronic Health Record Systems for Secondary Use［J］. Methods of Information in Medicine，2011，50（4）：319－325.

9 王爽，尹聪颖. 健康医疗大数据时代的隐私保护探析［J］. 医学信息学杂志，2019，40（1）：2－5.

10 包桉冰，徐佩. 医疗人工智能的伦理风险及应对策略［J］. 医学与哲学，2018，39（6A）：37－40.

11 谭太昌，王甲甲，王加强，等. “互联网＋”背景下医院信息系统风险管理研究［J］. 医学信息学杂志，2018，39（11）：36－39.