Editorial

Ethics in Managing Big Data: Ensuring Privacy and Data Security while Using ChatGPT in Healthcare

Russell D'Souza[1], Avinash De Sousa[2]

[1]Chair Department of Education International Chair in Bioethics (Formerly UNESCO Chair in Bioethics) Melbourne Australia.
[2]Consultant Psychiatrist and Founder Trustee, Desousa Foundation, Mumbai.
Corresponding Author: Avinash De Sousa
E-mail: avinashdes888@gmail.com

(Received – January 3rd 2023; Modified – January 10th 2023; Accepted – January 20th 2023)

Introduction
Designed and developed by San Francisco-based OpenAI, ChatGPT emerged as one of the most influential Artificial Intelligence (AI) based language models and is capable of mimicking conversations with humans [1-2]. Surpassing this, GPT-4 has taken the stage now. More than ever, GPT-4 fosters collaboration and creativity. It can produce, edit, and collaborate with users on artistic and technical writing jobs, including song writing, screenwriting, or figuring out a user's writing style. GPT-4 can generate descriptions, classifications, and analyses based on the inputs of photographs. GPT-4 can also process more than 25,000 words of written content, making it suitable for tasks like creating long documents, having lengthy discussions, and performing research and evaluations [3-4].

ChatGPT and its abilities
Although AI-based language models like ChatGPT-4 have shown outstanding capabilities, it is unclear as to how effectively they will work in everyday circumstances, especially in sectors like healthcare where nuanced reasoning at an advanced level is required [5]. ChatGPT-4 recognises and responds to numerous conversational inputs in healthcare, including enquiries, complaints, and instructions. It can communicate with patients in a natural and human-like manner, which is useful for chatbots, customer service representatives, and virtual assistants [6]. ChatGPT-4 may improve patient outcomes by increasing adherence to treatment regimens and providing more practical and accessible care than a human healthcare practitioner [7]. Patients may find ChatGPT-4 to be a convenient and welcoming way to obtain information and advice while determining how to manage their ailment. It provides solutions to patient inquiries, increasing satisfaction and decreasing the need for human care. It improves communication among patients, insurance companies, and healthcare experts [9]. ChatGPT-4 may assist in providing relevant stakeholders with timely access to essential healthcare information [10]. Also, patients who live in disadvantaged or remote regions may have difficulty physically meeting a licenced healthcare specialist. These individuals can sort the help of ChatGPT-4 to obtain assistance and knowledge from a reliable source, even if they are unable to visit the healthcare facility physically [11].

In addition to this, ChatGPT-4 can also support healthcare staff with mundane tasks such as report preparation and medical record transcribing [12]. The GPT-4 system should be trained to transcribe patient medical records, allowing medical professionals to spend more time connecting accurately and swiftly with patients and providing empathetical care. It can also reduce the likelihood of medical record mistakes [13]. However, these specialised natural language processing (NLP) algorithms trained on (bio)medical datasets pose a risk for vital clinical applications, as the most recent versions of ChatGPT have only average or 'passing' results in several assessments and are undependable for real clinical use [14].

Despite the numerous advantages that the newer versions of ChatGPT could provide, the ethical issues that stand ahead pose the major challenge to the successful implementation of such novel AI-based innovations. Ethical considerations surrounding using ChatGPT-4 in healthcare include data privacy and security, intellectual property, transparency and accountability, bias and fairness, misinformation, autonomy, misuse and abuse [15-16]. Particularly, the use of AI systems like ChatGPT-4 in healthcare raises significant privacy and data security concerns, particularly regarding the handling of sensitive health information.

Privacy and Security

To ensure privacy and data security, AI developers and policymakers must ensure compliance with data protection requirements. They must adhere to regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) [17] and the General Data Protection Regulation (GDPR) [18]. These standards outline procedures for managing, storing, and distributing confidential health data in an encrypted format. The HIPAA Privacy Rule's main purpose is to ensure that the health data of patients are appropriately protected while enabling the exchange of health information required to provide and foster superior medical care, as well as safeguard the public's health and well-being [19]. At the same time, the General Data Protection Regulation (GDPR) is a regulatory framework that establishes criteria for the gathering and handling of identifiable data from individuals living in and outside of the European Union (EU). The GDPR was approved in 2016, and its goal is to offer customers access to their private data by holding corporations accountable for how this data is handled and used [20].

Integrating privacy and data security into all stages of AI development is critical for assuring robust patient data protection. Developers may create AI systems that prioritise data protection from the start by adding privacy by design principles. Health data such as patients' personal information, disease history, treatment history, insurance policies etc, are highly sensitive and personal and need to be safeguarded by the information users. Any unauthorised disclosure or theft of data will lead to serious consequences. Thus, protecting and handling patients' health information is crucial in the cybersecurity of the healthcare industry. Thus, when AI models like ChatGPT-4 are to be implemented to advance the healthcare field, precautions and measures should be taken to secure patient data. This could be possible by encrypting the medical data with multi-factorial authentication such that unauthorised access to information can be prevented. Upgrading the software with the latest security patches and intrusion detectors may also be necessary. Also, evaluating and controlling possible risks to security regularly can assist medical organisations in discovering and fixing bugs before they are misused [21-22].

It is also critical to provide patients with clear and accessible consent methods for data sharing and processing to maintain control over their health information. There are many ethical and legal challenges alongside implementing AI systems like ChatGPT in healthcare and obtaining informed consent. AI literature's emphasis on transparency and explain ability is important to the idea that consent should be informed. Even though the focus is frequently on technologists, this presupposes that all stakeholders--those impacted by the AI component's output, those utilising it for decision assistance, and those designing it--are equally responsible for the consent process [23-24]. Thus, AI developers should prioritise transparency in their data management practices and give patients the tools they need to make informed data decisions.

Finally, data minimization and anonymization approaches can assist in protecting patient privacy while allowing AI systems to get significant insights from health data. Data minimisation is one of the directions in many privacy rules and data protection acts, and it refers to the practice of restricting private data gathering and processing to only what is essential to serve a given goal [25]. On the other hand, anonymisation is the process of altering one's identity into something unrecognisable so that the action of establishing an association with one's original identification is permanent [26]. The introduction of AI-based systems like ChatGPT should ensure that this big

medical data is handled ethically, and patient information is highly protected so that there is no secondary flow of information. Leakage of such personal information can lead breach of trust and reliability of healthcare systems [27]. As data minimisation and anonymisation play key roles in safeguarding patient health records, techniques such as differential privacy can be used to add statistical noise to data while maintaining individual privacy and preserving the data's utility for AI systems.

Conclusions

Thus, the integration of ChatGPT in healthcare has the potential to enhance patient outcomes and optimise healthcare delivery. However, it is of the utmost importance to protect patient privacy and ensure data security by following regulations such as HIPAA and GDPR, as well as implementing principles such as informed consent, transparency, data minimization, and anonymization, where patients are informed about the way the information they provide is being used, what dangers may be involved in it, and what strategies are being put in place to safeguard their privacy. Patients should also be given the right to decline using ChatGPT or any other likely AI model. Furthermore, to ensure the successful implementation of AI models like ChatGPT, developers, as well as healthcare providers, must be clear about how they use such technology to retain and manage any data that is collected.

REFERENCES

1. Introducing ChatGPT. Available from: https://openai.com/blog/chatgpt. [Last Accessed: 10 May 2023]
2. Chat GPT Online. Available from: https://chatgptonline.ai. [Last Accessed: 10 May 2023]
3. GPT-4 is OpenAI's most advanced system, producing safer and more useful responses. Available from: https://openai.com/product/gpt-4. [Last Accessed: 10 May 2023]
4. What is GPT-4 and how does it differ from ChatGPT? Available from: https://www.theguardian.com/technology/2023/mar/15/what-is-gpt-4-and-how-does-it-differ-from-chatgpt. [Last Accessed: 10 May 2023]
5. Cascella M, Montomoli J, Bellini V, Bignami E. Evaluating the feasibility of ChatGPT in healthcare: an analysis of multiple clinical and research scenarios. J Med Systems 2023;47(1):33-5.
6. Homolak J. Opportunities and risks of ChatGPT in medicine, science, and academic publishing: a modern Promethean dilemma. Croatian Med J 2023;64(1):1–3.
7. Santandreu-Calonge D, Medina-Aguerrebere P, Hultberg P, Shah MA. Can ChatGPT improve communication in hospitals? Profesional De La información 2023;32(2).
8. van Schalkwyk G. Artificial intelligence in pediatric behavioral health. Child Adolesc Psychiatry Ment Health 2023;17(1):1-2.
9. Xue VW, Lei P, Cho WC. The potential impact of ChatGPT in clinical and translational medicine. Clin Translat Med 2023;13(3):e1216.
10. Lee H. The rise of ChatGPT: Exploring its potential in medical education. Anatomical Sci Educ 2023;1:1– 6.
11. Iftikhar L. DocGPT: Impact of chatbot-3 on health services as a virtual doctor. EC Paediatrics 2023;12(1):45-55.
12. Eysenbach G. The Role of ChatGPT, Generative Language Models, and Artificial Intelligence in Medical Education: A Conversation With ChatGPT and a Call for Papers JMIR Med Educ 2023;9:e46885.
13. Javaid M, Haleem A, Singh RP. ChatGPT for healthcare services: An emerging stage for an innovative perspective. Bench Council Transactions on Benchmarks, Standards Evaluat 2023;3(1):100105..
14. Li J, Dada A, Kleesiek J, Egger J. ChatGPT in Healthcare: A Taxonomy and Systematic Review. medRxiv. 2023:2023-03.
15. Ray PP. ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope, Internet of Things and Cyber-Physical Systems, Volume 3, Pages 121-154; 2023.
16. Malik S. ChatGPT Utility in Healthcare Education, Research, and Practice: Systematic Review on the Promising Perspectives and Valid Concerns. Healthcare 2023;11(6):887.
17. Atchinson BK, Fox DM. The politics of the Health Insurance Portability and Accountability

Act. Health Affairs 1997;16(3):146–50.
18. Information Commissioner's Office Guide to the General Data Protection Regulation (GDPR) Available from: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/whats-new/ [Last Accessed: 11 May 2023]
19. Centres for Disease Control and Prevention. Available from: https://www.cdc.gov/phlp/publications/topic/hipaa.html [Last Accessed: 11 May 2023]
20. General Data Protection Regulation (GDPR) Definition and Meaning. Available from: https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp [Last Accessed: 11 May 2023]
21. Mijwil M, Aljanabi M, Ali AH. ChatGPT: Exploring the role of cybersecurity in the protection of medical information. Mesopotamian J Cybersecurity 2023;1:18-21.
22. Zhou J, Ke P, Qiu X. et al. ChatGPT: potential, prospects, and limitations. Front Inform Technol Electron Eng 2023;1.
23. Pickering B. Trust, but Verify Informed Consent, AI Technologies, and Public Health Emergencies. Future Internet 2022;13(5):132.
24. Astromskė K, Peičius E, Astromskis P. Ethical and legal challenges of informed consent applying artificial intelligence in medical diagnostic consultations. AI Soc 2021;36:509–20.
25. Mukta R, Paik H, Lu Q, Kanhere SS. A survey of data minimisation techniques in blockchain-based healthcare. Computer Networks 2022;205:108766.
26. Muñoz-Cobo JL, Rivera Y, Berna C, Escrivá A. Analysis of conductance probes for two-phase flow and holdup applications. Sensors 2020;20(24):7042.
27. Mittelstadt BD, Floridi L. The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. In: Mittelstadt, B., Floridi, L. (eds) The Ethics of Biomedical Big Data. Law, Governance and Technology Series, vol 29. Springer, Cham. 2023.

****

Acknowledgements: Nil
Conflict of interest: Nil
Funding: Nil