

Autonome KI-Agenten im Gesundheitswesen

Dresdner Forschende präsentieren Lösungen für sichere Zulassung von KI in der Medizin

Die Einsatzmöglichkeiten für Künstliche Intelligenz (KI) im Gesundheitswesen entwickeln sich rasant weiter. Autonome KI-Agenten haben großes Potenzial, die medizinische Versorgung grundlegend zu verändern und gewinnen deshalb zunehmend an Aufmerksamkeit. Forschende am Else Kröner Fresenius Zentrum (EKFZ) für Digitale Gesundheit an der Technischen Universität Dresden (TUD) weisen auf eine wachsende Diskrepanz zwischen den Fähigkeiten autonomer KI-Agenten und den bestehenden regulatorischen Rahmenbedingungen für Medizinprodukte in den USA und Europa hin. In ihrer Publikation schlagen sie deshalb innovative Regulierungsansätze vor, um diese Lücke zu schließen und gleichzeitig die Patientensicherheit zu gewährleisten. Der Artikel wurde in der Fachzeitschrift Nature Medicine veröffentlicht.

Von Assistenzsystemen zu autonomen Agenten

Der Einsatz von großen Sprachmodellen (Large Language Models, LLMs) und anderen Formen generativer KI (GenAI) im Gesundheitswesen hat in den letzten Jahren stark zugenommen. Durch ihren medizinischen Zweck gelten sie oft als Medizinprodukte und müssen spezifische Gesetze und regulatorische Vorgaben erfüllen. Aktuelle Entscheidungen zeigen, dass solche Systeme mit eng definierten Aufgaben prinzipiell zulassungsfähig sind. Die nächste Generation von KI-Systemen sind allerdings breit angelegte autonome KI-Agenten, die entwickelt werden, um komplexe, zielgerichtete Arbeitsabläufe eigenständig auszuführen. Sie haben großes Potenzial, um mittels KI die medizinische Versorgung in Zukunft zu unterstützen und weiter zu verbessern. KI-Agenten bestehen aus mehreren miteinander vernetzten Komponenten, darunter externe Datenbanken und computergestützte Werkzeuge für Bildanalyse, Notizen, klinische Leitlinien und das Management patientenbezogener Daten. Diese Komponenten werden von LLMs gesteuert, die Entscheidungsfindung, Fehlerbehandlung und die Erkennung von abgeschlossenen Aufgaben übernehmen.

„Wir erleben einen grundlegenden Wandel darin, wie KI-Tools in der Medizin eingesetzt werden können“, sagt Jakob N. Kather, Professor für Clinical Artificial Intelligence am EKFZ für Digitale Gesundheit der TUD und Onkologe am Universitätsklinikum Dresden. „Im Gegensatz zu früheren Systemen sind KI-Agenten in der Lage, komplexe klinische Arbeitsabläufe selbstständig durchzuführen. Das eröffnet große Chancen für die Medizin – wirft aber auch ganz neue Fragen zu Sicherheit, Verantwortlichkeit und Regulierung auf, die wir adressieren müssen“, ergänzt er.

KI-Agenten stellen bestehende Regulierungen vor Herausforderungen

Die aktuellen Vorschriften für Medizinprodukte wurden für statische, eng definierte Technologien entwickelt, die unter menschlicher Aufsicht stehen und sich nach Markteinführung nicht mehr weiterentwickeln. Im Gegensatz dazu weisen neue autonome und breit anwendbare Technologien grundlegend andere Eigenschaften auf. Sie verfügen über eine deutlich höhere Autonomie, Anpassungsfähigkeit und Einsatzbreite als bisherige KI-Technologien. Da sie komplexe Arbeitsabläufe selbstständig ausführen können, stellen sie Regulierungsbehörden und Entwickler vor große Herausforderungen.

„Um die sichere und effektive Einführung autonomer KI-Agenten im Gesundheitswesen zu

ermöglichen, müssen sich regulatorische Rahmenbedingungen weiterentwickeln – weg von statischen Paradigmen. Wir benötigen eine anpassungsfähige regulatorische Aufsicht und flexible, alternative Zulassungswege“, sagt Oscar Freyer, Erstautor der Publikation und wissenschaftlicher Mitarbeiter im Team von Professor Stephen Gilbert, Leiter der Gruppe Medical Device Regulatory Science am EKFZ für Digitale Gesundheit der TUD.

Regulierung neu denken: Zulassungswege für sichere und innovative KI-Technologien

Da die Fähigkeiten autonomer KI-Agenten den Rahmen aktueller Vorschriften überschreiten, schlagen die Forschenden verschiedene Lösungsansätze vor, um bestehende Hürden für deren praktischen Einsatz zu überwinden.

Kurzfristige Anpassungen könnten die Ausweitung von „Enforcement Discretion“-Regelungen umfassen, bei denen Behörden anerkennen, dass ein Produkt ein Medizinprodukt ist, aber auf die Durchsetzung bestimmter Anforderungen verzichten. Alternativ könnte eine Nicht-Medizinprodukt-Klassifizierung für Systeme angewandt werden, die zwar einen medizinischen Zweck erfüllen, aber außerhalb der traditionellen Medizinprodukteverordnung liegen.

Mittelfristig könnten freiwillige alternative Zulassungswege (Voluntary Alternative Pathways, VAPs) und adaptive regulatorische Rahmen die bestehenden Zulassungsverfahren ergänzen. Adaptive Wege lenken die Regulierung von statischer Vorabzulassung hin zu dynamischer Überwachung durch reale Leistungsdaten, Zusammenarbeit mit Stakeholdern und fortlaufende Anpassungen. Bei Auffälligkeiten oder Fehlverhalten könnten die Produkte in bestehende, konventionelle Verfahren überführt werden.

Darüber hinaus diskutieren die Forschenden auch langfristige Lösungsansätze, etwa eine Regulierung von KI-Agenten analog zur Qualifizierung von Mediziner:innen. In diesem Modell würde die Zulassung über strukturierte Trainingsprozesse erfolgen, bei denen die Systeme erst nach Nachweis sicherer und effektiver Leistung mehr Autonomie erhalten.

Die Forschenden stellen zudem fest, dass Instrumente wie Reallabore (Regulatory Sandboxes) zwar eine gewisse Flexibilität zum Testen neuer Technologien bieten, jedoch aufgrund des hohen Bedarfs an Ressourcen und Aufwandes für Regulierungsbehörden keine skalierbare Lösung für den breiten Einsatz darstellen.

In ihrem Artikel argumentieren die Forschenden, dass die Einführung autonomer KI-Agenten im Gesundheitswesen mittelfristig ohne umfassende regulatorische Reformen wahrscheinlich nicht möglich sein wird. Besonders freiwillige alternative Zulassungswege (VAPs) und adaptive regulatorische Ansätze werden als die wirksamsten und realistischsten Strategien hervorgehoben, um dieses Ziel zu erreichen. Sie betonen die Notwendigkeit einer engen Zusammenarbeit zwischen Regulierungsbehörden, Gesundheitsdienstleistern und Technologieentwicklern, um Rahmenbedingungen zu schaffen, die den besonderen Anforderungen autonomer KI-Agenten gerecht werden und zugleich die Patientensicherheit gewährleisten.

„Um das volle Potenzial autonomer KI-Agenten im Gesundheitswesen zu realisieren, sind mutige und zukunftsorientierte Reformen nötig“, sagt Stephen Gilbert, Professor für Medical Device Regulatory Science am EKFZ für Digitale Gesundheit der TU Dresden und Letztautor der Publikation. „Die Regulierungsbehörden müssen jetzt mit den Vorbereitungen beginnen, um in Zukunft die Patientensicherheit zu gewährleisten und klare Bedingungen zu schaffen, die sichere Innovationen ermöglichen“, fügt er hinzu.

Else Kröner Fresenius Zentrum (EKFZ) für Digitale Gesundheit:

Das EKFZ für Digitale Gesundheit an der TU Dresden und dem Universitätsklinikum Carl Gustav

Carus Dresden wurde im September 2019 gegründet. Es wird mit einer Fördersumme von 40 Millionen Euro für eine Laufzeit von zehn Jahren von der Else Kröner-Fresenius-Stiftung gefördert. Das Zentrum konzentriert seine Forschungsaktivitäten auf innovative, medizinische und digitale Technologien an der direkten Schnittstelle zu den Patientinnen und Patienten. Das Ziel ist dabei, das Potenzial der Digitalisierung in der Medizin voll auszuschöpfen, um die Gesundheitsversorgung, die medizinische Forschung und die klinische Praxis nachhaltig zu verbessern.

Originalpublikation:

Oscar Freyer, Sanddhya Jayabalan, Jakob N. Kather, and Stephen Gilbert: Overcoming Regulatory Barriers to the Implementation of AI Agents in Healthcare, Nature Medicine, 2025.

Link: <https://www.nature.com/articles/s41591-025-03841-1>

DOI: 10.1038/s41591-025-03841-1