swiss medical weekly

Technical comment | Published 28 February 2025 | doi:https://doi.org/10.57187/s.4359
Cite this as: Swiss Med Wkly. 2025;155:4359

Technical comment on: Nehme M, et al. Chatbots in medicine: certification process and applied use case

Hannah van Kolfschooten

Law Centre for Health and Life, University of Amsterdam, Amsterdam, Netherlands

The article by Nehme et al. [1] provides a comprehensive analysis of the regulatory and certification challenges faced by healthcare chatbots. Using the confIAnce chatbot as a case study, the authors explore its classification as a non-medical device under the EU Medical Device Regulation (MDR) and the Swiss Medical Devices Ordinance (MedDO). They outline the processes required for certification, emphasising the importance of defining the chatbot's scope, ensuring data protection and maintaining compliance with quality management standards. The article highlights the potential of chatbots to alleviate healthcare burdens, improve patient access to information and reduce physician workload when appropriately monitored and regulated. The authors also acknowledge the risks of misinformation and privacy breaches if safeguards are not implemented.

Building on the insights provided by Nehme et al., an additional concern is the growing reliance on generative AI systems, such as ChatGPT, in medicine. Unlike purpose-built healthcare chatbots like confIAnce, these general-purpose tools are not specifically designed for healthcare. Yet, they are increasingly used by medical professionals for tasks like summarising medical notes, drafting patient communication and exploring diagnostic options [2]. Patients also turn to these tools for medical advice or self-diagnosis [3]. Generative AI systems, however, lack the safeguards of certified medical chatbots.

First, Gen AI systems frequently generate outputs that may appear coherent but are factually incorrect, a phenomenon known as "hallucination". In a healthcare context, this could lead to serious consequences, such as incorrect self-diagnoses, inappropriate treatments or delays in seeking necessary medical attention. For example, a recent study found frequent hallucinations in medical records summarised by Gen AI systems [4]. Unlike purpose-built medical chatbots, trained on verified healthcare datasets and designed to operate within a defined scope, Gen AI tools lack such constraints, increasing the risk of misinformation.

Second, the use of Gen AI as medical chatbots raises significant data protection and privacy concerns. They often handle sensitive health-related queries without meeting stringent data protection standards. Unlike certified medical chatbots operating in secure, encrypted environments, Gen AI systems may lack such safeguards, increasing the risk of data breaches and unauthorised access [5].

Bias is another critical issue associated with Gen AI systems in healthcare. These tools, trained on extensive but often unstructured datasets, can inherit and amplify biases present in their training data [6]. Chatbots may produce recommendations that disproportionately favour certain demographic groups over others, leading to unequal access to accurate information or care. For example, ChatGPT performs relatively poorly when instructed in non-European languages, potentially limiting access to accurate information for marginalised populations [7].

While the MDR and MedDO regulate purpose-built healthcare chatbots, Gen AI systems fall outside the scope of these frameworks. Both frameworks rely on the intended purpose of a device for classification, meaning Gen AI chatbots like ChatGPT, not explicitly designed for medical use, fall outside their scope, leaving regulatory gaps. The same applies to the EU AI Act. The EU AI Act imposes strict safeguards on high-risk AI systems, such as AI systems providing medical diagnosis, mandating conformity assessments, risk management and robust oversight. However, the Act's reliance on theintended purposeof an AI system means that general-purpose AI systems (GPAI), such as ChatGPT, which are not explicitly designed for medical use, fall outside the high-risk category.

As a result, they are subject only to minimal obligations, even when they are used in practice for medical advice by professionals or patients. Under the EU AI Act, general-purpose AI systems are required to meet certain transparency and documentation standards. Developers of general-purpose AI must ensure transparency, disclose training data sources and label AI-generated content. Generative AI systems like ChatGPT must also label AI-generated content and include mechanisms to mitigate risks associated with their use. However, beyond these measures, the AI Act primarily relies on voluntary codes of practice to guide the deployment of GPAI [2]. Unlike high-risk AI systems, GPAI is not subject to external conformity assessments or robust monitoring, leaving it inadequately supervised when used for critical medical tasks. This distinction creates a regulatory gap [9].

Law Centre for Health and Life
University of Amsterdam
NL-1001 NJ Amsterdam
h.b.vankolf-schooten[at]uva.nl

In conclusion, while the regulatory focus on purpose-built healthcare chatbots is essential, the increasing reliance on generative AI systems like ChatGPT in medical contexts exposes critical gaps in regulation, including the EU AI Act and the Swiss MedDO. These tools, used increasingly by patients and professionals, require stricter oversight to mitigate risks and ensure safety. In Switzerland and beyond, policymakers should explore amendments to regulatory frameworks, such as the Swiss MedDO, the MDR and the EU AI Act, to address the unintended but significant use of general-purpose AI in healthcare. Simultaneously, medical professional bodies must take the lead in developing clinical guidelines to ensure the responsible integration of these tools into practice. Together, these efforts can address existing regulatory gaps and safeguard patient safety in the evolving role of AI in medicine.

Potential competing interests

The author has completed and submitted the International Committee of Medical Journal Editors form for disclosure of potential conflicts of interest. No potential conflict of interest related to the content of this manuscript was disclosed.

References

1. Nehme M, Schneider F, Amruthalingam E, Schnarrenberger E, Tremeaud R, Guessous I. Chatbots in medicine: certification process and applied use case. Swiss Med Wkly. 2024 Oct;154(10):3954–3954. http://dx.doi.org/10.57187/s.3954.
2. Blease CR, Locher C, Gaab J, Hägglund M, Mandl KD. Generative artificial intelligence in primary care: an online survey of UK general practitioners. BMJ Health Care Inform. 2024 Sep;31(1):e101102. http://dx.doi.org/10.1136/bmjhci-2024-101102.
3. Armbruster J, Bussmann F, Rothhaas C, Titze N, Grützner PA, Freischmidt H. "Doctor ChatGPT, Can You Help Me?" The Patient's Perspective: Cross-Sectional Study. J Med Internet Res. 2024 Oct;26:e58831. http://dx.doi.org/10.2196/58831.
4. Vishwanath PR, Tiwari S, Naik TG, Gupta S, Thai DN, Zhao W, Kwon S, Ardulov V, Tarabishy K, McCallum A, Salloum W. Faithfulness Hallucination Detection in Healthcare AI. 2024. Preprint available at https://openreview.net/forum?id=6eMIzKFOpJ&nesting=2&sort=date-desc
5. Duffourc M, Gerke S, Kollnig K. Privacy of Personal Data in the Generative AI Data Lifecycle. NYU JIPEL. 2024;13(2):219–68.
6. van Kolfschooten H, Pilottin A. Reinforcing Stereotypes in Health Care Through Artificial Intelligence–Generated Images: A Call for Regulation. Mayo Clin Proc Digit Health. 2024 Sep;2(3):335–41. http://dx.doi.org/10.1016/j.mcpdig.2024.05.004.
7. Chen WR, Adebara I, Doan KD, Liao Q, Abdul-Mageed M. Fumbling in Babel: An Investigation into ChatGPT's Language Identification Ability. 2024. arXiv Preprint at doi: http://dx.doi.org/10.48550. /arXiv.2311.09696. http://dx.doi.org/10.18653/v1/2024.findings-naacl.274.
8. Busch F, Kather JN, Johner C, Moser M, Truhn D, Adams LC, et al. Navigating the European Union Artificial Intelligence Act for Healthcare. NPJ Digit Med. 2024 Aug;7(1):210. http://dx.doi.org/10.1038/s41746-024-01213-6.
9. van Kolfschooten H, van Oirschot J. The EU Artificial Intelligence Act (2024): implications for healthcare. Health Policy. 2024 Nov;149:105152. http://dx.doi.org/10.1016/j.healthpol.2024.105152.