

Auch die Statusübergänge (Erstellung, Einlösung, Löschung von Rezepten) kann der Versicherte nachvollziehen. Die auf dem Fachdienst E-Rezept gespeicherten Daten werden 100 Tage nach dem Einlösen des Rezeptes automatisch gelöscht. Ein auf dem Fachdienst E-Rezept übertragenes Rezept kann der Arzt nicht mehr verändern. Er kann es lediglich löschen und ggf. neu ausstellen, solange es noch nicht eingelöst wurde. Wurde ein Rezept durch eine Apotheke dispensiert, ist es für eine weitere Nutzung gesperrt.

B/18.5 Künstliche Intelligenz

Das Thema Künstliche Intelligenz (KI) hat spätestens seit Anfang des Jahres 2023 rasant an Fahrt aufgenommen. Einen ersten deutlichen Sprung auch für Endbenutzer schaffte das US-amerikanische Unternehmen OpenAI mit seinem textbasierten Large-Language-Modell, das als Chatbot ChatGPT nutzbar gemacht wurde.

Mittlerweile arbeitet OpenAI eng mit Microsoft zusammen und viele Funktionen der Künstlichen Intelligenz stehen nicht mehr nur über Chateingaben zur Verfügung, sondern werden immer stärker auch direkt mit den Office-Anwendungen von Microsoft verbunden – dies geschieht derzeit unter dem Namen Copilot und insbesondere in den cloudbasierten Microsoft-365-Produkten.

Neben OpenAI sind aber auch andere große Tech-Unternehmen dazu übergegangen, Anwendungen, die Künstliche Intelligenz nutzen, anzubieten. Google bzw. Alphabet entwickeln unter dem Namen Bard ihre eigene KI-Anwendung. Und auch viele Produkte, die bisher als Software as a Service (SaaS) genutzt worden sind, weisen quasi über Nacht KI-Funktionalitäten auf, so zum Beispiel viele Anwendungen zur Bildgestaltung und -bearbeitung von Adobe.

Darüber hinaus kommen mittlerweile vielzählige KI-Anwendungen als Einzelanwendungen auf den Markt und Bereiche, in denen vorher kaum an eine Nutzung zu denken war, öffnen sich. Neben den bereits angesprochenen ChatBots, die zur Texterstellung, Recherche, Datenauswertung und zur Unterstützung von Programmierfähigkeiten etc. genutzt werden können, gibt es derzeit unter anderem alleine für Texteingaben vielzählige Möglichkeiten, die hier nur einmal grob und beispielhaft dargestellt werden sollen:

- Text zu Text
- Text zu Sprache
- Text zu Bild

- Text zu Video
- Text zu 3D-Modell

Neben den bisher bereits im Gesundheitswesen zu findenden Anwendungen zur KI-unterstützten Bilddiagnostik eröffnen sich durch die neuen Möglichkeiten ggf. auch in ganz anderen Bereiche Bedarfe, etwa:

- KI-Werkzeuge für die Unterstützung der Verwaltungsaufgaben unter Verwendung der bisherigen Office-Anwendungen
- Internetrecherche
- Auswertung von Datensätzen
- Live-Übersetzungsdienste für die Kommunikation mit Patienten
- Kreativwerkzeuge für die Marketingabteilung
- Diagnose- und Behandlungsempfehlungen und vieles mehr

Gesundheitseinrichtungen sollten sich mit dem Thema Künstliche Intelligenz gleich auf mehreren Ebenen beschäftigen und neben den datenschutzrechtlichen Fragen, die mit dem Einsatz entsprechender Werkzeuge einhergehen, auch im Bereich der technischen und organisatorischen Maßnahmen über neue Gefährdungen nachdenken.

Tatsächlich ist es, sofern personenbezogene Daten betroffen sein können, empfehlenswert, die Nutzung von KI-Anwendungen innerhalb der Gesundheitseinrichtung über eine verbindliche Richtlinie zu regeln. Den Beschäftigten sollte die Nutzung von KI-Anwendungen im Grundsatz verboten werden, außer dass diese von der Einrichtungsleitung ausdrücklich erlaubt sind. Dies schließt Dienste wie zum Beispiel die Online-Übersetzungstools zur Übersetzung von Dokumenten, Online-Bildbearbeitungsprogramme zur Bearbeitung von Personenabbildungen, personenbezogene Internetrecherchen und „Gespräche“ mit KI-Chatbots ein.

Die Gesundheitseinrichtung behält auf diese Weise die Kontrolle darüber, welche Daten von den entsprechenden Anwendungen genutzt werden, und kann prüfen, ob der Einsatz bestimmter Tools zweck- und rechtmäßig erscheint.

Darüber hinaus sollte die Gesundheitseinrichtung aber auch Sensibilisierungsmaßnahmen vorsehen, die vor Social-Engineering-Angriffen unter Verwendung von Künstlicher Intelligenz schützen. Hier können zum Beispiel Fälle aufgenommen werden, die in der Vergangenheit bereits für Schlagzeilen sorgten:

- Ein Anrufer gibt vor, der Leitung der Gesundheitseinrichtung anzugehören, und spricht tatsächlich mit der bekannten Stimme der Führungsperson. In Wirklichkeit handelt es sich aber um einen Angreifer, der versucht, Informationen mittels Social Engineering zu erbeuten bzw. die Zielperson dazu zu bringen, Geld zu transferieren. Hierbei nutzt der Angreifer ein KI-Tool, welches es erlaubt, die Stimme in Echtzeit so zu verändern, dass sie klingt wie die Stimme der Führungsperson. Für ein solches Anlernen der Künstlichen Intelligenz war es lediglich erforderlich, öffentlich verfügbare Aufnahmen der Führungsperson zum Training zu verwenden – also zum Beispiel Fernsehinterviews, Radiointerviews, Podcastauftritte oder ein YouTube-Video der letzten Rede.
- Noch erschreckender – aber ebenfalls bereits in der Praxis vorgekommen und eigentlich der gleichen Struktur folgend – sind Angriffe, bei denen nicht nur die Stimme, sondern gleich die bewegte Abbildung der Person in Videos übernommen wird. Die Person, die man glaubt während der Videokonferenz auf dem Bildschirm zu sehen, ist dabei in Wahrheit das veränderte Bild einer ganz anderen Person.

Gesundheitseinrichtungen sollten sich daher zuerst über diese beiden Punkte Gedanken machen:

- Erstellung einer Richtlinie zur geregelten Nutzung von KI-Anwendungen (Verbot mit Erlaubnisvorbehalt/Whitelist),
- Planung einer entsprechenden Awareness-Maßnahme, die den neuen Gefährdungen gerecht wird.

Darüber hinaus gilt es dann, die Anwendungen zu bewerten, die die Gesundheitseinrichtung gerne nutzen und ggf. sogar auf die Whitelist setzen möchte. Sofern nicht ausgeschlossen ist, dass personenbezogene Daten von der Anwendung erfasst werden, sind an dieser Stelle viele datenschutzrechtlich relevante Punkte zu beachten und der Datenschutzbeauftragte der Gesundheitseinrichtung ist möglichst frühzeitig zu beteiligen.

Grundsätzlich stellen sich im Zusammenhang mit den rechtlichen Rahmenbedingungen des Einsatzes von Künstlicher Intelligenz noch sehr viele Fragen, zum Beispiel aus dem Bereich Urheberrecht und ggf. in Zukunft auch im Hinblick auf eine etwaige Kennzeichnungspflicht von KI-generierten Inhalten bis hin zu bestimmten Anwendungsverböten, zum Beispiel im Bereich der biometrischen Identifizierung. Hier sind insbesondere auf EU-Ebene künftig neue

Vorgaben zu beachten, die Einrichtungen, die KI-Anwendungen nutzen, im Blick behalten sollten (z. B. die sogenannte KI-Verordnung der EU).

Auch datenschutzrechtlich stellen sich viele Anforderungen, die möglicherweise in Zukunft noch weiter spezifiziert werden. Im Grundsatz sind aber schon einige Mindestanforderungen deutlich, die beachtet werden müssen. Dabei stellen sich in der Praxis gelegentlich unerwartete Probleme. Im Folgenden soll anhand dieser kurz auf die Rahmenbedingungen eingegangen werden:

Vertrag zur Auftragsverarbeitung

Die meisten KI-basierten Anwendungen werden nicht von der Gesundheitseinrichtung selbst betrieben, sondern von Dienstleistern, die diese Anwendungen meist als Software as a Service bereitstellen. Die Bereitstellung einer solchen Anwendung durch Dienstleister wird in der Regel als Auftragsverarbeitung zu bewerten sein. In der Folge müssen Gesundheitseinrichtungen mit dem Anbieter der KI-Anwendung einen Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO schließen. Sofern Daten betroffen sind, die dem Berufsgeheimnis unterliegen, müssen zudem die Anforderungen des § 203 StGB eingehalten und der Dienstleister unter anderem als „mitwirkende Person“ zur besonderen Geheimhaltung verpflichtet werden.

Bereits an dieser Stelle entstehen in der Praxis Probleme. Insbesondere die Lizenzbedingungen der derzeit größten Anbieter (OpenAI und Microsoft) weisen bei genauer Betrachtung Unterschiede auf. So gibt es (Stand Februar 2024) nicht nur eine Version des Microsoft Copilot, sondern gleich mehrere Lizenzmodelle. Für Copilot, Copilot Pro und sogar für Microsoft Copilot with commercial data protection stehen keine Verträge zur Auftragsverarbeitung zur Verfügung. Teilweise sieht sich Microsoft sogar als die für die Datenverarbeitung verantwortliche Stelle an. Erst die zu Microsoft 365 separat erhältlichen kostenpflichtigen Lizenzen, die Unternehmen vorbehalten sind, werden mit Verträgen zur Auftragsverarbeitung hinterlegt. Unabhängig vom Anbieter müssen die Lizenzen also sehr genau geprüft werden, insbesondere:

- Wird überhaupt ein Vertrag zur Auftragsverarbeitung angeboten und ist die konkrete Lizenz von diesem umfasst?
- Ist die Nutzung der Daten zu Trainingszwecken ausdrücklich ausgeschlossen?