Journal of Arak University of Medical Sciences
Volume 28, Issue 5
December & January 2025-2026

Letter to Editor

The Ethical and Legal Imperative in the Age of AI: Safeguarding Patient Data and Privacy in Healthcare

Mir Amirhossein Seyednazari[1], Hamed Gholizad Gougjehyaran[2], Amin Soheili[3], Amir Mohammad Dorosti[*4], Rasul Asghari[5]

[1] MSc in Medical-Surgical Nursing, Department of Medical-Surgical Nursing, Khoy School of Medical, Khoy, Iran
[2] Student Research Committee, Tabriz University of Medical Sciences, Tabriz, Iran
[3] Associate Professor, Department of Nursing, Student Research Committee, Khoy University of Medical Sciences, Khoy, Iran
[4] MSc Student, Medical-Surgical Nursing, Student Research Committee, Khoy School of Medical Sciences, Khoy, Iran
[5] BSc in Nursing, Department of Nursing, School of Medical Sciences, Khoy, Iran.

*** Corresponding author**: Amir Mohammad Dorosti, Faculty of Medical Sciences, Khoy, Iran.
Email: amirdorosti2006@gmail.com

DOI: 10.61882/jams.28.5.320

How to Cite this Article:
Seyednazari MM, Gholizad Gougjehyaran H, Soheili A, Dorosti AM, Asghari R. The Ethical and Legal Imperative in the Age of AI: Safeguarding Patient Data and Privacy in Healthcare. *J Arak Uni Med Sci*. 2025;**28**(5): 320-23. DOI: 10.61882/jams.28.5.320

Received: 16.10.2025
Accepted: 09.11.2025

Keywords
Artificial Intelligence (AI);
Medical Ethics;
Data Privacy;
Health Data;
Black Box (Algorithm

Dear Editor

The rapid integration of Artificial Intelligence (AI) into medical sciences, while promising transformative breakthroughs in early diagnosis and personalized treatments (1), introduces a profound ethical and legal challenge: the management of the vast, sensitive, and unprecedented volume of health data and the preservation of patient privacy. The nature of this data, which includes clinical records, radiological images, genetic data, and even data from wearable health devices [2], extends beyond traditional identifiable information. It possesses the capability to reconstruct a comprehensive profile of an individual, rendering complete and permanent de-identification virtually impossible (1).

This massive volume of information has become the main fuel for deep learning algorithms, but any breach or disclosure could lead to serious discrimination in access to insurance, employment, and even judicial decision-making (2). The lack of Transparency regarding how these data are processed and analyzed by the algorithms, which often function as a "black box," erodes the trust of both patients and physicians (3). Healthcare providers cannot understand the AI's decision-making process, which not only hinders clinical adoption but also creates a legal gray area concerning accountability in the event of diagnostic or therapeutic error (4).

The current legal challenge stems from the fact that existing privacy laws were not designed to address advanced algorithms and real-time data collection (1, 4). AI constantly outpaces existing legal frameworks by creating novel methods of knowledge extraction from raw data. Furthermore, due to their reliance on large data networks, AI tools are exposed to advanced cyberattacks, which could lead to the mass disclosure of confidential data (5). Consequently, in the absence of a robust

and up-to-date data governance framework, AI's potential to improve public health is accompanied by the risk of undermining human dignity and violating fundamental patient rights (6).

To ensure that AI innovations advance with ethical and legal compliance, urgent measures must be taken to establish a comprehensive regulatory framework. This requires formulating a new, dynamic model of informed consent that goes beyond a one-time agreement, allowing patients continuous and informed control over how their data is used at different stages of AI training and deployment. Concurrently, developers must be mandated to embed privacy protection at the core design of every AI tool, which means utilizing advanced privacy-preserving techniques such as differential privacy and federated learning for on-premise data processing. Additionally, a multi-disciplinary oversight body composed of ethics, legal, computer science, and clinical experts must be established, ensuring that every AI tool undergoes a rigorous and transparent ethical and technical assessment and approval process before entering the clinical environment, thereby preventing potential biases and algorithmic errors. These measures will not only protect patients against misuse but also provide the necessary trust for the sustainable and safe advancement of this vital technology in society.

Ethical Consideration

Compliance with ethical guidelines

All procedures performed in the research involving human participants were in accordance with the ethical standards of the ethics committee

Funding

This research did not receive any grant from funding agencies in the public, commercial, or not for profit sectors.

Acknowledgements

The authors would like to express their sincere gratitude to the Khoy University of Medical Sciences.

Authors' contributions

The authors had equal contribution to the preparation of the manuscript.

Conflict of Interest

The authors declare no conflict of interest.

فراتر از الگوریتم: ضرورت تدوین قوانین اخلاقی برای حفظ حریم خصوصی داده‌های سلامت در عصر هوش مصنوعی

میر امیرحسین سید نظری[۱]، حامد قلیزادگوگجه یاران[۲]، امین سهیلی[۳]، امیرمحمددرستی*[۴]، رسول اصغری[۵]

[۱] گروه پرستاری داخلی جراحی، دانشکده علوم پزشکی خوی، خوی، ایران
[۲] کمیته تحقیقات دانشجویی، دانشگاه علوم پزشکی تبریز، تبریز، ایران.
[۳] دانشیار، گروه پرستاری، کمیته تحقیقات دانشجویی، دانشکده علوم پزشکی خوی، خوی، ایران
[۴] دانشجوی کارشناسی ارشد پرستاری داخلی و جراحی، کمیته تحقیقات و فناوری دانشجویی، دانشکده علوم پزشکی خوی، خوی، ایران
[۵] گروه پرستاری، دانشکده علوم پزشکی خوی، خوی، ایران

* نویسنده مسئول: امیرمحمددرستی، دانشکده علوم پزشکی خوی، خوی، ایران. ایمیل:amirdorosti2006@gmail.com

DOI: 10.61882/jams.28.5.320

تاریخ دریافت: ۱۴۰۴/۰۷/۲۴
تاریخ پذیرش: ۱۴۰۴/۸/۱۸

واژگان کلیدی:
هوش مصنوعی؛
اخلاق پزشکی؛
حریم خصوصی داده‌ها؛
داده‌های سلامت؛
جعبه سیاه (الگوریتم)

ارجاع: سید نظری میر امیرحسین، قلیزادگوگجه یاران حامد، سهیلی امین، درستی امیرمحمد، اصغری رسول. فراتر از الگوریتم: ضرورت تدوین قوانین اخلاقی برای حفظ حریم خصوصی داده‌های سلامت در عصر هوش مصنوعی. *مجله دانشگاه علوم پزشکی اراک* ۱۴۰۴؛ ۲۸ (۵): ۳۲۰- ۳۲۳.

نامه به سردبیر

ادغام سریع هوش مصنوعی (Artificial Intelligence) AI در علوم پزشکی، هرچند با وعده‌های تحول‌آفرین در تشخیص زودهنگام و درمان‌های شخصی سازی شده همراه است (۱)، اما یک چالش اخلاقی و حقوقی عمیق را به همراه دارد :مدیریت حجم عظیم، حساس و بی‌سابقه داده‌های سلامت و حفظ حریم خصوصی بیماران. ماهیت این داده‌ها، که شامل سوابق بالینی، تصاویر رادیولوژی، داده‌های ژنتیکی و حتی اطلاعات پوشیدنی‌های سلامت فردی است (۲)، فراتر از اطلاعات هویتی سنتی است و قابلیت باز سازی پروفایل کامل یک فرد را دارا ست؛ امری که هویت‌زدایی کامل و دائم آن‌ها را عملاً ناممار می‌سازد (۱).

این حجم گسترده از اطلاعات به سوخت اصلی الگوریتم‌های یادگیری عمیق تبدیل شده است، اما هر گونه نقض یا افشا، می‌تواند منجر به تبعیض جدی در دسترسی به بیمه، استخدام و حتی تصمیم‌گیری‌های قضایی شود (۲). فقدان شفافیت (Transparency) در مورد چگونگی پردازش و تحلیل این داده‌ها توسط الگوریتم‌ها، که اغلب به صورت «جعبه سیاه» عمل می‌کنند، اعتماد بیماران و پزشکان را تضعیف می‌کند (۳). کادر درمان نمی‌توانند فرآیند تصمیم‌گیری هوش مصنوعی را درک کنند، و این مسئله نه تنها مانع از پذیرش بالینی می شود، بلکه یک منطقه خاکستری حقوقی در مورد مسئولیت‌پذیری در صورت بروز خطای تشخیصی یا درمانی ایجاد می‌کند (۴).

چالش حقوقی موجود در این است که قوانین فعلی حریم خصوصی برای مواجهه با الگوریتم های پیشرفته و جمع‌آوری داده های لحظه‌ای طراحی نشده‌اند (۱، ۴). هوش مصنوعی با ایجاد روش‌های نوین استخراج دانش از داده‌های خام، دائماً از چارچوب‌های قانونی موجود پیشی می‌گیرد. علاوه بر این، ابزارهای هوش مصنوعی به دلیل اتکا به شبکه‌های داده‌ای بزرگ، در معرض حملات سایبری پیشرفته قرار دارند، که می‌تواند منجر به افشای گروهی داده‌های محرمانه شود (۵). در نتیجه، در غیاب یک چارچوب حکمرانی داده‌های محکم و به‌روز، پتانسیل هوش مصنوعی برای بهبود سلامت عمومی با خطر تضعیف کرامت انسانی و نقض حقوق بنیادی بیمار همراه است (۶).

برای تضمین اینکه نوآوری‌های هوش مصنوعی با رعایت اصول اخلاقی و حقوقی پیش می‌رود، ضـــروری اســـت که اقداماتی عاجل در جهت ایجاد یک چارچوب نظارتی جامع صورت پذیرد. این امر نیازمند تدوین یک مدل جدید و پویا از ر ضایت آگاهانه ا ست که فراتر از ر ضایت یک‌باره با شد و به بیماران اجازه دهد تا بر نحوه اســـتفاده از داده‌هایشـــان در مراحل مختلف آموزش و به‌کارگیری هوش مصنوعی کنترل مستمر و آگاهانه داشته باشند. همزمان، باید توسعه‌دهندگان را موظف کرد که حفاظت از حریم خصوصی را در هســـته طراحی هر ابزار هوش مصـــنوعی قرار دهند، که به معنای استفاده از تکنیک‌های پیشرفته حفظ حریم خصوصی مانند حریم خصوصی تفاضلی و یادگیری فدرال برای پردازش داده‌ها در محل است. علاوه بر این، باید با تشکیل یک نهاد نظارتی چند رشته‌ای متشکل از متخصصان اخلاق، حقوق، علوم کامپیوتر و بالینی، هر ابزار هوش مصـــنوعی قبل از ورود به محیط بالینی، تحت یک فرآیند ارزیابی و تأیید اخلاقی و فنی دقیق و شـــفاف قرار گیرد تا از تعصـــبات احتمالی و خطاهای الگوریتمی جلوگیری شود.این اقدامات نه تنها بیماران را در برابر سوءا ستفاده محافظت می‌کند، بلکه اعتماد لازم برای پیشـــبرد پایدار و ایمن این فناوری حیاتی را نیز در جامعه فراهم می‌آورد.

سهم نویسندگان

تمامی نویســـندگان در طراحـــی ایـــن مقالـــه، ارائـــه مطالـــب علمـــی، تهیـــه نســـخه خطـــی و تجدیدنظـــر نســـخه نهایـــی بـــه صورت مســـاوی مشـــارکت داشـــته‌اند.

تضاد منافع

بنابر اظهار نویسندگان، این مقاله تعارض منافع ندارد.

سهم نویسندگان

تمامی نویسندگان در تمامی قسمت‌های مقاله نقش داشتند.

تضاد منافع

نویسندگان تصدیق می‌کنند که هیچ تضاد منافعی وجود ندارد.

References

1. Kooli C, Al Muftah H. Artificial intelligence in healthcare: a comprehensive review of its ethical concerns. Technological Sustainability. Technological Sustainability. 2022;1(2):121–31. **doi:**10.1108/TECHS-12-2021-0029
2. Price WN 2nd, Cohen IG. Privacy in the age of medical big data. Nat Med. 2019;25(1):37-43. **pmid:** 30617331 **doi:** 10.1038/s41591-018-0272-7
3. Mennella C, Maniscalco U, De Pietro G, Esposito M. Ethical and regulatory challenges of AI technologies in healthcare: A narrative review. Heliyon. 2024;10(4):e26297. **pmid**: 38384518 **doi:** 10.1016/j.heliyon.2024.e26297
4. Singh MP, Keche YN. Ethical Integration of Artificial Intelligence in Healthcare: Narrative Review of Global Challenges and Strategic Solutions. Cureus. 2025;17(5):e84804. **pmid**: 40568260 **doi**: 10.7759/cureus.84804
5. Rieke N, Hancox J, Li W, Milletarì F, Roth HR, Albarqouni S, et al. The future of digital health with federated learning. NPJ Digit Med. 2020;3:119. doi:10.1038/s41746-020-00323-1
6. Abujaber AA, Nashwan AJ. Ethical framework for artificial intelligence in healthcare research: A path to integrity. World J Methodol. 2024;14(3):94071. **pmid**: 39310239 **doi**: 10.5662/wjm.v14.i3.94071