# Agentic AI reshapes healthcare, but governance must keep pace



Agentic AI is emerging as a transformative force in healthcare, enabling digital agents to perform complex, multi-step tasks autonomously. These systems go beyond traditional AI by acting as digital workers—handling clinical note summarisation, document review, staff coaching, scheduling and even recruitment. Centria Health, for example, has used agentic AI to streamline the hiring of Applied Behavioural Analysis technicians, cutting costs and improving access to care for children with autism. As adoption expands from large hospitals to smaller medical groups, agentic AI is poised to become central to healthcare operations.

Yet the integration of agentic AI brings sharp governance challenges. Healthcare data is highly sensitive and subject to strict regulation under laws such as HIPAA in the US and the EU AI Act. The autonomous nature of agentic systems heightens privacy risks, as they process large volumes of patient data across functions with limited human oversight. This requires tailored security frameworks with strong encryption, anonymisation, and strict access controls.

Bias is another major concern. AI models trained on incomplete or skewed data can reinforce disparities in patient care or hiring. Because agentic systems evolve over time, these biases may not be immediately visible. Continuous bias audits and monitoring are essential to maintain fairness and trust.

Transparency and explainability are equally critical. Given their internal complexity, agentic AI systems must provide clinicians and administrators with tools to understand decision-making processes. Audit trails and explainability methods like LIME and SHAP help ensure AI outputs are interpretable and challengeable.

Human oversight remains a cornerstone of responsible deployment. AI can reduce workloads, but final accountability rests with healthcare professionals. Verification of AI outputs through human review is key to aligning with legal and ethical standards.

The regulatory environment is tightening. Alongside HIPAA, new AI-specific rules are emerging across jurisdictions. The EU AI Act emphasises transparency, human control and data quality, with fines for breaches potentially reaching a percentage of global turnover. Risk assessments and compliance reviews must be ongoing.

Best practice begins with cross-functional governance frameworks involving clinical, IT, legal and compliance teams. These should establish data quality standards, privacy protections, transparency protocols and oversight mechanisms tailored to healthcare. Ethical impact assessments—guided by frameworks such as NIST’s AI Risk Management Framework—help identify and mitigate risks throughout the AI lifecycle.

Privacy by design is vital. This includes encryption at rest and in transit, role-based access controls, data minimisation and continuous monitoring of AI logs for anomalies. Real-time dashboards showing AI health scores, alerts and audit trails support safe deployment and rapid response.

Training across clinical, administrative and technical teams ensures understanding of AI capabilities and limitations. Staff feedback channels and error reporting mechanisms support continuous improvement. Agentic AI is already delivering measurable benefits. AI-powered phone agents ease front-line staff burdens, while automation streamlines clinical documentation and resource scheduling. Compliance monitoring systems can detect procedural deviations before they escalate.

Executive leadership must drive governance forward. Viewing AI oversight as a strategic priority rather than a technical detail ensures accountability, protects patient trust and preserves institutional reputation.

The UK’s ambition to lead in responsible AI innovation can be realised by embedding rigorous governance at the heart of health systems. With principled oversight, agentic AI can safely enhance healthcare delivery—offering better outcomes for patients while maintaining the highest ethical and regulatory standards.

Created by [Amplify](https://www.hbmadvisory.com/amplify): AI-augmented, human-curated content.

## Bibliography

1. <https://www.simbo.ai/blog/challenges-and-best-practices-for-governance-transparency-and-maintaining-accountability-in-enterprise-grade-agentic-ai-deployments-in-medical-institutions-1249754/> - Please view link - unable to able to access data
2. <https://www.simbo.ai/blog/challenges-and-best-practices-for-governance-transparency-and-maintaining-accountability-in-enterprise-grade-agentic-ai-deployments-in-medical-institutions-1249754/> - This article discusses the challenges and best practices for governance, transparency, and accountability in deploying agentic AI systems within medical institutions. It highlights the importance of maintaining data privacy and security, mitigating bias, ensuring transparency and explainability, establishing accountability and human oversight, and navigating the evolving regulatory environment. The article also provides best practices for AI deployment, including establishing comprehensive AI governance frameworks, implementing continuous risk and ethical impact assessments, adopting transparency and explainability tools, designing privacy and security protections by default, incorporating human-in-the-loop controls, and investing in training and cross-functional collaboration.
3. <https://www.simbo.ai/blog/challenges-and-governance-in-implementing-agentic-ai-solutions-in-healthcare-ensuring-safety-and-compliance-3102555/> - This article examines the challenges in implementing agentic AI solutions in healthcare, focusing on safety and compliance risks. It discusses the importance of adhering to strict laws like HIPAA to protect patient data, the risks associated with AI systems learning from biased data, and the need for transparency and explainability in AI decision-making. The article also addresses the necessity of human oversight in AI systems and the challenges of integrating AI with existing healthcare infrastructures.
4. <https://www.ibm.com/think/insights/ai-agent-governance> - This article from IBM explores the challenges and opportunities in AI agent governance. It discusses issues such as bias in AI systems, security and compliance risks, and the complexities of managing autonomous AI agents. The article emphasizes the need for robust governance frameworks to ensure the safe and ethical deployment of AI agents in various sectors, including healthcare.
5. <https://pmc.ncbi.nlm.nih.gov/articles/PMC12092461/> - This article discusses the vision for adaptive, efficient, and ethical healthcare through the use of AI with agency. It highlights the potential of AI to transform healthcare by improving operational efficiency and patient care. The article also addresses the challenges of integrating AI into healthcare, including ethical concerns around patient privacy, data security, and the need for compliance with regulations like HIPAA and GDPR.
6. <https://www.forbes.com/councils/forbestechcouncil/2025/01/15/protecting-patient-care-in-the-age-of-algorithms-an-ai-governance-model-for-healthcare/> - This Forbes article discusses the unique risks associated with AI in healthcare and the need for structured governance approaches to ensure safe, secure, and ethical AI adoption. It emphasizes the importance of protecting patient safety, minimizing ethical concerns, and establishing clear accountability in the deployment of AI systems in healthcare settings.
7. <https://telehealthandmedicinetoday.com/index.php/journal/article/view/521> - This article presents a discussion on AI governance in healthcare, focusing on best practices, solutions, and unresolved issues. It covers topics such as the challenges of AI adoption in healthcare, the role of AI governance in managing opportunities and risks, and the importance of responsible evaluation and deployment of new technology in the healthcare sector.