BJPsych | The British Journal of Psychiatry (2026)
1–2. doi: 10.1192/bjp.2026.10716

Guest Editorial

Artificial intelligence evolution in medicine

Scott Monteith, Tasha Glenn, John Richard Geddes, Eric D. Achtyes, Rita Bauer, Michael Gitlin and Michael Bauer

Summary

Recently a new type of generative artificial intelligence, agentic artificial intelligence, has been developed that extends product capabilities to act autonomously. Although agentic artificial intelligence systems offer a unique approach to supporting physicians, the products also pose many validity, privacy and security risks. Physicians need to understand the basic features of agentic artificial intelligence.

Keywords

Artificial intgelligence; agentic artificial intelligence; artificial intelligence agents; healthcare; autonomous artificial intelligence.

Copyright and usage

© The Author(s), 2026. Published by Cambridge University Press on behalf of Royal College of Psychiatrists.

Artificial intelligence is a transformative technology included in the range of applications found in everyday life that are routinely used by the general public, as well as in products designed for physicians. In medicine, applications include artificial intelligence decision support tools, wearables and monitoring devices for physicians, patients and caregivers. Products that incorporate artificial intelligence are usually based on large language models (LLMs) such as ChatGPT from OpenAI (San Francisco, California, USA; https://chatgpt.com), Gemini from Google (Mountain View, California, USA; https://gemini.google.com) and Claude from Anthropic (Mountain View, California, USA; https://claude.com), including most online self-help applications available on the market today. A new type of generative artificial intelligence is agentic artificial intelligence, which extends the capabilities of generative artificial intelligence by making decisions and acting automatically in a human manner based on perception and reasoning.[1] Agentic artificial intelligence is autonomous, can specialise in specific tasks, can adapt and learn from experience and can respond to natural language prompts.[2] Agentic artificial intelligence can proactively initiate and reconfigure processes based on changing conditions. There has been a recent expansion of agentic artificial intelligence agents embedded in medical products. The purpose of this paper is to describe how medical products using artificial intelligence are evolving with autonomous agentic artificial intelligence agents.

Agentic artificial intelligence agents

Although there is no standardised definition, agentic artificial intelligence agents typically use LLMs to perform a wide range of tasks and actions, including decision-making, problem-solving and interacting with the product environment. Although artificial intelligence agents act independently, their actions are based on the predefined rules and goals defined by humans during training, and by the user who provides the specific goals and available tools.[3] For example, an agentic artificial intelligence agent will automatically ask questions of a user, look up the responses internally and determine whether it can respond or whether the question needs to be passed to a human. Multiple types of agentic artificial intelligence agents are used commercially. Some agentic artificial intelligence agents are simple reflex agents that respond identically based on predefined rules. There are also multiple types of model-based agentic artificial intelligence agents that are designed to achieve specific goals, to use algorithms based on past experiences or to optimise responses. One example of an agentic agent released by Microsoft adds automatic updates to correct or enhance Word, Excel and PowerPoint documents as the user enters data.[4]

Agentic artificial intelligence in healthcare

There are many potential uses for agentic artificial intelligence in healthcare, including both physician- and patient-facing applications. However, the need for patient safety and privacy, the potential for serious errors and the tight regulatory environment pose major and unique challenges that, to date, have limited the adoption of agentic artificial intelligence in healthcare.[5] Expansion of the use of agentic artificial intelligence in patient care will require ongoing research and testing. Unlike general-purpose artificial intelligence applications that interact with users, agentic artificial intelligence will need to be carefully and repeatedly validated, and safely integrated within existing healthcare systems. It is important that the physician remains 'in the loop' overseeing the agentic training, process implementation and outcomes. The need for rigorous oversight and validation includes the use of agentic artificial intelligence in medical situations that are currently automated with LLMs, such as laboratory medicine.[6] Additionally, both organisational and project-level steps and guardrails must be in place before the implementation of agentic artificial intelligence in clinical settings. Agentic artificial intelligence can also be used to provide administrative support. For example, an agentic product may connect with the electronic health record to provide services such as patient verification, scheduling, documentation and prior authorisation processes.[7,8] Agentic artificial intelligence is also being used in medical education to simulate patient encounters.

It is important to recognise the challenges related to implementing agentic artificial intelligence systems, which have the same limitations, risks, biases and privacy and cybersecurity concerns as standard artificial intelligence algorithms. Some of the critical challenges regarding agentic artificial intelligence in healthcare include obtaining high-quality, representative data for training the model while preventing bias. Agentic artificial intelligence systems may introduce a variety of security risks, which may be magnified in poorly designed systems.[2,9] Successful implementation will require the challenging process of implementing agentic artificial intelligence into the interdisciplinary clinical workflow. Physician oversight and involvement are required for successful agentic artificial intelligence implementation, which would require physician training and commitment. Organisations need to determine

https://doi.org/10.1192/bjp.2026.10716 Published online by Cambridge University Press

who will be responsible for identifying when agentic artificial intelligence makes an error or responds inconsistently. There is an ongoing need for interdisciplinary cooperation between technology developers and experienced physicians. Ethical and regulatory standards regarding agentic artificial intelligence are needed, and may change over time as legal frameworks are established. Considerable real-world research including patients and real-life workflows will be required to best understand how to implement agentic artificial intelligence. Agentic artificial intelligence systems offer a unique approach to supporting physicians in dealing with the challenges of clinical medicine but also pose validity, privacy, malpractice and security risks. With the expansion of agentic artificial intelligence agents throughout healthcare, physicians need to understand its basic features. Increasingly, physicians will be working in environments that include agentic artificial intelligence models that may be acting autonomously.

Scott Monteith, Department of Psychiatry, Michigan State University College of Human Medicine, USA; **Tasha Glenn**, ChronoRecord Association, Fullerton, California, USA; **John Richard Geddes**, Department of Psychiatry, University of Oxford, UK; **Eric D. Achtyes**, Department of Psychiatry, Western Michigan University Homer Stryker M.D. School of Medicine, Kalamazoo, Michigan, USA; **Rita Bauer**, Department of Psychiatry and Psychotherapy, University Hospital Carl Gustav Carus, Dresden, Germany; **Michael Gitlin**, Department of Psychiatry, University of California Los Angeles (UCLA), USA; **Michael Bauer**, Department of Psychiatry, University Hospital Carl Gustav Carus, Technische Universitat Dresden, Germany

Correspondence: Scott Monteith. Email: monteit2@msu.edu

First received 4 May 2026 UTC, final revision 4 May 2026 UTC, accepted 24 May 2026 UTC

Author contributions

S.M. and T.G. wrote the initial draft. All authors reviewed and approved the final manuscript.

Funding

This research received no specific grant from any funding agency, commercial or not-for-profit sectors.

Declaration of interest

J.R.G. is a member of the *BJPsych* editorial board but did not take part in the review or decision-making process of this paper. The other authors declare no potential conflicts of interest.

References

1 Stackpole B. *Agentic AI, Explained*. MIT, 2026 (https://mitsloan.mit.edu/ideas-made-to-matter/agentic-ai-explained).

2 Stryker C. *What is Agentic AI?* IBM, 2025 (https://www.ibm.com/think/topics/agentic-ai).

3 Gutowska A. *What Are AI Agents?* IBM, 2026 (https://www.ibm.com/think/topics/ai-agents).

4 Chauhan S. *Copilot's Agentic Capabilities in Word, Excel, and PowerPoint Are Generally Available*. Microsoft, 2026 (https://www.microsoft.com/en-us/microsoft-365/blog/2026/04/22/copilots-agentic-capabilities-in-word-excel-and-powerpoint-are-generally-available/).

5 Xu G, Li X, Chen Y, Duan Y, Wu S, Yu A, et al. *A Comprehensive Survey of Agentic AI in Healthcare*. Authorea Preprints, 2025.

6 Gruson D, Gouget B, Lee W, Greaves R, Liu Y, Ebert S, et al. From automation to agentic artificial intelligence in laboratory medicine: an opinion of the IFCC Division on Emerging Technologies. *Clin Chem Lab Med (CCLM)* 2025; **64**: 985–8.

7 Amazon. *AWS Launches Amazon Connect Health to Reduce Administrative Burden in Health Care*. Amazon, 2026 (https://www.aboutamazon.com/news/aws/amazon-connect-health-ai-healthcare).

8 Rengasamy B. Agentic artificial intelligence for prior authorization workflows in healthcare. *J Comp Sci Technol Stud* 2025; **7**: 108–19.

9 Hassan N. *Security Risks in Agentic AI Systems and How to Evaluate Threats*. TechTarget, 2025 (https://www.techtarget.com/searchenterpriseai/feature/Security-risks-in-agentic-AI-systems-and-how-to-evaluate-threats).

https://doi.org/10.1192/bjp.2026.10716 Published online by Cambridge University Press