



KI-Dokumentation in der Arztpraxis: Unterstützung bei Auswahl und Einführung

Praxisnaher Leitfaden zu Funktionsweise, Einführung, Risiken und regulatorischen Anforderungen von KI-Dokumentation in der Arztpraxis

Stand: Januar 2026



Dieses Dokument dient ausschließlich Informationszwecken und stellt keine rechtliche oder medizinische Beratung dar.

Einleitung

Ärztinnen und Ärzte verbringen einen erheblichen Teil ihrer Arbeitszeit mit Dokumentationsaufgaben statt mit der direkten Patientenbetreuung. Die Belastung durch Bürokratie kann die Arzt-Patienten-Interaktion beeinträchtigen und das Risiko von Erschöpfung erhöhen. Gleichzeitig steigen die Anforderungen an Dokumentationsqualität und -vollständigkeit kontinuierlich an.

Künstliche Intelligenz (KI) bietet neue Möglichkeiten, den Dokumentationsaufwand zu reduzieren, ohne die Genauigkeit zu kompromittieren. Insbesondere KI-gestützte medizinische Dokumentationssysteme können Routineaufgaben übernehmen, indem sie Patientengespräche erfassen, in Text übertragen und strukturiert zusammenfassen. So bleibt mehr Zeit für die Patientenversorgung, während die Dokumentation im Hintergrund vorbereitet wird.

Dieses Whitepaper gibt einen umfassenden Überblick über die Funktionsweise solcher Systeme, die technischen Grundlagen, Voraussetzungen für eine erfolgreiche Einführung, mögliche Schwachstellen sowie die relevanten rechtlichen Rahmenbedingungen in Deutschland. Zudem enthält es eine Checkliste, mit der Sie die Eignung und Datenschutzkonformität eines KI-Dokumentationssystems – beispielhaft dargestellt an der Medistella AI Box – für Ihre Praxis bewerten können. Ziel ist ein fundierter und verständlicher Leitfaden, der den sicheren und effizienten Einsatz von KI in der Praxisdokumentation unterstützt.

Funktionsweise KI-gestützter medizinischer Dokumentation

KI-gestützte Dokumentationssysteme übernehmen Teilschritte der schriftlichen Dokumentation und entlasten damit die Behandlerin oder den Behandler. Typischerweise läuft der Prozess in mehreren Schritten ab:

- **Gesprächsaufzeichnung und Transkription:** Das Arzt-Patienten-Gespräch wird aufgezeichnet (z.B. über ein Mikrofon im Sprechzimmer oder per Diktierfunktion). Eine automatische Spracherkennung (Automatic Speech Recognition, ASR) wandelt die gesprochene Sprache in Text um.
- **Inhaltsanalyse und Zusammenfassung:** Ein Large Language Model (LLM) verarbeitet den transkribierten Text, filtert medizinisch relevante Inhalte heraus und formuliert eine strukturierte Zusammenfassung. Wichtiges wird von Unwichtigem getrennt; redundante oder nicht-medizinische Passagen werden reduziert.
- **Strukturierte Dokumentation und Ausgabe:** Die Ergebnisse können in der gewünschten Dokumentationsstruktur ausgegeben werden (z.B. Anamnese, Befund, Beurteilung, Plan) oder als Arztbrief-Entwurf. Fortgeschrittene Systeme können Inhalte für die elektronische Akte vorbereiten und strukturiert bereitstellen.

- **Manuelle Überprüfung und Freigabe:** Vor der Übernahme in die Patientenakte wird der Vorschlag durch die Ärztin bzw. den Arzt geprüft und bei Bedarf korrigiert. Dieser Schritt ist zentral, um medizinische Korrektheit und Vollständigkeit sicherzustellen („Human in the Loop“).

Zusammengefasst funktioniert KI-Dokumentation wie ein digitaler medizinischer Schreibassistent: Er „hört zu“, schreibt mit und formuliert einen Dokumentationsvorschlag. Die Ärztin bzw. der Arzt behält jedoch stets die Kontrolle, passt den Vorschlag an und gibt ihn final frei.

Technische Grundlagen (ASR und Large Language Models)

Die beschriebenen Funktionen werden durch zwei zentrale KI-Technologien ermöglicht: automatische Spracherkennung und große Sprachmodelle.

Automatische Spracherkennung (ASR)

Moderne Spracherkennungssysteme basieren auf KI und Deep-Learning-Verfahren. Sie analysieren akustische Sprachmuster und rekonstruieren daraus den gesprochenen Text. Im medizinischen Kontext ist ASR anspruchsvoll, da Fachbegriffe, Abkürzungen und unterschiedliche Sprechweisen vorkommen können. Die erreichbare Genauigkeit hängt deswegen auch von Audioqualität, Sprechweise und der Anpassung an medizinisches Vokabular ab.

Large Language Models (LLMs)

LLMs sind Sprachmodelle, die auf großen Textmengen trainiert wurden und Sprache kontextuell verarbeiten sowie selbst generieren können. In Dokumentationslösungen übernehmen sie die sprachliche und inhaltliche Aufbereitung: Aus dem Transkript wird ein strukturierter Text mit klinisch relevanten Informationen. Für den medizinischen Einsatz sind spezialisierte oder feinjustierte Modelle vorteilhaft, um Terminologie korrekt zu handhaben und Fehlinterpretationen zu reduzieren.

Technisch erfordert der Betrieb dieser KI-Komponenten eine erhebliche Rechenleistung. Spracherkennung und Sprachgenerierung in Echtzeit sind rechenintensiv und erfordern entweder Cloud-Server oder lokale Hochleistungs-Hardware. Die Medistella AI Box verfolgt hier den Ansatz, die nötige KI-Infrastruktur direkt in die Praxis zu bringen. In dem kompakten Gerät steckt spezialisierte Hardware (vergleichbar mit einem kleinen Server oder leistungsfähigen PC), die die ASR- und LLM-Modelle ausführt. Alternativ greifen Cloud-basierte Dienste auf entfernte Rechenzentren zu, was allerdings hohe Anforderungen an Datenschutz und Regulatorik mit sich bringt.

Unabhängig vom Bereitstellungsmodell bilden ASR und LLM das technische Herzstück: Erst durch ihr Zusammenspiel – präzise Transkription plus intelligente Textgenerierung – wird eine vollautomatische Dokumentation möglich.

Voraussetzungen und Anforderungen bei der Einführung

Damit eine KI-gestützte Dokumentation zuverlässig und effizient in Ihrer Praxis funktioniert, müssen einige **Voraussetzungen** erfüllt sein und **Anforderungen** bedacht werden. Die Einführung betrifft sowohl technische als auch organisatorische Aspekte:

Hochwertige Audioerfassung

Die Grundlage jeder Spracherkennung ist ein klares Audiosignal. Empfehlenswert sind gute Mikrofone in der Nähe von Arzt und Patient sowie eine möglichst ruhige Umgebung. Hintergrundgeräusche, mehrere gleichzeitige Sprecher und ungünstige Raumakustik können die Erkennungsqualität deutlich verschlechtern.

Technische Integration in die Praxis-IT

Um effiziente Arbeitsabläufe zu gewährleisten, sollten KI-Dokumentationssysteme stabil in den bestehenden Praxisablauf eingebettet werden. Die technische Integration kann entweder als eigenständige Anwendung (App) auf dem Arzt-PC erfolgen, oder das KI-Dokumentationssystem wird über den Browser aufgerufen. Im Fall von Medistella etwa wird auf dem Praxis-PC eine App installiert, die als Benutzeroberfläche dient.

Lokale Verarbeitung vs. Cloud

Die eigentliche KI-Verarbeitung der Daten findet dann entweder auf einem separaten Gerät in der Praxis (z.B. Medistella AI Box) oder in einem Rechenzentrum statt (Cloud). Bei der lokalen Installation verbinden Sie die Anwendung auf ihrem PC mit dem lokalen KI-Rechner. Hierfür benötigen Sie lediglich ein Netzkabel und Strom. Bei Anbietern mit Cloud-Verarbeitung verbindet sich ihr Browser über Ihre stabile Internetverbindung mit dem Rechenzentrum ihres Anbieters. In beiden Fällen ist auf aktuelle Sicherheitsstandards zu achten: die Verbindungen sollten verschlüsselt erfolgen, und unberechtigter Zugriff muss ausgeschlossen sein.



Integration in das PVS

Weiterhin sollte geprüft werden, **wie das System mit dem Praxisverwaltungssystem (PVS)** interagiert: Idealerweise gibt es Plugins oder Schnittstellen, die es der KI-App erlauben, Dokumentationstexte direkt in die elektronische Patientenakte zu übertragen. Viele Anbieter werben mit Kompatibilität zu gängigen PVS – in der Praxis kann dies vom einfachen Copy-Paste bis zur tiefen Integration per API reichen. Klären Sie vorab, ob Ihr PVS unterstützt wird und ob eventuell Updates oder Zusatzmodule nötig sind.

Workflow und Verhalten

Die Einführung einer KI für Dokumentation erfordert ggf. **Anpassungen im Arbeitsablauf**. Zunächst müssen das Praxisteam und die Patienten über den Einsatz der Technik informiert sein. Es sollte festgelegt werden, *wann* und *wie* Aufzeichnungen gestartet werden – z.B. per Klick in der Software, per Tastenkombination oder automatisiert über das PVS.

Ärzte müssen sich daran gewöhnen, möglichst **alles Relevante mündlich auszusprechen**, da nur Gesagtes von der KI erfasst wird. Falls bestimmte Untersuchungsergebnisse normalerweise wortlos notiert würden (etwa Blutdruck, der vom Gerät angezeigt wird), müssen diese aktiv diktiert werden, damit die KI sie aufnehmen kann. Hier kann eine kurze Eingewöhnungszeit nötig sein, bis die neue „Mitschreib-Assistenz“ in den Alltag integriert ist. Das bewusste Aussprechen hat dabei noch einen

positiven Nebeneffekt: Es verbessert sich die Kommunikation mit dem Patienten und sie geben bewusster und gezielter Informationen an ihre Patienten weiter.

Auch sollte definiert sein, wer die KI-Ergebnisse kontrolliert: In der Regel wird dies der Arzt selbst tun, eventuell unterstützt von MFA bei der Nachbearbeitung. Planen Sie für diese **Überprüfungsphase** pro Bericht anfangs etwas Zeit ein – die Erfahrung zeigt jedoch, dass mit steigender KI-Qualität und Gewöhnung dieser Aufwand sinkt.

Organisatorische Anforderungen

Aus datenschutzrechtlicher Sicht muss vor Inbetriebnahme geprüft werden, ob eine **Datenschutz-Folgenabschätzung** nötig ist (insbesondere bei der Nutzung von Cloud Services kann dies häufig der Fall sein) und ob ein Datenschutzbeauftragter eingebunden werden muss. Gegebenenfalls sind entsprechende Dokumentationen anzufertigen und die technischen und organisatorischen Maßnahmen des Anbieters sollten kritisch geprüft werden. Ferner sollten Verträge mit dem Anbieter abgeschlossen sein (z.B. Auftragsverarbeitung bei Cloud-Lösungen).

Die Praxis sollte intern festlegen, wie mit den KI-generierten Dokumenten verfahren wird: Werden Audioaufnahmen und Transkriptionen gespeichert oder nach Verarbeitung gelöscht? Letzteres ist aus Datenschutzgründen zu bevorzugen und wird von einigen Systemen automatisiert erledigt. Gibt es Fallback-Lösungen, falls die KI temporär ausfällt (z.B. zurück zum klassischen Dokumentieren oder handschriftlichen Notizen)? Auch die IT-Sicherheit der Praxis insgesamt (aktueller Virenschutz, Firewall etc.) muss auf dem Stand sein, insbesondere wenn neue Geräte ins Netz kommen.

Zusammengefasst erfordert die Einführung von KI-Dokumentation **technische Vorbereitungen (Hardware, Software, Netzwerkanbindung), organisatorische Maßnahmen (Schulungen, Patienteninformation) und rechtliche Abklärungen (Verträge, Datenschutzfolgeabschätzung)**. Ist all dies sorgfältig erfüllt, steht einer erfolgreichen Integration nichts im Wege. Insbesondere die Medistella AI Box wurde darauf ausgelegt, schnell und einfach in bestehende IT-Strukturen eingebunden zu werden und möglichst geringen administrativen und regulatorischen Aufwand zu erzeugen. Die Anfangsinvestition an Zeit zahlt sich im laufenden Betrieb durch erhebliche Zeitersparnis bei der Dokumentation aus.

Schwächen und potenzielle Fehlerquellen

Trotz aller Fortschritte ist es wichtig zu verstehen, dass KI-Systeme nicht unfehlbar sind. Bei der KI-gestützten Dokumentation gibt es einige **potenzielle Schwachstellen und Fehlerquellen**, derer man sich bewusst sein sollte.

Halluzinationen und inhaltliche Fehler

Große Sprachmodelle neigen gelegentlich dazu, *plausibel klingende, aber falsche Informationen* zu generieren. Dieses Phänomen wird als *Halluzination* bezeichnet. In der Praxis könnte dies bedeuten, dass das System einen medizinischen Sachverhalt erwähnt oder interpretiert, der so gar nicht im Gespräch fiel oder nicht zutrifft. Zum Beispiel könnte aus einer unscharfen Aussage des Patienten eine konkrete Diagnose gemacht werden, die nicht vom Arzt geäußert wurde. Solche Fehler sind besonders tückisch, weil sie auf den ersten Blick überzeugend wirken. Daher muss jeder von der KI verfasste Dokumentationstext **kritisch gegengelesen** werden. Die ärztliche Freigabe ist genau aus diesem Grund unverzichtbar. Nur so lassen sich Halluzinationen oder Fehldeutungen sicher ausmerzen, bevor sie in der Akte landen.

Erkennungs- und Verständnisfehler

Die automatische Spracherkennung kann bei ungünstigen Bedingungen Fehler machen. **Akustische Missverständnisse** treten etwa bei starkem Dialekt, sehr schnellem Sprechen oder mehreren Leuten, die durcheinanderreden, auf. Ein versprochenes „kein Fieber“ könnte fälschlich als „Fieber“ transkribiert werden, wenn die Audioqualität schlecht ist. Ebenso kann das Sprachmodell Inhalte falsch interpretieren - z.B. ironische Bemerkungen wörtlich nehmen oder Nebensächliches überbewerten. Es besteht auch die Gefahr, dass relevante Details unter den Tisch fallen, wenn sie vom Patienten nur beiläufig erwähnt wurden. Hier zeigt sich die Grenze der KI: Kontext und Bedeutung medizinischer Aussagen korrekt einzuschätzen, ist anspruchsvoll. Die heutigen Modelle sind zwar erstaunlich gut, aber nicht perfekt. **Doppeldeutigkeiten** oder fehlende Informationen (etwa Laborwerte, die noch nicht vorliegen) können die KI verwirren.

Fachsprache, Abkürzungen und Strukturierung

Obwohl KI-Modelle mit medizinischen Begriffen trainiert werden, kann es zu Problemen kommen, wenn sehr spezielle **Fachterminologie** oder klinikspezifische Abkürzungen verwendet werden. Ein Begriff wie „ZTg“ dürfte ein generisches Modell nicht verstehen. Es kann entweder etwas Unsinniges daraus machen oder den Begriff auslassen. Solche Lücken müssen im Nachhinein manuell korrigiert werden. Einige Systeme erlauben es, eigene Wortlisten oder Abkürzungsverzeichnisse zu hinterlegen, um das Modell zu „trainieren“. In jedem Fall sollte man darauf gefasst sein, dass **sehr fachspezifische Ausdrücke** nicht immer richtig erfasst oder interpretiert werden.

Mitunter teilt die KI die Zusammenfassung nicht perfekt passend in die gewünschten Kategorien ein. Beispielsweise könnte ein Symptom irrtümlich im Abschnitt „Befund“ statt „Anamnese“ landen, wenn es im Gespräch erst später erwähnt wurde. Auch hier gilt: Die KI liefert einen *Entwurf*, der dem Arzt viel Arbeit abnimmt, aber Feinschliff durch fachkundiges Auge bleibt nötig. Der Mensch muss prüfen, ob die Gliederung und Gewichtung der Informationen stimmen.

Technische Ausfälle sowie Datenschutz- und Sicherheitsrisiken

Wie jedes IT-System kann auch eine KI-Lösung ausfallen oder Verzögerungen verursachen. Für diesen Fall sollten Ausweichmöglichkeiten geplant werden. Eine häufig diskutierte Schwachstelle – vor allem bei Cloud-Lösungen – ist das *Datenschutzrisiko*. Wenn sensible Patientendaten zur Verarbeitung ins Internet gesendet werden, besteht immer ein Restrisiko des unbefugten Zugriffs oder Datenlecks, insbesondere bei unsicheren Konfigurationen. Auch die **Weiterverwendung der Daten** zu KI-Trainingszwecken ist ein potenzielles Problem, falls der Anbieter dies nicht vertraglich ausschließt. Bei lokalen Lösungen (wie der Medistella AI Box) sind diese Risiken deutlich reduziert, da die Daten die Praxis nicht verlassen. Dennoch muss auch intern für IT-Sicherheit gesorgt sein (Schutz vor Hackerangriffen, Zugriffsrechte nur für befugtes Personal etc.).

Rechtliche Verantwortung

Am Ende trägt trotz KI-Unterstützung der Arzt bzw. die Ärztin die volle Verantwortung für den Dokumentationsinhalt und die datenschutzkonforme Verarbeitung der Gesundheitsdaten. Ein KI-Fehler entbindet nicht von haftungsrechtlicher Verantwortung. Daher muss jedem klar sein: Die KI ist ein Hilfsmittel, *kein* Ersatz für die klinische Beurteilung. In Rechtsfragen (z.B. Behandlungsfehler-Prozessen) zählt, was in der Patientenakte steht – unabhängig davon, ob es von einem Menschen oder einer KI formuliert wurde. Dementsprechend sollte man im Zweifel eher konservativ entscheiden: lieber eine AI-generierte Passage verwerfen, wenn man unsicher ist, und selbst schreiben, als blind zu vertrauen. Und lieber ein System auswählen, welches das Risiko eines Datenschutzverstoßes reduziert – oder am besten komplett ausschließt.

Diese potenziellen Schwächen bedeuten **nicht**, dass KI-Dokumentation unzuverlässig wäre. Im Gegenteil, die meisten Erfahrungen sind positiv. Aber wie jedes technische System verlangt es informierte, verantwortungsvolle Anwendung. Durch sorgfältige Schulung, konsequente Endkontrolle und Auswahl eines qualitativ hochwertigen Systems lassen sich die genannten Risiken minimieren. Die Medistella-Lösung begegnet einigen dieser Punkte z.B. dadurch, dass der Dokumentationsvorschlag *immer* manuell freigegeben werden muss und die Patientendaten die Praxis zu keiner Zeit verlassen. Dennoch sollte man stets wachsam bleiben. Letztlich ist die Kombination aus KI-Power *und* ärztlichem Verstand der Schlüssel zur besten Dokumentationsqualität.

Regulatorische und rechtliche Rahmenbedingungen

Der Einsatz von KI in der medizinischen Dokumentation berührt mehrere Rechtsbereiche. In Deutschland gelten strenge Vorgaben zum Schutz personenbezogener Daten und zur Wahrung der ärztlichen Schweigepflicht. Zusätzlich kommen neue europäische Anforderungen für KI-Systeme hinzu.

Datenschutz (DSGVO) und Einwilligung

Gesundheitsdaten gehören zu den besonders schützenswerten personenbezogenen Daten. Für die Verarbeitung ist eine tragfähige Rechtsgrundlage erforderlich. In vielen Praxisszenarien ist eine ausdrückliche Einwilligung der Patientin oder des Patienten sinnvoll bzw. notwendig - insbesondere bei Aufzeichnung und KI-Auswertung von Gesprächen.

Praktisch bedeutet dies: Vor Einsatz der KI-Dokumentation informieren Sie Ihre Patienten und lassen Sie sich schriftlich bestätigen, dass sie mit der Aufzeichnung des Gesprächs und der KI-Auswertung einverstanden sind. Am besten integriert man dies in die allgemeinen Datenschutz- und Behandlungsinformationen, die neue Patienten ohnehin unterschreiben. Da es sich um Gesundheitsdaten handelt, muss die Einwilligung *ausdrücklich* erfolgen (ein stillschweigendes Dulden reicht nicht). Im Zweifel sollte man Rechtsrat einholen, um den Text der Einwilligung korrekt zu gestalten.

Darüber hinaus gelten die DSGVO-Grundsätze (Datenminimierung, Zweckbindung, Speicherbegrenzung, Integrität und Vertraulichkeit). Prüfen Sie insbesondere, ob Audioaufnahmen gespeichert oder nach Verarbeitung gelöscht werden und wie Auskunfts- und Löschbegehren umgesetzt werden.

Insgesamt lässt sich festhalten, dass bei lokaler Verarbeitung in der Praxis (wie Medistella es ermöglicht) der DSGVO-Aufwand überschaubar bleibt: *Die Daten verbleiben intern*, es werden keine Dritten involviert, somit reduziert sich das Risiko von Verstößen erheblich. Dennoch bleibt die Information und Einwilligung der Patienten sowie eine DSGVO-konforme Dokumentation der Verarbeitungstätigkeit Pflicht.

Berufsgeheimnis (§203 StGB) und Auftragsverarbeitung

Ärztinnen und Ärzte unterliegen der **berufsrechtlichen Schweigepflicht**. Sie dürfen Patientengeheimnisse nicht unbefugt an Dritte weitergeben. Dieses *Berufsträgergeheimnis* stellt besondere Anforderungen, wenn externe IT-Dienstleister oder KI-Anbieter in die Verarbeitung involviert sind. Grundsätzlich gilt:

Keine unbefugte Weitergabe: Sobald Patientendaten die Praxis verlassen – etwa zur Verarbeitung auf einem Cloud-Server eines Anbieters – liegt eine *Datenweitergabe* an einen Dritten vor. Um dies straffrei zu gestalten, muss eine gesetzliche Erlaubnis oder Einwilligung vorliegen. Die Einwilligung des Patienten deckt zwar datenschutzrechtlich viel ab, entbindet aber nicht automatisch von §203 StGB. Dieser wurde allerdings dahingehend **erweitert**, dass die Einbeziehung externer Dienstleister erlaubt ist, wenn sie *als „Hilfsperson“ in die berufliche Tätigkeit einbezogen* sind und ihrerseits der Verschwiegenheit verpflichtet wurden. In der Praxis bedeutet das: Der externe KI-Dienstleister muss vertraglich auf Geheimhaltung verpflichtet sein und darf die Daten nur im Auftrag und nach Weisung der Arztpraxis verarbeiten

Auftragsverarbeitungs-Vertrag (AVV): Datenschutzrechtlich und berufsrechtlich unerlässlich ist bei externen Cloud-Diensten der Abschluss eines Auftragsverarbeitungs-Vertrags gemäß Art. 28 DSGVO. Darin wird festgelegt, dass der Anbieter die Daten *ausschließlich* für den definierten Zweck (Dokumentation) verwendet, **weisungsgebunden** tätig wird und geeignete Vertraulichkeits- und Sicherheitsmaßnahmen trifft. Die Arztpraxis bleibt „Herrin der Daten“ und der Dienstleister handelt als verlängerter Arm. Ein solcher AV-Vertrag stellt sicher, dass keine unbefugte Offenbarung im Sinne des §203 StGB vorliegt, weil der Dienstleister eben offiziell zur Verschwiegenheit verpflichtet und Teil des Behandlungsteams im weiteren Sinne ist.

Wichtig: Viele Cloud-KI-Anbieter nutzen die verarbeiteten Daten gern zur Verbesserung ihrer Modelle. Jedoch kann eine solche Weiterverarbeitung zur Verbesserung des KI-Systems *nicht* einfach durch den AV-Vertrag abgedeckt werden kann. In der Praxis sollte man darauf drängen, dass *keine* Patientendaten für Training oder andere Zwecke genutzt werden – oder dies nur nach ausdrücklicher zusätzlicher Patienteneinwilligung geschieht.

Lokale Verarbeitung als Vorteil: Um die Schweigepflichtproblematik elegant zu lösen, setzen Lösungen wie die Medistella AI Box konsequent auf **lokale Verarbeitung**. Hier verbleiben alle Patientendaten physisch und technisch in der Arztpraxis; es findet kein externes „an Dritte Weitergeben“ statt. Damit gibt es auch keine *Hilfsperson* im Sinne des §203 StGB, der man Daten anvertrauen müsste - die KI-Box ist ja Teil Ihrer eigenen Infrastruktur. Dies minimiert das Risiko einer Verletzung des Berufsgeheimnisses erheblich. Natürlich sollten auch interne Mitarbeiter auf Vertraulichkeit verpflichtet sein und Zugriffe z.B. durch Passwörter geschützt werden, aber das sind ohnehin Standards.

Cloud-Anforderungen: DigiG und C5-Zertifizierung

Seit Kurzem gibt es in Deutschland spezielle gesetzliche Vorgaben für den Einsatz von **Cloud-Computing im Gesundheitswesen**. Mit dem Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz, DigiG) wurde zum 1. Juli 2024 § 393 SGB V in Kraft gesetzt. Dieser Paragraph definiert **Mindeststandards für die Cloud-Nutzung** bei der Verarbeitung von Sozial- und Gesundheitsdaten. Für Arztpraxen und deren KI-Dokumentationslösungen sind insbesondere folgende Punkte relevant:

Territoriale Beschränkung: Gesundheitsdaten dürfen laut §393 SGB V nur in Deutschland, der EU, dem EWR oder der Schweiz verarbeitet werden, oder in anderen Ländern mit offiziellem EU-Adequanzbeschluss (angemessenes Datenschutzniveau). Falls ein Cloud-Anbieter die Daten außerhalb Deutschlands verarbeitet, muss er *zusätzlich* eine Niederlassung in Deutschland unterhalten, damit ein inländischer Ansprechpartner und Geltungsbereich vorhanden sind. Praktisch heißt das: US- oder sonstige Drittland-Clouds ohne EU-Standort sind für Gesundheitsdaten tabu. Anbieter wie z.B. Microsoft oder Amazon Cloud müssten garantieren, dass

die Daten in EU-Rechenzentren bleiben und dass ihre Firma einen Sitz in Deutschland hat, um §393 gerecht zu werden.

C5-Testat des BSI: §393 SGB V fordert weiter, dass der Cloud-Anbieter ein gültiges **C5-Attest** vorlegt. C5 steht für *Cloud Computing Compliance Criteria Catalogue*, einen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelten Kriterienkatalog für Cloud-Sicherheit. Ein C5-Testat bestätigt, dass der Cloud-Dienst die rund 125 Sicherheitsanforderungen des BSI-Katalogs erfüllt (bzgl. Zutrittskontrollen, Verschlüsselung, Incident-Management etc.). Seit dem 1. Juli 2025 muss ein *C5-Typ2*-Attest vorliegen, zuvor reichte übergangsweise Typ1. Auch Subunternehmer des Cloud-Anbieters müssen entsprechend zertifiziert sein. Kurz: **Ohne C5-Zertifizierung kein Cloud-Einsatz** – das Gesetz macht dies zur Pflichtvoraussetzung. Alternativ werden gleichwertige Zertifikate (z.B. ISO 27001 mit Gesundheitsprofil) anerkannt, sofern per Verordnung bestimmt. Tipp: Achten Sie darauf, dass der Anbieter Ihrer Cloud-basierten KI-Dokumentation selbst ein C5-Testat vorweisen kann und nicht lediglich die Daten in einem C5-Rechenzentrum verarbeiten lässt.

Technisch-organisatorische Maßnahmen: Über die Zertifizierung hinaus verlangt §393 SGB V, dass dem *Stand der Technik* entsprechende Maßnahmen für Informationssicherheit getroffen werden. Für Vertragsärzte und -zahnärzte verweist das Gesetz auf § 390 SGB V, der branchenspezifische Sicherheitsstandards einfordert. Im Grunde bedeutet dies: Cloud-Lösungen müssen höchsten Sicherheitsstandards genügen – von Ende-zu-Ende-Verschlüsselung über Zugriffsschutz bis hin zu regelmäßigen Penetrationstests. Und Sie als Arzt bzw. Ärztin sollten im Zweifel auch geprüft haben, dass die Technisch-organisatorischen Maßnahmen ordnungsgemäß umgesetzt wurden.

Für eine niedergelassene Praxis, die einen KI-Dokumentationsdienst aus der Cloud nutzen will, heißt das in der Konsequenz: **Fragen Sie den Anbieter gezielt nach C5-Zertifizierung und dem Datenhost-Standort.** Seriöse Anbieter werden diese Anforderungen kennen und erfüllen (müssen).

Sind diese Hürden hoch? Ja – *bewusst hoch*, um Sozialdaten zu schützen. Einige Beobachter sprechen von Innovationshemmenden Vorgaben, aber sie sind geltendes Recht. Wenn ein Anbieter die Anforderungen nicht erfüllt, wäre dessen Einsatz rechtswidrig. Die gute Nachricht: Mit Lösungen wie der Medistella AI Box können Sie diese Cloud-Problematik **umgehen**. Da hier *keine* Cloud genutzt wird, entfallen Nachweise wie C5-Testat und Standortbindung – die Verarbeitung in Ihrer eigenen Praxis unterliegt nicht §393 SGB V in dem Sinne. Die lokale KI-Box ermöglicht es also, modernste KI zu nutzen, ohne die regulatorischen Hürden des Cloud-Einsatzes überspringen zu müssen. Trotzdem bleibt natürlich die Pflicht, für angemessene Sicherheit zu sorgen, aber das liegt weitgehend in Ihrer eigenen Hand und Kontrolle.

EU AI Act und Anforderungen an vertrauenswürdige KI

Der EU AI Act führt einen risikobasierten Regulierungsrahmen für KI-Systeme ein. Anwendungen im Gesundheitsbereich können als hochriskant eingestuft werden. Dies kann Anforderungen an Risikomanagement, Dokumentation, Transparenz, menschliche Aufsicht, Robustheit und Cybersecurity nach sich ziehen. Für Praxen wird es zunehmend wichtig, dass Anbieter nachvollziehbar darlegen, wie sie diese Anforderungen erfüllen.

Zusätzlich wird diskutiert, ob bestimmte KI-Dokumentationsfunktionen als **medizinisches Gerät** (Medical Device) im Sinne der MDR einzustufen sind. Rein administrative Dokumentation fällt tendenziell *nicht* darunter, solange keine diagnostischen oder therapeutischen Entscheidungen beeinflusst werden. Sollte eine KI jedoch medizinische Inhalte interpretieren in einer Weise, die die Behandlung steuert, könnte eine Zertifizierung als Klasse-I-Software nötig sein.

Alles in allem schafft der EU AI Act ein Rahmenwerk, das **vertrauenswürdige KI** fördern soll. Für die Arztpraxis heißt das: KI-Dokumentationssysteme werden in Zukunft geprüft und reguliert sein, was die Sicherheit erhöht. Lösungen wie Medistella, die schon jetzt auf transparente Prozesse (z.B. keine Black-Box-Entscheidungen ohne Ihr Zutun) setzen, sind gut aufgestellt, diese Anforderungen zu erfüllen.

Praxisempfehlung: seriös, sicher und effizient einführen

KI-Dokumentation kann die Praxis spürbar entlasten – vorausgesetzt, sie wird professionell eingeführt und verantwortungsvoll betrieben. Achten Sie auf die Kombination aus hoher technischer Qualität, klaren Verantwortlichkeiten, konsequenter Endkontrolle und einem datenschutz- sowie schweigepflichtkonformen Architekturansatz.

Medistella positioniert sich hierbei mit einem On-Premise-Ansatz: Die Medistella AI Box bringt KI in die Praxis, ohne Cloud, sodass Patientendaten die Praxis nicht verlassen. Dieser Ansatz kann regulatorische Komplexität reduzieren und die digitale Souveränität der Praxis stärken. Entscheidend bleibt: Der menschliche „Final Check“ ist immer Pflicht.

Checkliste: Eignung und Datenschutzkonformität prüfen

Die folgende Checkliste unterstützt bei der Auswahl und Einführung eines KI-Dokumentationssystems. Sie dient als praxisnahe Orientierung und ersetzt keine individuelle Rechtsberatung.

☐ **Verarbeitungsort der Daten:** Bleiben Patienteninformationen vollständig in der Praxis (lokale Verarbeitung) oder werden sie zur KI-Auswertung in eine Cloud übertragen?

- ☐ Bei *Cloud-Lösungen*: Werden die gesetzlichen Vorgaben erfüllt (Serverstandort EU/Deutschland, Niederlassung des Anbieters in DE, **C5-Zertifizierung** vorhanden)?
- ☐ Wenn lokal: Ist sichergestellt, dass *keine* Patientendaten unbefugt das Netzwerk verlassen und die KI-Module offline arbeiten?
- ☐ Handelt es sich um einen **externen Dienstleister**? Falls ja: Wurde ein Auftragsverarbeitungs-Vertrag (AVV) gemäß Art. 28 DSGVO abgeschlossen, der die Vertraulichkeit der Daten garantiert?
- ☐ Sind im AVV insbesondere die **Weiterverwendung der Daten** (z.B. zu Trainingszwecken) ausgeschlossen oder klar geregelt?
- ☐ Wird das Berufsträgergeheimnis (§203 StGB) eingehalten? Sind externe Hilfspersonen korrekt eingebunden und verpflichtet?
- ☐ Gibt es eine klare Rechtsgrundlage und einen sauberen Einwilligungsprozess inkl. Dokumentation?
- ☐ Ist eine Datenschutz-Folgenabschätzung (DSFA) erforderlich und durchgeführt? Sind TOMs dokumentiert?
- ☐ Wie werden Audioaufnahmen und Transkripte gespeichert, geschützt und gelöscht? (Speicherbegrenzung, Löschkonzept, Verschlüsselung)
- ☐ Ist die Anwendung mit dem bestehenden PVS kompatibel? Wie funktioniert die Übernahme ins PVS? (z.B. GDT-Schnittstelle, Exportformate, Copy-Paste, API)
- ☐ Sind Audioqualität und Hardware geeignet (Mikrofon, Raumakustik, Prozesse im Sprechzimmer)?
- ☐ Ist „Human in the Loop“ technisch und organisatorisch abgesichert (Pflicht zur Prüfung und Freigabe durch Ärztin/Arzt, Möglichkeit zur manuellen Nachbearbeitung)?
- ☐ Unterstützt das System Mehrsprachigkeit und medizinischen Kontext (Fachtermini, Medikamentennamen, Abkürzungen)?
- ☐ Gibt es Support, Updates, Wartungs- und Notfallprozesse (Fallback bei Ausfall)?
- ☐ Sind Kostenmodell, Vertragslaufzeiten und Rechte an den erzeugten Dokumenten transparent geregelt?
- ☐ Wie stellt der Anbieter Compliance mit künftigen Anforderungen (z.B. EU AI Act) dar?

Fazit

Die medizinische Dokumentation mittels KI-Unterstützung ist vom Zukunftstrend zum greifbaren **Mehrwert im Praxisalltag** geworden. Richtig eingesetzt, kann ein KI-Dokumentationssystem Ärztinnen und Ärzte signifikant von Schreibarbeit entlasten, Fehler in der Dokumentation reduzieren und mehr Zeit für die Patientenversorgung schaffen. Gleichzeitig müssen aber die besonderen Anforderungen des Gesundheitswesens beachtet werden: Datenschutz und Schweigepflicht haben oberste Priorität, und die Qualität der Dokumentation muss jederzeit gewährleistet bleiben. Dieses Whitepaper hat gezeigt, dass *technisch* bereits alle Bausteine vorhanden sind – von exzellenter Spracherkennung bis zu intelligenten Sprachmodellen – und dass *organisatorisch* sowie *rechtlich* durch sorgfältige Planung und Kontrolle ein sicherer Einsatz möglich ist.

Die **Medistella AI Box** steht exemplarisch für eine Lösung, die viele der angesprochenen Herausforderungen durch ihren Ansatz umgeht oder minimiert. Durch die lokale Verarbeitung der Daten innerhalb der Praxis werden Cloud-Risiken und komplexe Datenschutzprobleme vermieden. Die moderne KI-Infrastruktur liefert präzise Transkriptionen und smarte Zusammenfassungen, speziell abgestimmt auf medizinische Inhalte. Dabei bleibt die volle Integration in bestehende Praxissoftware gewährleistet, sodass der Übergang in den gewohnten Workflow reibungslos verläuft. All dies geschieht, ohne das ärztliche Berufsgeheimnis zu kompromittieren – Patientendaten verlassen zu keinem Zeitpunkt die sichere Umgebung der Praxis. Natürlich gilt auch hier: Der Arzt behält das letzte Wort und prüft die KI-Dokumente, bevor sie endgültig werden. Doch gerade diese Kombination – **KI-Power, Datenschutz plus menschliche Expertise** – führt zu optimalen Ergebnissen.



Über Medistella

Medistella entwickelt KI-basierte Systeme zur datenschutzkonformen medizinischen Dokumentation. Der Fokus liegt auf lokal betriebenen Lösungen für Arztpraxen, bei denen Patientendaten die Praxis nicht verlassen.

Medistella richtet sich an niedergelassene Ärztinnen und Ärzte mit hohen Anforderungen an Datenschutz und digitale Souveränität.

Kontakt

Medistella GmbH

www.medistella.de

info@medistella.de

Medistella GmbH · Sitz: Regensburg

Geschäftsführer: Florian Zenk

© 2026 Medistella GmbH

Dieses Dokument dient ausschließlich Informationszwecken und stellt keine rechtliche oder medizinische Beratung dar.