

Datenschutz und Sicherheit beim Einsatz von KI in der Arztpraxis

Teilnehmer-Handout | KI in der Arztpraxis, Modul 3 | Webinar am 6. Oktober 2026

Dr. med. Christian Mauch, Facharzt für Orthopädie und Unfallchirurgie, Maybach Medical MVZ Stuttgart. Maybach Medical Akademie. Anerkannt von der Landesärztekammer Baden-Württemberg mit 2 CME-Punkten der Kategorie A.

Interessenkonflikt: Dr. med. Christian Mauch ist Gründer der SummitGO GmbH & Co. KG. SummitGO wird im Vortrag als offengelegtes Architekturbeispiel gezeigt. Keine finanziellen Beziehungen zu OpenAI, Anthropic oder Google.

Worum es in diesem Modul geht

Jede Anfrage an ein Sprachmodell ist eine Datenübermittlung. Wer einen Befund in ein Chatfenster kopiert, gibt ihn an ein Unternehmen weiter, dessen Server, Vertragswerk und Rechtsordnung die Praxis meist nicht kennt. Modul 3 klärt, welche Regeln dabei greifen, wie sie zusammenhängen und welche Nachweise eine Praxis von ihrem Anbieter verlangen sollte. Es geht um den rechtlichen Rahmen in der Breite, den eine Arztpraxis kennen muss, und um die wenigen Prüfschritte, die im Alltag tatsächlich anfallen.

Das Handout begleitet den Vortrag vom 6. Oktober 2026. Es wiederholt die Folien nicht, es ordnet sie ein und liefert die Belege. Die Folienangaben in Klammern beziehen sich auf das Deck mit 42 Folien. Eine Rechtsberatung im Einzelfall ersetzt der Text nicht.

Was beim Eintippen geschieht

Der Weg ist kurz. Die Ärztin tippt oder diktiert, der Text geht an die Server des Anbieters, das Modell rechnet eine Antwort, die Antwort kommt zurück (Folie 6). Was in diesen Sekunden mit den Daten geschieht, regeln die Nutzungsbedingungen. Bei Verbraucherkonten der großen Chat-Assistenten dienen Eingaben in der Grundeinstellung der Verbesserung des Modells. Wer das nicht will, muss selbst widersprechen. Gespeicherte Chats bleiben bis zur Löschung erhalten, gelöschte und temporäre Chats noch bis zu 30 Tage. Mitarbeiter des Anbieters können Inhalte in begrenztem Umfang einsehen, etwa zur Missbrauchskontrolle.

Der entscheidende Punkt für die Praxis ist das Fehlen eines Vertrags. Verbraucherkonten kommen in der Regel ohne Auftragsverarbeitungsvertrag. Damit fehlt die Grundlage, auf der eine Praxis Patientendaten an einen Dienstleister geben darf. Geschäftskonten und Programmierschnittstellen derselben Anbieter sehen andere Bedingungen vor, oft mit Vertrag, ohne Training und mit kurzen Löschfristen. Die Bezeichnung des Werkzeugs sagt darüber nichts. Es kommt auf den Vertrag an, der hinter dem Konto steht.

Wichtig

Patientendaten gehören nicht in ein privates oder kostenloses KI-Konto. Für Versuche mit Verbraucherkonten genügen erfundene Fälle. Wer echte Daten verarbeiten will, braucht ein Geschäftskonto mit Auftragsverarbeitungsvertrag und einer Verpflichtung nach § 203 StGB.

Die Lage in den Praxen

Drei Erhebungen beschreiben die Ausgangslage (Folie 7). Im Doctolib Digital Health Report 2026 mit 414 befragten Ärzten und in der Umfrage von Bitkom und Hartmannbund 2025 mit 616 Ärzten nennen je nach Frage 54 bis 72 Prozent den Datenschutz als größte Sorge beim Einsatz von KI. Rund die Hälfte der Befragten arbeitet dennoch mit Werkzeugen, die niemand in der Praxis geprüft hat. Die Sorge ändert das Verhalten also nicht, solange keine geprüfte Alternative bereitsteht.

Der Bitkom Cloud Report vom Juni 2026 ergänzt das Bild aus der Gesamtwirtschaft. 85 Prozent der 603 befragten Unternehmen halten Deutschland für zu abhängig von US-Anbietern, ein Jahr zuvor waren es 78 Prozent. 37 Prozent würden Nachteile hinnehmen, wenn ihre Daten ausschließlich in Deutschland verarbeitet werden, nach 27 Prozent im Vorjahr. Diese Zahlen stammen aus allen Branchen und lassen sich auf Arztpraxen nur als Stimmungsbild übertragen.

Drei Einschränkungen gehören zu diesen Zahlen. Es handelt sich um Befragungen mit Selbstauskunft, die Antwortenden wählen sich selbst aus, und eine der drei Erhebungen stammt von einem Anbieter digitaler Praxisdienste. Keine Studie fragt Ärzte direkt, ob sie ihre KI lieber in der Cloud oder auf einem Rechner in der Praxis betreiben wollen (Folie 8). Aus Gesprächen mit Kollegen ergibt sich die Neigung, keinen zusätzlichen Server ins Haus zu stellen. Gemessen hat das niemand.

Drei Rechtsräume, fünf Regelwerke

Wer in der Praxis KI mit Patientendaten nutzt, bewegt sich gleichzeitig in drei Rechtsräumen (Folie 19). Das EU-Recht bringt die Datenschutz-Grundverordnung und die KI-Verordnung mit. Das deutsche Strafrecht schützt mit § 203 StGB das Patientengeheimnis. Das US-Recht wirkt über den CLOUD Act und Section 702 des Foreign Intelligence Surveillance Act auf jeden Anbieter mit US-Bezug. Keines dieser Regelwerke verdrängt ein anderes. Die Praxis muss alle fünf zugleich bedienen.

Datenschutz-Grundverordnung

Die DSGVO gilt seit Mai 2018 und schützt alle personenbezogenen Daten. Gesundheitsdaten zählen nach Art. 9 zu den besonderen Kategorien mit erhöhtem Schutz. Verarbeitet ein externer Anbieter solche Daten im Auftrag der Praxis, verlangt Art. 28 einen Auftragsverarbeitungsvertrag (Folie 15). Er legt fest, was der Anbieter mit den Daten tun darf, wie er sie schützt und welche Unterauftragnehmer er einsetzt. Sobald Daten die EU verlassen oder ein Anbieter aus einem Drittland darauf zugreifen kann, kommen die Regeln aus Kapitel V hinzu.

Nicht jeder Anbieter ist Auftragsverarbeiter. Verwendet er die Eingaben auch für eigene Zwecke, zum Beispiel zum Training seines Modells, wird er insoweit selbst zum Verantwortlichen. Dann reicht ein Auftragsverarbeitungsvertrag für die Weitergabe nicht aus, und die Praxis bräuchte eine eigene Rechtsgrundlage, die für Patientendaten kaum zu finden ist. Deshalb fragt die Checkliste am Ende des Vortrags ausdrücklich nach der Rolle des Anbieters.

KI-Verordnung

Die KI-Verordnung (EU) 2024/1689, englisch AI Act, ist seit August 2024 in Kraft (Folien 13, 16, 21). Seit dem 2. Februar 2025 gilt Art. 4 zur KI-Kompetenz. Der Digital Omnibus, Verordnung (EU) 2026/1744, hat den Artikel mit Wirkung zum 27. Juli 2026 neu gefasst. Anbieter und Betreiber müssen Maßnahmen ergreifen, die die KI-Kompetenz ihrer Mitarbeiter fördern, passend zu den eingesetzten Systemen und Aufgaben. Ein bestimmtes Kompetenzniveau jeder einzelnen Person schreibt das Gesetz nicht mehr vor. Eine Praxis erfüllt die Pflicht mit dokumentierten Schulungen, einer schriftlichen Regelung und Unterweisungen am konkreten Werkzeug. Ein Zertifikat ist nicht erforderlich.

Seit dem 2. August 2026 gilt Art. 50 Abs. 1. Ein System, das mit Menschen spricht oder schreibt, muss erkennen lassen, dass eine KI antwortet. Das betrifft vor allem Telefon- und Chatassistenten am Empfang. Die Hochrisikopflichten hat der Omnibus verschoben: für die Bereiche aus Anhang III auf den 2. Dezember 2027, für KI in Produkten nach Anhang I, zu denen die Medizinprodukte gehören, auf den 2. August 2028. Gestrichen wurde keine dieser Pflichten. In Deutschland ist seit dem 29. Juli 2026 das KI-Marktüberwachungs- und Innovationsförderungsgesetz in Kraft, das die Bundesnetzagentur zur zentralen Aufsichtsbehörde bestimmt.

Für die Einordnung eines Systems gilt eine einfache Regel. Gesundheitsdaten allein machen ein System nicht zum Hochrisiko-System. Maßgeblich ist, ob es als Medizinprodukt der Prüfung durch eine Benannte Stelle unterliegt (Art. 6 Abs. 1). Software, die Briefe vorformuliert oder Gespräche verschriftlicht, liegt in der Regel darunter. Software, die Röntgenbilder befundet, liegt in der Regel darüber.

Strafgesetzbuch § 203

Die ärztliche Schweigepflicht ist strafbewehrt. Wer unbefugt ein Patientengeheimnis offenbart, riskiert Geldstrafe oder Freiheitsstrafe bis zu einem Jahr (Folie 17). Seit der Reform vom 9. November 2017 dürfen Ärzte externe Dienstleister einbeziehen, etwa für IT, Abrechnung oder Cloud-Dienste. Die Reform knüpft das an vier Voraussetzungen (Folie 39). Die Mitwirkung muss für die ärztliche Tätigkeit erforderlich sein. Der Dienstleister muss schriftlich zur Geheimhaltung verpflichtet und über die strafrechtlichen Folgen belehrt sein. Der Arzt muss ihn sorgfältig auswählen und überwachen.

Der Auftragsverarbeitungsvertrag und die Verpflichtung nach § 203 StGB werden oft verwechselt. Sie stammen aus zwei Rechtsgebieten und schützen zwei Rechtsgüter: der Vertrag die informationelle Selbstbestimmung des Patienten, die Verpflichtung das Vertrauensverhältnis zum Arzt. Viele Anbieter legen den Vertrag vor und vergessen die Verpflichtung. Die Praxis braucht beides.

Wichtig

Vor dem ersten echten Patientendatensatz liegen zwei Unterschriften vor: der Auftragsverarbeitungsvertrag nach Art. 28 DSGVO und die Geheimhaltungsverpflichtung nach § 203 StGB. Fehlt eine davon, wird das Werkzeug nur mit erfundenen Daten genutzt.

CLOUD Act und FISA Section 702

Die meisten großen KI-Anbieter sind US-Unternehmen oder gehören zu einem US-Konzern. Zwei US-Gesetze sind deshalb für deutsche Praxen relevant (Folie 18). Der Clarifying Lawful Overseas Use of Data Act von 2018 erlaubt US-Behörden, von US-Unternehmen die Herausgabe von Daten zu verlangen, auch wenn diese auf Servern in Frankfurt oder Dublin liegen. Der Serverstandort in der EU schützt also nicht allein. Es kommt auf den Konzern an, der den Server betreibt.

Section 702 des Foreign Intelligence Surveillance Act erlaubt US-Geheimdiensten, Kommunikation von Personen außerhalb der USA ohne richterliche Einzelfallanordnung zu erfassen. Der Kongress hat die Vorschrift 2024 mit dem Reforming Intelligence and Securing America Act verlängert. Nach zwei kurzen Übergangsverlängerungen ist die gesetzliche Grundlage im Juni 2026 ausgelaufen. Die Erhebung läuft auf Grundlage der geltenden Anordnungen des Überwachungsgerichts bis März 2027 weiter, über eine Neuregelung wird verhandelt. Für die europäische Bewertung ändert sich damit wenig, denn die Befugnisse bestehen faktisch fort.

Daten in die USA: was heute trägt

Der Datentransfer in die USA hat eine wechselvolle Geschichte (Folie 14). Das Abkommen Safe Harbor von 2000 erklärte der Europäische Gerichtshof 2015 nach einer Klage des österreichischen Juristen Max Schrems für ungültig. Den Nachfolger Privacy Shield kippte das Gericht 2020 im Urteil Schrems II. Seit dem 10. Juli 2023 gilt das Data Privacy Framework. Die USA haben dafür erstmals ein Beschwerdegericht für Europäer eingerichtet, den Data Protection Review Court. Das Gericht der EU hat eine Klage des französischen Abgeordneten Philippe Latombe am 3. September 2025 abgewiesen. Latombe hat Rechtsmittel beim EuGH eingelegt, das Verfahren läuft unter dem Aktenzeichen C-703/25 P.

Für die Praxis ergeben sich drei Wege (Folie 27). Ist der US-Empfänger unter dem Data Privacy Framework zertifiziert, trägt der Angemessenheitsbeschluss nach Art. 45 DSGVO den Transfer. Fehlt die Zertifizierung, bleiben Standardvertragsklauseln nach Art. 46 mit einer dokumentierten Transferfolgenabschätzung, dem Transfer Impact Assessment. Das ist aufwendig und für eine Einzelpraxis kaum selbst zu leisten. Die Ausnahmen nach Art. 49, etwa die ausdrückliche Einwilligung, sind für Einzelfälle gedacht und taugen nicht für die tägliche Routine.

Wichtig

Ein Angemessenheitsbeschluss ist eine Rechtsgrundlage auf Zeit. Zwei Vorgänger des Data Privacy Framework sind gescheitert. Wer einen Anbieter auswählt, fragt deshalb auch, was geschieht, wenn der Beschluss fällt: Gibt es eine Verarbeitung allein in der EU, und wie schnell lässt sie sich umstellen?

Technische Standards: BSI, C5 und NIS2

Das Bundesamt für Sicherheit in der Informationstechnik ist die Cybersicherheitsbehörde des Bundes und gehört zum Geschäftsbereich des Bundesinnenministeriums (Folie 20). Es prüft keine Arztpraxen. Seine Standards bestimmen aber, was ein Cloud-Anbieter im Gesundheitswesen nachweisen muss. Der wichtigste ist der Cloud Computing Compliance Criteria Catalogue, kurz C5.

Nach § 393 SGB V dürfen Leistungserbringer Gesundheitsdaten nur dann in der Cloud verarbeiten lassen, wenn ein aktuelles C5-Testat der datenverarbeitenden Stelle vorliegt (Folie 22). Ein Wirtschaftsprüfer stellt es aus. Typ 1 bescheinigt, dass die Kontrollen zu einem Stichtag angemessen ausgestaltet sind. Typ 2 bestätigt zusätzlich, dass sie über einen Prüfungszeitraum wirksam angewendet wurden. Bis zum 30. Juni 2025 genügte Typ 1, seit dem 1. Juli 2025 ist Typ 2 erforderlich. Für Systeme, die nach dem 30. Juni 2025 erstmals auf den Markt kommen, reicht Typ 1 für die ersten 18 Monate. Ein gleichwertiger oder höherer Standard ist zulässig.

Zwei Feinheiten entscheiden in der Praxis. Maßgeblich ist das Testat der Stelle, die die Daten verarbeitet, also der Anwendung. Das Testat des Rechenzentrums darunter genügt allein nicht. Und das BSI hat 2026 einen neuen Katalog veröffentlicht, C5:2026 mit 168 Basiskriterien statt bisher 121. Testate nach dem alten Katalog bleiben übergangsweise gültig, ab dem 1. Juni 2027 gilt nur noch der neue.

Das NIS2-Umsetzungsgesetz ist seit dem 6. Dezember 2025 in Kraft (Folie 23). Es verpflichtet Einrichtungen ab 50 Beschäftigten oder mehr als 10 Millionen Euro Jahresumsatz und Jahresbilanzsumme in bestimmten Sektoren, darunter das Gesundheitswesen, zu Risikomanagement, Zwei-Faktor-Anmeldung, Datensicherung, Notfallplänen und vertraglicher Bindung ihrer Dienstleister. Nach einem Angriff muss eine Erstmeldung binnen 24 Stunden an das BSI gehen, ein Bericht nach 72 Stunden, ein Abschluss nach einem Monat. Die Einzelpraxis erreicht diese Schwellen nicht, größere MVZ-Verbünde und Kliniken sollten ihre Einordnung prüfen. Die DSGVO mit der 72-Stunden-Meldung bei Datenpannen nach Art. 33 gilt für alle.

Spracherkennung, Sprachmodell und die zweite Freigabe

Modul 2 hat die Abgrenzung eingeführt, hier dient sie dem Datenschutz (Folie 24). Die Spracherkennung verschriftlicht das gesprochene Wort. Sie arbeitet mit neuronalen Netzen und ist im Sinne der KI-Verordnung ein KI-System, aber kein Sprachmodell. Ihre Fehler sind hörbar falsche Wörter. Das Sprachmodell liest den Text und formuliert ihn um. Seine Fehler lesen sich fehlerfrei. Systeme zur Gesprächsdokumentation schalten beide Techniken hintereinander. Für den Datenschutz heißt das: zwei Verarbeitungsschritte, zwei mögliche Orte der Verarbeitung, zwei Fragen an den Anbieter. Wo läuft die Spracherkennung, und wo das Sprachmodell?

Der Vortrag zeigt auf Folie 26 eine Architektur, bei der die Audiodaten die Praxis nicht verlassen und identifizierende Angaben vor der Cloud durch Platzhalter ersetzt werden. Es handelt sich um das System des Referenten, der Interessenkonflikt ist offengelegt. Das Beispiel dient der Veranschaulichung des Prinzips. Die zehn Prüffragen am Ende gelten für jedes Produkt, auch für dieses.

Was Patienten wahrnehmen

Moritz Reis, Florian Reis und Wilfried Kunde haben 2025 in JAMA Network Open untersucht, wie Patienten auf offengelegte KI-Nutzung reagieren (Folien 34 und 35). In einem randomisierten Online-Experiment sahen 1.276 Erwachsene aus den USA vier Fassungen derselben Anzeige eines Hausarztes. Einziger Unterschied war ein Satz: kein Hinweis auf KI, KI für die Verwaltung, für die Diagnose oder für die Therapie. Die Teilnehmer bewerteten Kompetenz, Vertrauenswürdigkeit, Empathie und ihre Bereitschaft, einen Termin zu vereinbaren, auf einer Fünf-Punkte-Skala.

Jede KI-Variante schnitt schlechter ab als die Anzeige ohne Hinweis, auch die reine Verwaltung. Bei der Behandlungsvariante sank die Kompetenz von 3,85 auf 3,58, das Vertrauen von 3,88 auf 3,61 und die Empathie von 4,00 auf 3,72. Die Terminbereitschaft fiel von 3,61 auf 3,15. Die Effektstärken lagen bei Cohen's d zwischen 0,16 und 0,41 und gelten damit als klein.

Die Studie misst, wie Patienten einen Arzt wahrnehmen. Die Qualität der Behandlung erfasst sie nicht. Die Teilnehmer lasen eine erfundene Anzeige und hatten keinen Arztkontakt. Ob sich das Ergebnis auf Patienten in Deutschland und auf ein Gespräch im Sprechzimmer übertragen lässt, ist offen. Für die Praxis bleibt dennoch ein Befund: Die bloße Information über KI kostet Vertrauen. Da Transparenz rechtlich geboten ist, kommt es auf die Art der Erklärung an. Ein Satz zum konkreten Nutzen, zum Schutz der Daten und zur ärztlichen Endverantwortung wirkt anders als ein Hinweis im Kleingedruckten.

Wie groß ist das Risiko wirklich?

Der Vortrag trennt zwei Risiken (Folie 38). Das operative Zugriffsrisiko, also die Gefahr, dass ein Geheimdienst gezielt die Daten einer orthopädischen Praxis anfordert, ist realistisch sehr gering. Das organisatorische Risiko ist größer und liegt in der Hand der Praxis. Aufsichtsbehörden wie der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg prüfen Dokumentation und Verträge. Fehlt der Auftragsverarbeitungsvertrag, die Verpflichtung nach § 203 StGB oder eine tragfähige Transfergrundlage, liegt ein Verstoß vor, gleich ob jemals ein Zugriff stattgefunden hat.

Zur Verantwortung gehört die Plausibilisierung. Nach der Stellungnahme der Zentralen Ethikkommission bei der Bundesärztekammer von 2021 bleibt die Verantwortung für Diagnose und Therapie beim Arzt (Folien 25 und 37). Ein KI-Ergebnis wird geprüft, bevor es in die Akte oder an den Patienten geht.

Zehn Fragen an jeden KI-Anbieter

Die Checkliste von Folie 40 lässt sich ohne juristische Vorbildung abarbeiten. Ein Anbieter, der Patientendaten verarbeiten will, sollte jede Frage schriftlich beantworten können. Die rechte Spalte nennt, worauf die Praxis bei der Antwort achtet.

Nr.	Frage an den Anbieter	Worauf achten
1	Wo werden Daten verarbeitet und gespeichert?	Land und Rechenzentrum für jeden Verarbeitungsschritt, auch für Spracherkennung und Sprachmodell getrennt
2	Wer ist Vertragspartner, welche Konzern- und Subprozessorstruktur gibt es?	Liste der Unterauftragnehmer, US-Muttergesellschaft im Konzern
3	Welche Rolle hat der Anbieter?	Auftragsverarbeiter, eigener Verantwortlicher oder gemeinsam Verantwortlicher
4	Gibt es einen Auftragsverarbeitungsvertrag und eine Verpflichtung nach § 203 StGB?	Beide Dokumente, unterschriftsreif
5	Werden Eingaben, Ausgaben oder Rückmeldungen für Training oder Produktverbesserung genutzt?	Ausschluss im Vertrag, nicht nur in einer Einstellung
6	Gibt es menschliche Durchsicht, Supportzugriffe oder Annotation?	Wer, wann, mit welcher Protokollierung
7	Welche Aufbewahrungs- und Löschfristen gelten?	Konkrete Fristen, Möglichkeit ohne Speicherung beim Modellanbieter
8	Welcher Transfermechanismus gilt?	Verarbeitung nur in der EU, Data Privacy Framework oder Standardvertragsklauseln mit TIA
9	Wie sieht das Schlüssel- und Zugriffsmodell aus?	Verschlüsselung bei Übertragung und Speicherung, wer die Schlüssel hält
10	Welche Sicherheitsnachweise liegen vor?	Aktuelles C5-Testat Typ 2 der Anwendung, ISO 27001

Wichtig

Die Antworten des Anbieters werden mit Datum abgelegt. Das Protokoll belegt die sorgfältige Auswahl nach § 203 StGB und dient zugleich als Nachweis der KI-Kompetenzmaßnahmen nach Art. 4 KI-VO.

Prompt-Bibliothek Modul 3

Die folgenden Aufträge arbeiten ohne Patientendaten. Sie folgen dem Fünf-Baustein-Modell aus Modul 2: Rolle, Kontext, Aufgabe, Format, Leitplanken. Die Leitplanke steht jeweils am Ende und wird nicht weggelassen.

Entwurf einer Praxisregelung zur KI-Nutzung

Du bist Datenschutzberater für Arztpraxen in Deutschland. Meine Praxis ist eine orthopädische Einzelpraxis mit zwei Ärzten und sechs Medizinischen Fachangestellten. Wir nutzen ein Praxisverwaltungssystem und wollen KI für Textentwürfe einsetzen. Entwirf eine Praxisregelung zur Nutzung von KI-Werkzeugen. Sie soll festlegen, welche Werkzeuge erlaubt sind, welche Daten eingegeben werden dürfen, wer Ergebnisse prüft und wie Schulungen dokumentiert werden. Format: höchstens zwei Seiten, nummerierte Abschnitte, verständlich für das Praxisteam. Erfinde keine Rechtsvorschriften. Kennzeichne Stellen, an denen ich praxisspezifische Angaben ergänzen muss, und Stellen, an denen du dir rechtlich unsicher bist.

Anfrage an einen Anbieter

Du bist Ärztin in einer Praxis in Baden-Württemberg und schreibst an einen Anbieter von KI-Dokumentationssoftware. Ich möchte vor einer Entscheidung schriftliche Auskunft zu Datenschutz und Sicherheit. Formuliere eine höfliche, knappe E-Mail, die die folgenden zehn Fragen stellt: [Fragen 1 bis 10 aus der Tabelle einfügen]. Bitte um Antwort binnen zwei Wochen und um Übersendung von Auftragsverarbeitungsvertrag, Verpflichtung nach § 203 StGB und C5-Testat. Format: E-Mail mit Betreffzeile, Fragen nummeriert. Ergänze keine eigenen Fragen und keine Behauptungen über den Anbieter.

Antworten eines Anbieters auswerten

Du bist Datenschutzbeauftragter einer Arztpraxis. Unten steht die Antwort eines Software-Anbieters auf zehn Fragen zu Datenschutz und Sicherheit. Prüfe jede Antwort darauf, ob sie die Frage konkret beantwortet, ausweicht oder offenlässt. Format: Tabelle mit den Spalten Frage, Antwort des Anbieters in einem Satz, Bewertung (beantwortet, unklar, fehlt), Nachfrage. Zitiere nur, was in der Antwort steht. Erfinde keine Angaben, die der Anbieter nicht gemacht hat, und kennzeichne, wo du eine rechtliche Bewertung nicht sicher treffen kannst. [Antwort des Anbieters einfügen, ohne Patientendaten]

Patienteninformation zum KI-Einsatz

Du bist Ärztin in einer orthopädischen Praxis. Wir setzen eine Software ein, die aus dem Gespräch einen Briefentwurf erstellt, den ich vor dem Versand prüfe und freigebe. Schreibe eine Patienteninformation für den Aushang am Empfang. Sie soll erklären, wozu wir die Software nutzen, was mit den Daten geschieht, dass jeder Brief ärztlich geprüft wird und dass Patienten die Aufzeichnung ablehnen können. Format: höchstens 150 Wörter, einfache Sprache, keine Fachbegriffe. Verspreche nichts, was nicht im Text oben steht, und erfinde keine technischen Details.

Morgen früh

Drei Aufgaben, jede unter zehn Minuten und ohne Patientendaten. Erstens: Prüfen Sie, welche KI-Werkzeuge in Ihrer Praxis tatsächlich genutzt werden, auch auf privaten Telefonen am Empfang. Fragen Sie das Team, ohne zu tadeln. Zweitens: Suchen Sie für das wichtigste dieser Werkzeuge den Auftragsverarbeitungsvertrag und die Verpflichtung nach § 203 StGB heraus. Fehlt eines davon, legen Sie fest, dass das Werkzeug bis zur Klärung nur mit erfundenen Daten genutzt wird. Drittens: Notieren Sie Datum und Inhalt dieser Fortbildung in Ihrer Schulungsdokumentation. Das ist Ihr Nachweis nach Art. 4 KI-VO.

Die Hausaufgabe bis Modul 4 am 4. November 2026: Gehen Sie die zehn Fragen an einem KI-Werkzeug Ihrer Praxis durch und notieren Sie, was der Anbieter offenlässt.

Quellen

1. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (Datenschutz-Grundverordnung). ABl. L 119 vom 4.5.2016, S. 1. Art. 9, 28, 33, 44 bis 49.
2. Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 (KI-Verordnung). ABl. L, 2024/1689, 12.7.2024. Art. 4, 5, 6, 50, 99, 113.
3. Verordnung (EU) 2026/1744 zur Änderung der Verordnung (EU) 2024/1689 (Digital Omnibus zur KI-Verordnung). In Kraft seit 27.7.2026.
4. KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG) vom 22. Juli 2026. BGBl. 2026 I Nr. 223. In Kraft seit 29.7.2026.
5. Strafgesetzbuch, § 203 Verletzung von Privatgeheimnissen, Fassung durch Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. Oktober 2017. BGBl. 2017 I S. 3618.
6. Sozialgesetzbuch V, § 393 Cloud-Einsatz im Gesundheitswesen, Abs. 3 und 4. Wortlaut abgerufen am 4.10.2026 über dejure.org.
7. Bundesamt für Sicherheit in der Informationstechnik. Cloud Computing Compliance Criteria Catalogue, C5:2020 und C5:2026. Bonn: BSI. bsi.bund.de.
8. Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG). In Kraft seit 6.12.2025. Richtlinie (EU) 2022/2555.
9. Europäischer Gerichtshof. Urteil vom 16.7.2020, C-311/18, Data Protection Commissioner gegen Facebook Ireland und Maximilian Schrems (Schrems II).
10. Europäische Kommission. Durchführungsbeschluss (EU) 2023/1795 vom 10.7.2023 über die Angemessenheit des Schutzniveaus nach dem EU-US-Datenschutzrahmen.
11. Gericht der Europäischen Union. Urteil vom 3.9.2025, T-553/23, Latombe gegen Kommission. Rechtsmittel anhängig unter C-703/25 P.
12. Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Pub. L. 115-141, Div. V, 2018.
13. Foreign Intelligence Surveillance Act, Section 702; Reforming Intelligence and Securing America Act, Pub. L. 118-49, 2024. Stand der Verlängerung: Brennan Center for Justice, Section 702 Resource Page, abgerufen am 4.10.2026.
14. Reis M, Reis F, Kunde W. Public perception of physicians who use artificial intelligence. JAMA Netw Open. 2025;8(7):e2521643.
15. Doctolib. Digital Health Report 2026. Befragung von 414 Ärzten.
16. Bitkom, Hartmannbund. Ärztebefragung 2025 (616 Ärzte).
17. Bitkom. Cloud Report, Juni 2026 (603 Unternehmen aller Branchen).
18. Zentrale Kommission zur Wahrung ethischer Grundsätze in der Medizin und ihren Grenzgebieten (ZEKO) bei der Bundesärztekammer. Entscheidungsunterstützung ärztlicher Tätigkeit durch Künstliche Intelligenz. Dtsch Arztebl. 2021;118(33-34).
19. OpenAI. Help Center: Data retention and Temporary Chats. Abgerufen am 4.10.2026.

Stand der Rechtslage: 4. Oktober 2026. Das Handout dient der Fortbildung und ersetzt keine Rechtsberatung im Einzelfall.